



Proceedings of
Ist International e-Conference
on
**Emerging Trends in Circuit-branch
Technologies and Applications**

(ETCTA2021)

3rd - 4th April, 2021

Editor-in-Chief

Dr. A.D. Sarma

Editorial Board

Associate Editors

Dr. Y. Rama Devi

Dr. G. Suresh Babu

Dr. D. Krishna Reddy

Dr. K. Radhika

Dr. D. L. Srinivas Reddy

Content Editors

Dr. P Sathish

Dr. N. V. Phanendra Babu

Organized by

Chaitanya Bharathi Institute of Technology

(Autonomous under UGC)

Affiliated to Osmania University

Hyderabad-500075

Telangana State, INDIA

www.cbit.ac.in



CHAITANYA BHARATHI
INSTITUTE OF TECHNOLOGY (A)

Kokapet (Village), Gandipet, Hyderabad, Telangana-500075. www.cbit.ac.in



ISO Certified
9001:2015

COMMITTED TO
RESEARCH,
INNOVATION AND
EDUCATION

42
years

Proceedings of the International Conference On Emerging Trends in Circuit-branch Technologies and Applications (ETCTA-2021)

Editor-in-Chief

Dr. A.D. Sarma

Editorial Board

Associate Editors

Dr. Y. Rama Devi

Dr. D. Krishna Reddy

Dr. G. Suresh Babu

Dr. K. Radhika

Dr.D.L .Srinivas Reddy

Content Editors

Dr. P Sathish

Dr. N. V. Phanendra Babu



Proceedings of the International Conference on Emerging Trends in Circuit Branches Technologies and Applications (ETCTA2021)

Edition: First-2021

No part of this book may be reproduced or transmitted in any form by any means, electronic or mechanical, including photocopy, recording or any information storage and retrieval system, without permission in writing from the copyright owners.

DISCLAIMER

The author is solely responsible for the contents published in this book. The publishers or editors do not take any responsibility for the same in any manner. Errors, if any, are purely unintentional and readers are requested to communicate such errors to the editors or publishers to avoid discrepancies in future.

ISBN: 978-1-68576-062-5

Publishing Typeset & Distribution by
INSC PUBLISHING HOUSE (IPH)
Pushpagiri Complex, Beside SBI
Housing Board, K.M. Road
Chikkamagaluru Karnataka
Tel.: +91-7619574868
E-mail: iph@insc.in



**CHAITANYA BHARATHI
INSTITUTE OF TECHNOLOGY (A)**

Kokapet (Village), Gandipet, Hyderabad, Telangana-500075. www.cbit.ac.in



COMMITTED TO
RESEARCH,
INNOVATION AND
EDUCATION

42
years

**1st INTERNATIONAL E-CONFERENCE
ON
EMERGING TRENDS IN CIRCUIT-BRANCH TECHNOLOGIES AND
APPLICATIONS (ETCTA-2021)**
3 - 4 April, 2021

Chief Patrons

Sri. N.Subhash, President, CBIT

Kavi kireeti Dr. V. Malakonda Reddy, Former President, CBIT

Conference Chair

Dr. G. P. Saradhi Varma, Principal, CBIT

Technical Advisor

Dr. A.D. Sarma, Director R & D, CBIT

Conveners

Dr. Y. Rama Devi, HoD, CSE,
Vice-Chairperson

Dr. D. Krishna Reddy, HoD, ECE,
Vice-Chairperson

Dr. G. Suresh Babu, HoD, EEE

Dr. K. Radhika, HoD, IT

Dr.D.L .Srinivas Reddy, HoD, MCA

Co-Conveners

Dr. T. Sridevi, CSE Dept.

Dr. N. V Phanendra Babu, EEE Dept.

Dr. R. Ravinder Reddy, CSE Dept.

Dr. M. Venugopalachary, IT Dept.

Dr. P. Sathish, ECE Dept.

Dr. B. Veerajyothi, IT Dept.

Dr. K. Suman, ECE Dept.

Dr. K. S. Sadasiva Rao, MCA Dept.

Dr. B. Suresh Kumar, EEE Dept

Dr. G N R Prasad, MCA Dept.

International Advisory Committee

1. Prof. B. M. Azizur Rahman, Professor, City, University of London, U. K.
2. Dr. Burganskiy, Deputy Design General, Tactical Missiles Corporation, Mashinostroeniya, Moscow, Russia.
3. Dr. Hassan Haes Alhelou, Tishreen University, Syria.
4. Dr. Pawan Lingras, Saint Mary's University, Canada
5. Prof. Yu-Dong Zhang, University of Leicester, United Kingdom.
6. Prof. João Manuel R. S. Tavares, Universidade do Porto (FEUP) Porto, Portugal.
7. Prof. Aime Lay-Ekuakille, Dept of Innovation Engineering University of Salento, Italy.
8. Dr. Harikishan Eppanapalli, Chairman & CEO, The CIC Group, Inc. New Jersey, USA.
9. Prof. Pierluigi Siano, University of Salerno, Italy
10. Prof. Baseem Khan, Hawassa University, Hawassa, Sidama Region, Ethiopia.

National Advisory Committee

1. Dr. B N De Bhowmic, ED-TD, PGCIL
2. Sri. C Anand, ED, R&D, BHEL
3. Prof. Krishna Vasudevan, EEE, IIT Madras
4. Dr. Sudeb Das Guptha, HoD-ECE, IIT Roorkee, India.
5. Dr. E Damoder Reddy, NIT, Goa, India.
6. Dr. Ashish K Sukla, Scientist/Engineer, SAC-ISRO, India.
7. Dr. R. Padmavathi, Associate Professor, CSE, NIT – Warangal
8. Prof. C R Rao, HCU
9. Prof. K Shyamala, professor & Dean of Informatics, Osmania University
10. Prof. V Kamakshi Prasad, Director Evaluation, JNTUH
11. Prof. C Shoba Bindu, Director R&D, JNTUA
12. Prof. R. sridevi, professor, centre of excellence in cyber security cell, JNTUH, hyd.
13. Prof. K. Shahu Chatrapati, HoD, CSE, JNTUH -Manthani

Internal Advisory Committee

1. Dr. Umakanta Choudhury, Director I&I, CBIT
2. Dr. Suresh Pabboju, Director-IQAC,CBIT
3. Dr. K. Krishna Veni, Director-Academics, CBIT
4. Dr. M Swamy Das, Joint Director-Academics, CBIT

**Smt. P. SABITHA INDRA REDDY
MINISTER FOR EDUCATION
Government of Telangana.**



**Off.: 3rd Floor, SCERT Building
Opp. LB Stadium "E" Gate
Basheer Bagh, Hyderabad-
500001
Phone : 040-23459922
Fax : 040-23459912
Mail :
sabithaindrareddi@gmail.com**

MESSAGE

I am glad to note that Chaitanya Bharathi Institute of Technology is organizing a Two-day Online International Conference and would like to congratulate the management, the principal and the faculty of Chaitanya Bharathi Institute of Technology.

I am sure that this conference on the Emerging Technologies in the field of engineering and its applications will offer a great platform to the academicians, research scholars, faculty and the industry practitioners for the exchange of the latest developments, ideas and research.

I wish this conference to be a splendid event, both in terms of intellectual quality and social gratification. You have the right mix of topics, diverse et of speakers and high-level array of participants that will definitely make it a successful event.

My best wishes to you all for making it very engaging and insightful conference with great learning experience during this pandemic situation.

(P SABITHA INDRA REDDY)

Prof. Ch. Gopal Reddy, M.Sc, Ph.D
Professor of Physics
OSMANIA UNIVERSITY Registrar (FAC)
HYDERABAD 500 007



(Accredited by NAAC with the
Highest Grade "A+")

Phone No: 040-2709 8043 (0)

: 040-2768 2363 (0)

: 040-2322 2615 (R)

Fax: 040-2709 0020 (0)

&

e-mail:registrar@osmania.ac.in



March 15, 2021

MESSAGE

It gives me a great pleasure to know that the Chaitanya Bharathi Institute of Technology (A), Affiliated to Osmania University, Hyderabad is organizing a two day International Conference on "**Emerging Trends in Circuit branch Technologies and Applications (ETCTA-2021)**" during April 3-4, 2021.

I am sure that the conference will provide a forum where Researchers, Engineers, Eminent professionals and Scientists will interact on circuit branch technologies such as Signal Processing, Satellite Communications, Power Systems, Artificial Intelligence and Machine Learning, etc. and chalk out a concrete road map for latest and innovative developments in circuit branch technologies for various industrial applications.

I wish the conference a great success and the participants a fruitful interaction with some of the legends of the circuit branch technologies and carry back home some wonderful memories and insightful thoughts. I appreciate the efforts of CBIT for taking the lead in organizing the International Conference and wish that the conference will be a grand success.

(Prof. Ch. Gopal Reddy)



Message from President, CBIT

Chaitanya Bharathi Institute of Technology (CBIT), committed to Research and Innovation, with an objective to facilitate Individual and Collaborative Research for Sponsored and Consultancy Projects had established, in August, 2018, a State-of-the-Art Research and Entrepreneurship Hub, to support advanced Research and Innovation Ecosystem, connecting Innovators across Industry and Individuals. The Mission of the Hub is to streamline the Research Activities and contribute Products, Processes and Systems, to make a mark, in the ‘Make in India’ Program actively and aggressively promoted by the Government of India. To achieve this, each of the Departments will engage in Advanced Research of their Projects in the Independent space earmarked to them.

It gives me immense pleasure to partake in the International conference on **“Emerging Trends in Circuit branch Technologies and Applications”** (ETCTA-2021), during April 3-4, 2021, Organized by Departments of CSE, ECE, EEE, IT and MCA in coordination with R&D Centre as the Vision shared by the Members of the Board of Governors, is manifesting as a reality, during the 42th Year of Institutes successful Journey.

ETCTA2021 will reflect the state of art on the applications of Artificial Intelligence, Machine Learning, Deep Learning, IoT, Data science in to various fields engineering such as circuit and non-circuit branch technologies. This will provide a forum where researchers, academicians, industry personnel, and scientists can present their original research, exchange ideas and promote networking for scientific and industrial collaboration. The keynote address by eminent persons, Invited talks, paper presentations will be an integral part of the conference.

I congratulate the academic, non-teaching and other staff for ushering in the change towards research by conducting the international conference by inviting Scientists, Engineers academicians and research scholars from India and abroad to present their works in areas of their interest. Government of India and the Academic Regulatory Bodies are encouraging Research, innovations and incubations which would enable Innovation in Technology, Developing Products and hence valuable Patents. Faculty in turn can crystallize their areas of Research interest and pursue towards achieving long term Research Goals. Research Groups have been formed in the Institute involving Staff and Students with inter disciplinary interests, to take up Research of contemporary times. Carrying on the qualitative Research of yester years, duly protecting its values and ethics which are essential in this context.

I am encouraged to see that the Principal, Director R&D, staff and students of the institute are committed to excel in the research and hope that you will raise the Banner of the Institute amongst the recognized Centers of Excellence for Advanced Research in the Country and abroad.

Wish you all success in every sphere of Research and Development.

N. Subash,
President, CBI

Chaitanya Bharathi Institute of Technology (A)
📍 Chaitanya Bharathi (PO), Kokapet (V), Gandipet (M),
Ranga Reddy District, Hyderabad - 500 075, Telangana, India
📞 040-24193276; 79, 80
✉️ principal@cbit.ac.in | 🌐 www.cbit.ac.in





CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY (A)

Foreword

In the month of November 2020, it was decided by the Principal, Director R&D and HoDs to conduct an international conference in the present academic year (2020-21) to provide a platform for faculty and students to present their research findings. Research and development form the backbone of our curriculum at CBIT. The staff and students are engaged in various path-breaking innovative research activities all throughout the year. Due to COVID pandemic conditions, the International Conference is planned in virtual mode by the institute. The International Conference on "**Emerging Trends in Circuit Branch Technologies and Applications**" (ETCTA 2021) planned combined by the departments of CSE, ECE, EEE, IT and MCA during 3-4 April 2021 provides a platform for scientists, academicians, research scholars and industry personnel globally to discuss on latest trends and innovations in Electrical, Computers and Communication areas.

The ETCTA 2021 Organizing committee rigorously publicized the event and invited research papers both from academic institutions and research organizations. It is stressed that the papers should be original research articles that illustrate research results, application projects, survey works and industrial experiences describing significant advances in the disciplines of Electrical, Computer and Communication Engineering fields. This effort guaranteed submissions from significant number of well recognized researchers. All the submissions underwent a strenuous peer-review process which comprised expert reviewers. The papers were then reviewed based on their contributions, technical content, originality and clarity. The entire process which includes the submissions, review and acceptance process, was done electronically. The meticulously selected abstracts have been compiled and published as *souvenir* showcasing the research in progress and the outcomes of the completed projects. All the accepted papers for presentation will be published in the proceedings of ETCTA 2021. All the these efforts undertaken by the Organizing and Technical Committee has led to an exciting and a high-quality technical conference program, featuring excellent presentations for all attendees to enjoy, appreciate and expand their expertise in the latest developments in the areas of their interest.

Chaitanya Bharathi Institute of Technology (A)

📍 Chaitanya Bharathi (PO), Kokapet (V), Gandipet (M),
Ranga Reddy District, Hyderabad - 500 075, Telangana, India
📞 040-24193276, 79, 80
✉️ principal@cbit.ac.in • www.cbit.ac.in





CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY (A)

The knowledge gained from this international conference will not only help the Participants to better define their requirements and develop advanced Products but also encourage the Industries to develop high performance, cost effective and affordable Products in addition to stimulating the Academic Faculty to focus on developing Innovative Products. The International / National Advisory and Editorial Committee members and Conveners, Co-conveners of the Dept. of CSE, ECE, EEE, IT, MCA and other teaching and non-teaching staff undertaken their Assignments and their efforts will remain laudable in the Years to come.

With great pleasure, we thankfully acknowledge the participation of all the Delegates and hope they would be our Knowledge Partners in all the future Annual Programs of the Technical events, and we formally through this message, invite them to virtually participate in the International conference during 3-4 April 2021.

I wish the conference all the very best and urge all participants to brainstorm on the various thrust areas of the conference.

With Warm Wishes

Dr. A. D. Sarma
Technical Advisor ETCTA-2021
Director R&D

Prof. G. Pardha Saradhi Varma
Chairman ETCTA-2021
Principal

Chaitanya Bharathi Institute of Technology (A)
Chaitanya Bharathi (PO), Kokapet (V), Gandipet (M),
Ranga Reddy District, Hyderabad - 500 075, Telangana, India
040-24193276, 79, 80
principal@cbit.ac.in www.cbit.ac.in





**CHAITANYA BHARATHI
INSTITUTE OF TECHNOLOGY (A)**

Intent of Quintet

Our joy knew no bounds while we were asked to host an ONLINE International Conference on Emerging Trends in Circuit Branch Technologies and Applications [ETCTA2021] which is debut in the annals of academics in our campus. The congregation becomes perfect blend of Emerging Trends, Technologies and Applications of Cute branches of Engineering centering Circuit.

The necessity of Big Data for smart computing to arrive Internet of things has become curtain raiser to process the signal with systematic Power.

A green Signal (of organizing an International Conference) is processed from highly systematic Power (Management) through Global Positioning Systems (Principal) to Smart celebrity (Director R&D) for the benefit of Big Data (society) where the Quintet (we) are only Things.

We are bestowed to be the convenors for this International Conference where emanation of Knowledge takes place when watched through ETCTA Kaleidoscope.

This Souvenir is the hard memory that lasts long for the soft indelible mark you left with us.

We thank Management, Principal, Director R&D, Reverend Speakers, Stalwart Chairpersons, Speaker Celebrities, Honorable Juries, Dedicated Researchers, Devoted Audience and finally YOU the curious reader of this Treatise.

Yours sincerely

- | | |
|-----------------------------|---------|
| 1. Dr .Y.RamaDevi | HoD-CSE |
| 2. Dr.D.Krishna Reddy | HoD-ECE |
| 3. Dr G.Suresh Babu | HoD-EEE |
| 4. Dr K.Radhika | HoD-IT |
| 5. Dr. D L. Srinivasa Reddy | HoD-MCA |

Program Schedule

International Conference on Emerging Trends in Circuit-branch Technologies and Applications (ETCTA-2021)

DAY-1	April 03, 2021				Time			
	Inaugural Session				09:30-10:45			
	Session-A		Session-B					
	A1	Machine Learning and IoT Applications (CSE)	B1	VLSI and Embedded Systems (ECE)	11:00-13:00			
	Lunch Break				13:00-13:45			
	A2	Electrical Power Engineering (EEE)	B2	Big Data and Data Mining (IT)	13:45-15:30			
	Tea Break				15:30-15:45			
	A3	Artificial Intelligence and Deep Learning (MCA)	B3	Natural Language Processing and Computer Vision (CSE)	15:45-17:30			
DAY-2	April 04, 2021				Time			
	A4	Cloud Computing and Cyber Security (CSE)	B4	RF Communications and Applications (ECE)	09:30-11:15			
	Tea Break				11:15-11:30			
	A5	Health Monitoring and Forecasting Pandemic			11:30-13:15			
	Lunch Break				13:15-14:30			
	Valedictory				14:30-15:40			



Keynote Address

Prof. B M Azizur Rahman

School of Engineering and Mathematical Sciences, City, University of London EC1V 0HB, UK

Tel: +44-20-7040-8123 *Mobile:* +44-79-31-256-982

Email: B.M.A.Rahman@city.ac.uk

Photonics, a Key Enabling Technology – Its Emergence and the Opportunities

With the advent of semiconductor lasers and low-loss optical fibres in mid 60s, the progress of Photonics technology has been rapid. Photonics, as the name indicates, manipulates photon or light, similar as Electronics manipulate electrons, but much faster. Photonics made a significant impact, in the field of optical fibre links, joining all the countries and major cities by faster Tbit/sec bandwidth link, made Internet almost free, thinner flat screen display for computers and mobile phones, CD and DVD for data storage, and lasers for healthcare and material processing applications. During the last EU research cycle, Horizon2020, Photonics was identified as one of the 6 Key Enabling Technologies, and expected to play a key role in shaping the technology landscape of this century.

However, as the Photonics has reached maturity, the associated devices have themselves become more complex. The optimization of such advanced devices requires an accurate knowledge of their light wave propagation characteristics and their dependence on the system fabrication parameters. The intricate arrangement of photonic crystal fibres, low-cost production of 220 nm thick silicon nanowire and even thinner 30-40 nm thick plasmonic guided-wave devices are establishing as exotic functional photonic devices. Optical sensors are now more widely being considered over electrical or electro-chemical sensors because of their many advantages, such as small size, electro-magnetic immunity, high sensitivity and these fibre-based sensors can be easily multiplexed.

The optimization of existing realistic designs or the evaluation of new designs for photonic devices and sub-systems has created significant interest in the development and use of effective numerical methods. Of the different numerical approaches for modal solutions reported so far, the finite element method (FEM) [1] has been established as one of the most powerful and versatile methods. Prof. Rahman was first in the world to develop finite element based computer code to characterize optical waveguides and photonic devices. Numerically simulated results for some important guided-wave photonic devices and optical sensors, by using the full vectorial finite element-based approaches, will be presented.

References

- [1] B M A Rahman and J B Davies, *J. Lightwave Tech.*, **2**, pp.682-688, Oct. 1984.

Sessions Schedule

<u>Paper ID</u>	<u>Paper Titles</u>	<u>Page No.</u>
<u>Session-A1: Machine Learning and IoT Applications</u>		
ETCTA21_124	IoT For Monitoring Oxygen Levels in Shrimp Ponds for Better Nutrient Management <i>Authors: Raghavendar Raju L, Tejendar Kaur, K Kiran, M Jaya Shravani</i>	3 - 8
ETCTA21_121	Enhancing Zero-Day Attacks Detection Rate Using Machine Learning – A Survey <i>Authors: K. Swathi, G. Narsimha</i>	9 - 14
ETCTA21_107	A survey on Feature Selection and Feature Extraction in Deep Learning <i>Authors: A. Thatikonda Somashekar, B.B Srinaiyah</i>	15 - 20
ETCTA21_148	Detection of plant Disease Using Image Processing based on KNN and GLCM Algorithms <i>Authors: N.S. Shivani, M.V. Jeeva, Dr.R Ravinder Reddy</i>	21 - 24
ETCTA21_102	Music Genre Classification <i>Authors: G Naga Sujini, J Sreedevi, Dr M Ramabai, V.Mounica</i>	25 - 32
ETCTA21_152	A Review on Neuro Feedback System using Brain Computer Interface <i>Authors: G.Kavita, Namya Reddy, Akshitha</i>	33 - 36
<u>Session-B1: VLSI and Embedded Systems</u>		
ETCTA21_204	Design and Analysis of Approximate Lower-Part OR Adder for Low Power Computations <i>Authors: Varala Pasula Nikhila, Dr. N. Alivelu Manga</i>	39 - 42
ETCTA21_203	Implementation of FPGA based Image Processing Algorithm Using Xilinx EDK <i>Authors: Aruna Kokkula, B. Indira Priyadarshini, P.Amulya, B. Charan Supraj</i>	43 - 48
ETCTA21_208	Trust Computational Methodology for an Internet of things <i>Authors: M.Rajendra Prasad and D.Krishna Reddy</i>	49 - 56
ETCTA21_214	A Prototype Wi-Fi Controlled Car using NodeMCU <i>Authors: T. Satya Sai Kiran, T. Sridher</i>	57 - 60
ETCTA21_207	Deep learning in sensing and Detecting Modulation scheme in Cognitive Radio <i>Authors: P Ravinder Kumar, Sandeep VM, Subhash S Kulkarni,</i>	61 - 64
<u>Session-A2: Electrical Power Engineering</u>		
ETCTA21_307	Optimal Distributed Generator and Shunt Capacitor in Radial Distribution System Using Particle Swarm Optimization <i>Authors: P.Sree Lekha, Dr.P.Venkata Prasad</i>	67 - 72
ETCTA21_308	AI based Cyber-attack Resistant Microgrid System with IRNSS Synchronization <i>Authors: M Balasubbareddy, P Venkata Prasad, Saini Varshini, A D Sarma.</i>	73 - 76
ETCTA21_305	Power Quality Concerns in Implementing Smart Distribution Grid Applications <i>Authors: S. Swathi, Dr.B.Suresh Kumar, Dr. J. Upendar</i>	77– 82
ETCTA21_309	Power Quality Conditioning by UPQC using PQ and DQ Theory <i>Authors: M Balasubbareddy, Saini Varshini.</i>	83 - 86

Session-B2: Big Data and Data Mining

ETCTA21_402	Ransomware Attacks – Prevention and Mitigation	89 - 94
	<i>Authors: Goutham Rayapati, Suma Sri Mandru</i>	
ETCTA21_428	Towards Privacy-Preserving of Time Series IoT Data Publishing	95 - 98
	<i>Authors: J.Aruna Santhi</i>	
ETCTA21_414	Intelligent System to Manage and Monitor Machine Health	99 - 104
	<i>Authors: J. Hima Bindu, V. Amrutha Valli.</i>	
ETCTA21_415	The Verge of Extinction	105 - 110
	<i>Authors: K. Suganya, B. Surya Samantha, S. Vamsi Krishna..</i>	
ETCTA21_417	Stock Price Prediction on News Data and Market Data Using ML Techniques	111 - 120
	<i>Authors: Veena Madhuri. S, Sirisha. A</i>	
ETCTA21_418	A Deep Learning Approach to Identify Missing Children	121 - 126
	<i>Authors: K.Sanjay Kumar, M.Banu Teja, P.Vasantha sena, Dr.M.Venugopala chary, Prof. Sammula Porika</i>	

Session-A3: Artificial Intelligence and Deep Learning

ETCTA21_505	Implementation of A Privacy Based Deep Learning Algorithm for Medical Data Analytics	129 - 134
	<i>Authors: A. Thirupathi Battu, B. Dr.D.Lakshmi Sreenivasa Reddy</i>	
ETCTA21_506	A Review of Wi-Fi Security Protocols and Detailed Discussion on WPA3	135- 142
	<i>Authors: Jithender Reddy Machana, Ashrith Kotha, Sumanth Pulluru.</i>	
ETCTA21_507	The Deep Learning Algorithm for Animal Detection	143 - 148
	<i>Authors: A. Thirupathi Battu, B. Dr.D.Lakshmi Sreenivasa Reddy, C.Thatikonda Soma Shekar</i>	
ETCTA21_508	Smart Farming using IOT and Machine Learning	149 - 154
	<i>Authors: Sandeep Kalari, Dr.B.Indira.</i>	
ETCTA21_426	Internet of Things Applications Enablement its Challenges and Trends	155 - 158
	<i>Authors: Vivek Veeraiah, Dr. G. K. Ravikumar.</i>	
ETCTA21_501	Decision Support Tool for Examination Questions according to Bloom's Taxonomy	159 - 162
	<i>Authors: Dr. G. N. R. Prasad, Bhavani uddagiri</i>	

Session-B3: Natural Language Processing and Computer Vision

ETCTA21_104	Automated Attendance Using: Facial Recognition	165 – 168
	<i>Authors: Vijay Kumar, Janith Adavala, Devendar Maddeboina</i>	
ETCTA21_144	Comparative Study of Single Image Super Resolution Techniques	169 - 178
	<i>Authors: Hruday Tej Akkaladevi, A Nagesh , N. Rama Devi</i>	
ETCTA21_142	A Review: Image Synthesis from Textual Descriptions using GANs	179 - 184
	<i>Authors: Srinivas Pavan , Varun Sundaram , Dr. K. Sagar</i>	
ETCTA21_137	A Survey on Speaker Diarization Techniques	185 - 190
	<i>Authors: Saad Ahmed, Shaik Abdul Muqtadeer, Zubair Ahmed</i>	
ETCTA21_138	Opinion of Specific Tweets on Twitter	191 - 196
	<i>Authors: Sai Goutham Goli, Sanjeev Varkala, Sai Tarun Chinthalapati, Venkataramana Battula</i>	
ETCTA21_401	Types of Cyber-attacks and Defense Strategies	197 - 202
	<i>Authors: Mandru Suma Sri, Rayapati Goutham</i>	

Session-A4: Cloud Computing and Cyber Security

- ETCTA21_101** DOALB: Nature inspired Meta heuristic -Dragonfly Optimization Algorithm based Improved Load balancing Technique for Cloud
Authors: Vijayakumar Polepally. 205 - 210
- ETCTA21_119** Exploiting the vulnerabilities of Traditional Captcha System and Exemplifying Smart Captcha System *Authors: Mrs. S. Sandhya, Ms. Satvika Eda,* 211 - 216
Ms. Prathyusha Kundavaram, Ms. Srishti Mathur
- ETCTA21_139** A Trust Based Approach for Providing Security in Mobile Ad hoc Networks
Authors: Venkata Krishna Reddy M ,Dr. Ravinder Reddy. 217 - 222
- ETCTA21_128** Load Balancing policy to reduce the Data Center Processing time in Cloud Environment using Cloud Analyst
Authors: Ramana Reddy B , Indiramma M 223 - 226

Session-B4: RF Communications and Applications

- ETCTA21_213** Performance Evaluation of GNSS system using Z-test for RAIM 229 - 232
Authors: D.Sony, JB Farheen, Dr.D.Krishna Reddy Dr.P.Naveen Kumar
- ETCTA21_201** Analytical Study of Global Solar Radiation Estimation and Forecasting methods: a review 233 - 238
Authors: Deepa Rani Yadav, Stuti Shukla Datta
- ETCTA21_215** Satellite Selection Algorithm for RAIM Applications 239 - 242
Authors: D.Sony, S.Chandravardhan, D.Krishna Reddy, .P.Naveen Kumar
- ETCTA21_205** Design and Analysis of High Speed Parallel Meander Transmission Lines 243- 248
Authors: B.HariPrasad Naik , A.Gopal , D.Krishna Reddy

Session- A5: Health Monitoring and Forecasting Pandemic

- ETCTA21_216** Preliminary Result of COVID-19 Detection through Chest X-Ray using Artificial Intelligence 251- 254
Authors: Nitta Nikhila Raj , Vyshnavi Cheedepudi, Abhishek Adire, T Sridher
- ETCTA21_136** Applying Relu and Tanh Functions for the Detection of Lung Cancer using Deep Learning 255- 260
Authors: Madhavi Aluka¹, Sumathi Ganesan, Vijay Pal Reddy P
- ETCTA21_422** Survey on Diabetic Retinopathy Detection 261- 266
Authors: Pravallika Elluri, Sirisha Alamanda
- ETCTA21_211** A Simple Model for Forecasting Confirmed COVID-19 Cases in a Given System 267 - 271
Authors: A.D. Sarma, K. Lakshmana and T. Sridher

Session-A1:

Machine Learning and IoT Applications

IoT for Monitoring Oxygen Levels in Shrimp Ponds for Better Nutrient Management

Raghavendar Raju L

Department of CSE

Matrusri Engineering College

Hyderabad, Telangana-500059, India

lraghavenderraju@gmail.com

Tejender Kaur

Department of CSE

Matrusri Engineering College

Hyderabad, Telangana-500059, India

tejender2000@gmail.com

K Kiran

Department of CSE

Matrusri Engineering College Hyderabad,

Telangana-500059, India

Abstract: The freshwater shrimp fisheries sector plays an important role to the economy for the fishmongers and health of the citizens. It also has an significant role in providing nutrition, employment, reducing poverty. Increasing population growth, environmental degradation, and a worldwide temperature alteration are diminishing the level of the fisheries (freshwater shrimp) area. There are different ecological measurements, for example, temperature, salinity, turbidity, ph, dissolved oxygen level etc, which are a valuable part in the production levels of shrimps. Nevertheless, old- fashioned (i.e. manual) monitoring systems are slow, complicated, inefficient and never performed. Therefore, freshwater farming should be made to address these problems in real time in which the computerized system will be constant. This monitoring system is made by the use of technologies like IoT (Arduino), web applications, various sensors which all together will deliver the information on the web application from where farmer can check the water parameter values like temperature, salinity, turbidity, ph, dissolved oxygen due to which the farmer can check the status of the pond and take the required care as needed. Different characteristics of shrimp like weight ,survival rate etc will be monitored through this system. The wireless sensor network- based system is made by the use of sensors like temperature, turbidity, salinity, ph, dissolved oxygen to measure the quality of water. Therefore, it allows the farmers to easily check the water parameter and keep it properly controlled so that the water quality is maintained regularly.

Key words: IoT, Shrimp pond, Oxygen levels, Sensor nodes.

I. Introduction

The fresh water shrimp monitoring system is made by the use of technologies like IoT (Arduino), web applications, various sensors which all together will deliver the information on the web application from where farmer can check the water parameter values like temperature, salinity, turbidity, ph, dissolved oxygen due to which the farmer can check

the status of the pond and take the required care as needed. This system will monitor the size, weight, and percentage of shrimp survival rate which will ensure good production level of the shrimp every year.

A. Motivation

Life is getting simpler and easier with the advancement of technology, with all told aspects. Eventually after a while, IoT has the potential to be limitless. In present time manual systems are less preferred over the maul system. Nevertheless, old- fashioned (i.e. manual) monitoring systems are slow, complicated, inefficient and are actually not performed. Therefore, in real time to handle these problems freshwater water shrimp farm monitoring system should be made which is able to be a computerized and constant monitoring system for the shrimps. This is the foremost primary reason for the motivation for this work that will be automatically able to monitor the various factors and send the data to the farmers in order that they can take the required care as needed of their shrimp ponds.

B. Applications of IoT

In an Internet of Things (IoT), Internet and Physical devices like sensors are two most important things for connectivity and information collection. The main purpose is to collect data of the sensors. Sensors is the front end IoT which are connected to IoT networks directly or indirectly after signal conversion and processing. In the period of eventually growing technology there are many real applications of IoT.

Some of the applications of IoT are given below:

- Smart Pond Monitoring System
- Wearables (fitness band)
- Health
- Traffic Monitoring
- Smart Farming
- Smart Grids
- Water Supply

- Maintenance Management
- Smart City

C. Smart Pond Monitoring System

The development of Smart Pond Monitoring System which has been designed using IoT is done keeping the high risk associated with aquaculture farming in mind. It gives the shrimp ponds a dynamic boost for farm yielding and productivity.

The most important factor is the quality of the water as it directly affects mortality rates and health status of shrimp. Parameters like temperature, pH, salinity, turbidity and so on are measured in this system.

D. Main Objectives

The objective of this project is to create monitoring system to check the quality of pond water which is to be made by the use of various sensors such as temperature, conductivity, pH, dissolved oxygen and turbidity with the use of IoT technologies and web applications so the data can be sent to the farmers and they can take the required care as needed for their ponds. This system makes the task easy for shrimp farmers as this system will monitor the characteristics of shrimp like weight, survival rate etc which will ensure good production level of the shrimp regularly.

The purpose of the Smart Pond Monitoring System is to produce top quality shrimps by creating a safe and secure habitat that will maintain the water quality in the shrimp pond. Water quality plays an important role in this project. Therefore, we should keep a track and check the system constantly.

E. Background

The environment metrics required for shrimp farming are given below which include water temperature, pH level of water, turbidity of water, water salinity, dissolved oxygen levels in water etc.

The most suitable values are as follows

- Temperature(°C): 25-31
- Ph: 4-6,8-9
- Dissolved oxygen (ppm): 4- 7
- Salinity (ppt): 1- 15
- turbidity(% clay): 35

Zain Uddin et al designed the system for measuring the quality of the pond which was designed for Vannamei shrimp cultivation. This system was used for monitoring the quality of pond water which is to be made by the use of various sensors such as temperature, pH, conductivity,

electro-chemical dissolved oxygen and turbidity with the use of IoT technologies and web applications so the data can be sent to the farmers and they can take the required care as needed for their ponds. At Mappakasunggu District, Takalar in Indonesia the implementation of this system took place.

“SAM- IoT” collects the data of various environment metrics needed for a shrimp pond.

F. Problem Statement

The shrimp farming industry globally faces numerous challenges which include various water diseases. old- fashioned (i.e. manual) monitoring systems are slow, complicated, inefficient, and are actually never really performed in real time. There is a huge increase of demand in the fishery markets for nutritious shrimps. To overcome this problem, a computerized monitoring system that will be constantly monitoring must be made. The main barrier of this industry's trouble and difficulties is poor water due to which shrimp farms are getting affected by various diseases, which eventually increases the mortality rate of shrimp as a result, farmers are facing financial losses and are gradually losing their interest in shrimp farming. In order to grow up healthy shrimp, it is mandatory to have right level of water and good water quality in fishponds.

II. Proposed Method

The proposed system contains sensors like temperature, salinity, turbidity, pH, dissolved oxygen level to measure the water parameters with the use of IoT technology. This system will decrease the mortality rate and will bring a huge improvement in shrimp production. It contains of mainly 3 layers which are

- hardware layer
- web application layer
- cloud layer

The physical layer contains of all different sensors and Arduino Yun. This layer will provide all the data collected to an online database which is a part of the next main layer that is cloud layer. Cloud layer handles the data. For application layer, the cloud layer is the data source. Graphical user interface for real- time data visualization to the users is provided by the web application layer that provides the information on daily, weekly, or monthly basis.

This system is mainly designed for shrimp farmers. This system will contain both hardware and software like IoT sensors, web applications based on IoT and cloud computing architecture.

III. Description of Components

This system consists of three layers: Physical Layer, Cloud Layer, Web Application Layer.

A. Physical Layer

Several sensors along with a controller board (Arduino) are present in hardware layer or physical layer. Sensors used in the physical layer are given below

- **pH sensor:** The concentration of hydrogen ions present in solution is known by pH. It ranges from 0 to 14 and is used to measure acidity or alkalinity of the solution. An electrical conductivity- based sensor that measures the potential difference between two electrodes is used. The electrodes used are a glass electrode and a reference electrode probe (silver/silver chloride). 0- 14 pH with accuracy of ± 0.1 is the measurement range of this sensor.
- **Salinity sensor:** The salinity level of water is determined using the salinity sensor. To measure the level of salinity, electrical conductivity properties are used by the sensor. It is measured in terms of ppt (parts per thousand).0 to 50 ppt is the measurement range of salinity.
- **Dissolved oxygen sensor:** The amount of oxygen dissolved in an solution is measured with the help of a dissolved oxygen meter. We will be using the gravity analog dissolved oxygen sensor in this project. It has a galvanic type probe which stays available at any time and do not need polarization time. Membrane cap is filled with 0.5 mol/L NaOH solution as the filling solution. This is also known as lambda sensor which ranges from 0.00 ppm to 20.00 ppm with accuracy up to $\pm 0.2\%$.
- **Turbidity sensor:** To measure the clearness of the water an infrared diode- based turbidity sensor¹⁹ is used . NTU: Nephelometric turbidity units is measurement units of turbidity (1 NTU = 1/3 mg/L).
- **Temperature sensor:** To measure the temperature of the water, waterproof liquid temperature sensor is used. The temperature sensor offers operating range of about -10°C to $+85^{\circ}\text{C}$ and a high accuracy of ($\pm 0.5^{\circ}\text{C}$).

Controlling unit: Arduino Yun development board is the processing unit. It gathers the information from sensors, process them and send them to cloud layer. It acts as an intermediate between the sensors and the cloud layer. Arduino

Yun board is connected with all the sensors with the use of input or output pins. These pins are used for data collection. The collected data is uploaded to the cloud layer by the Yun board through the internet. After the collected data is uploaded to the cloud by Arduino Yun board, the data is made available for the application layer. 20 digital input/output pins, micro- SD card slot, built- in Wi-Fi with Ethernet support, a USB- A port, a micro USB connection and three reset buttons are present in the Arduino Yun board.

B. Cloud Layer

The sensor data is present in the cloud layer. Systems physical location and user profiles are also included in the systems data. Data storage and manipulation of resources of shrimp pond monitoring system is present in this layer. The time series data supporting all services is stored in the cloud database and presented to the users. The application layer is supported the cloud layer by providing range of requested services including:

- From sensors data, reports are generated.
- By analysing the sensors data we need to ensure standard quality level of water.
- Visualization of Real- time sensor data.
- Visualization of Historical data.
- Push notification- based messaging.
- User authentication and validation.

C. Application Layer

The monitoring services are accessed by the user which are provided by web application. All real time data can be viewed by the users through the web application. Threshold level setup for sensors, setting the notification based on threshold and so on additional services are also provided by the web application.

D. External Interface Requirements

- User Interface The user interface of this system was developed by using PHP.
- Hardware Interface Arduino Yun is used for the interaction between hardware and cloud layer which transfers the data to the web application.
- Software Interface XAMPP server is used to store the information in MySQL provided by users.

E. System Requirements Specification

1. Software Requirements

- Arduino IDE
- PHP

- Xampp Server
- MySQL
- Brackets (text editor)

2. Hardware Requirements

- pH sensor kit: pH sensor, PLC connector, variable resistor
- Salinity sensor/TDS sensor: electrode, signal connector board
- Dissolved oxygen sensor: Analog dissolved oxygen sensor, signal connector board, NaOH solution
- Turbidity sensor
- Temperature sensor: DS18B20 temperature sensor
- Arduino Uno development board
- Jumper wires
- 4.7kohms resistor
- LCD 16x2

F. System Architecture

The architecture of this system is inherited from the cloud computing and the IoT architecture that means it will contain of both web applications based on cloud and hardware.

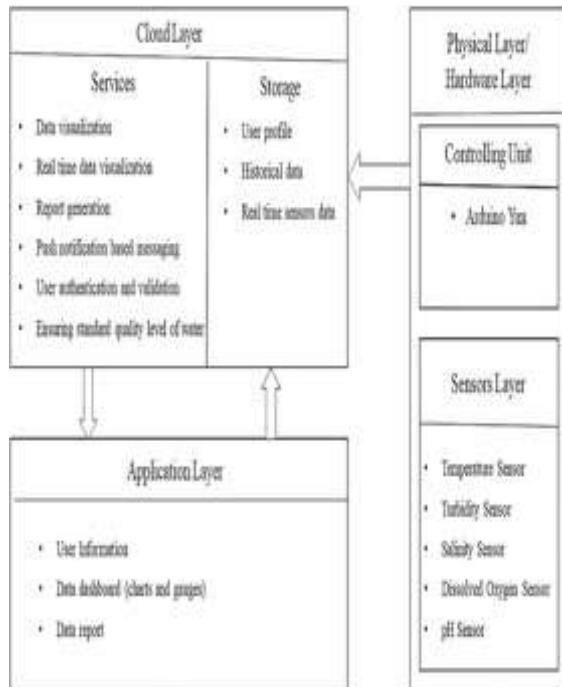


Fig 1: System Architecture

This system comprises of three layers that are

- Hardware Layer
- Cloud Layer
- Application Layer

IV. Proposed Method Working Process

Healthy production levels of shrimp can be ensured through continuous monitoring. Several sensors are used by the system for measuring the quality of water.

1. By performing the data analysis model, the measurement of quality of water is done.
2. Data collection and transfer operation is done by the physical devices.
3. Data storing is done by the cloud layer. An additional task for cloud layer is Real- time data analysis.
4. Data visualization and notification services are also provided by the cloud layer on demand.
5. The information is collected from the cloud layer to web application and is presented to the user.

The real- time data or historical data are presented by using various tables in the web application.

V. Results

The screenshots of the web application are shown in Figures 2-9. The data was collected from the cloud database. Total 120 days data were collected in the testing phase.

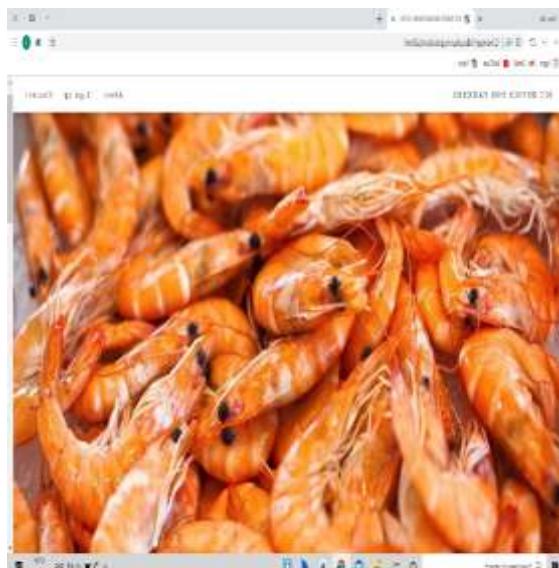


Fig 2: Main page



Fig 3: About page

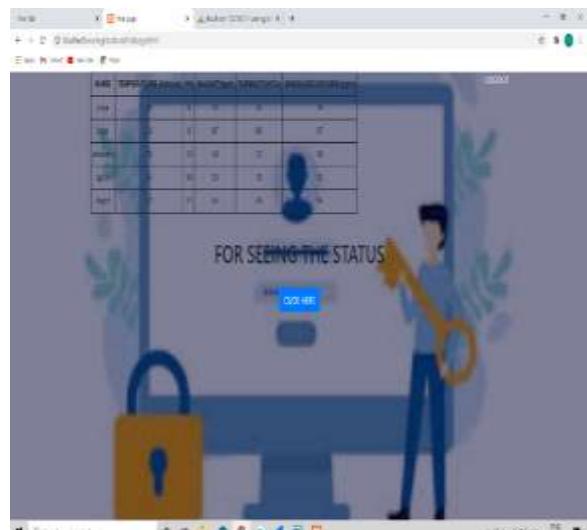


Fig 6: Information page

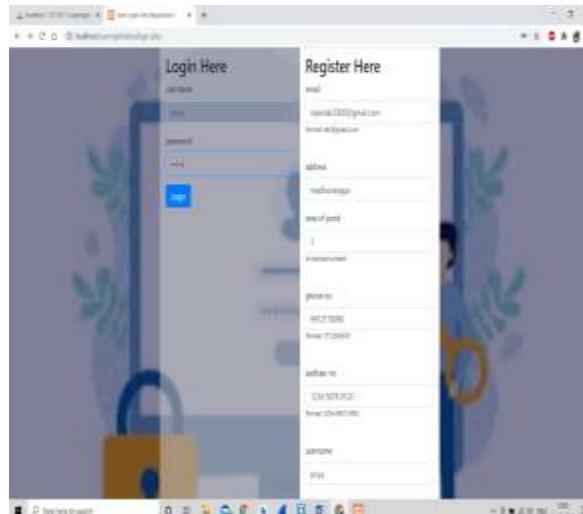


Fig 4: Registration and login page



Fig 7: Status page

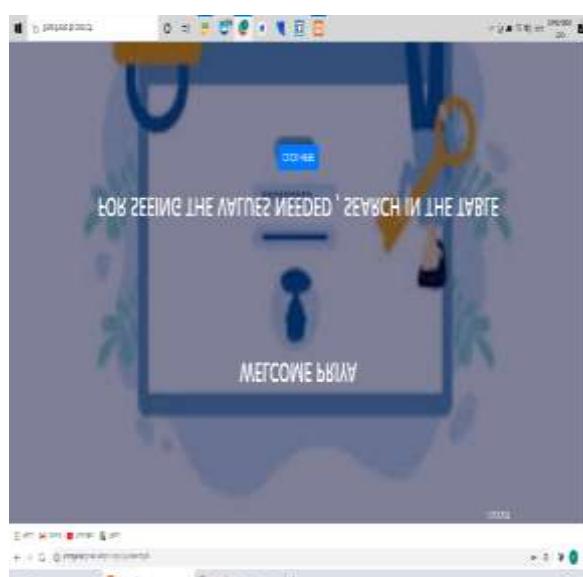


Fig 5: Home page

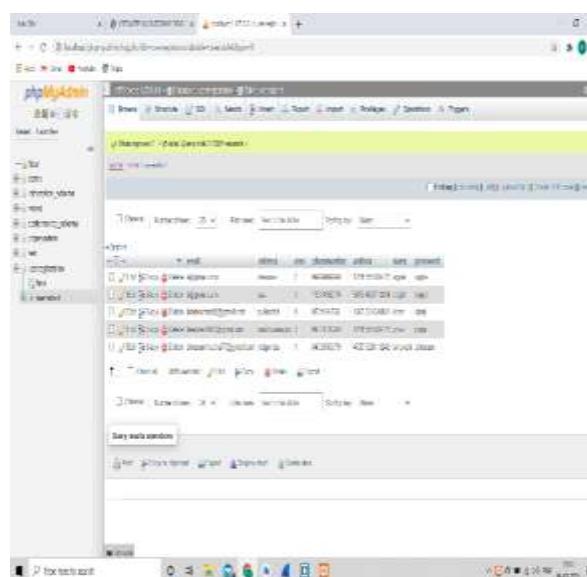


Fig 8: Database page

VI. Conclusion

Our proposition is giving the following advantages to the shrimp farming process which are reduction in shrimp mortality rate, giving water score data to user which will prevent the diseases in a way and improve production. Secondly, the implementation costs of this system is minimized due to IoT technology. Thus, for the shrimp farmers it is a feasible solution.

Based on observed values, after a year or so we can predict in which month the shrimp farm requires extra care, in which months the shrimp quality production is best and so on. Based on these predictions we can apply a perfect timing for extra production in good months through which farmers can increase their production and the shrimp contribution to the global market will increase again.

References

- [1] Ahmed S. Bangladesh: Past and Present. APH Publishing; 2004.
- [2] Fisheries Dept BD. Fisheries report of Bangladesh. Bangladesh Fisheries Department Report; 2016.
- [3] Yasmin F, Hossain M, Islam MS, Rashid MHA. Economics of fresh water prawn farming in southwest region of Bangladesh. Progress Agri. 2010; 21(1-2): 223- 231.
- [4] Ahmed ACA. Prospects, importance, problems and impacts of shrimp cultivation in Bangladesh: a literature review; 2010.
- [5] Hossain M, Shahadat DNG. GIS-based multi-criteria evaluation to land suitability modelling for giant prawn (*Macrobrachium rosenbergii*) farming in Companigonj Upazila of Noakhali, Bangladesh. Comput Electr Agric. 2010; **70**(1): 172- 186.
- [6] Zainuddin Z, Idris R, Azis A. Water Quality Monitoring System for Vannamiae Shrimp Cultivation Based on Wireless Sensor Network in Taipa, Mappakasunggu District. Takalar: Atlantis Press; 2019.
- [7] Ismail W, Shinohara N, Nameh SMIS, et al. Development of Smart Aquaculture Quality Monitoring (AQM) System with Internet of Things (IoT). Malaysia: IEEE; 2019.

Enhancing Zero-Day Attacks Detection Rate Using Machine Learning – A Survey

K. Swathi

CSE Department

CVR College of Engineering, Hyderabad-501510,

India

swathireddykathi@gmail.com

G. Narsimha

CSE Department

CVR College of Engineering,

Hyderabad-501510, India

narsimha06@gmail.com

Abstract - The vulnerabilities of many networked applications can be found by highly-skilled attackers. As the vulnerability of software or application always remains unchanged, there is a significant increase in the danger of data violations. Hackers can access and steal sensitive data through the use of such vulnerabilities (called zero-day). Because no signature information is known in nil attacks, detecting zero-day attacks with traditional defenses is difficult. Information about the signature. As a result, in order to detect zero-day attacks and assess the severity of the zero-day vulnerability, a new security solution is required. In this paper we discuss the work done on the extraction of signature attacks by zero-days and the solutions provided by different authors.

Keywords: Zero-day vulnerability, exploit, zero-day attack, attack signatures, Machine Learning.

I. Introduction

In order to reach confidentiality, integrity and availability cyber security is a range of processes and techniques that help to protect connected Internet Systems, such as resources, networks, software programmes, and data. The surface of the attack, which results in attacks, as the number of internet systems grows, so does the number of people using them.

Traditional network security monitoring requires static control of security devices at specific borders and nodes in accordance with pre-defined rules, such as firewalls and intrusion detection systems (IDSs) (IPSs). In order to avoid security measures, attackers become more sophisticated, developing zero-day exploits and malware. This allows them to operate for longer periods of time without being detected. Zero-day exploits are attacks that have never been seen before, but are variations of known attacks. Protection measures are taken. The security and external threats posed by people or entities within an organization who abuse their authorized access to insider threats are also important. The multitude of data generated by interactions between machine by machine and human by machine include applications, servers, intelligent devices, and other cyber resource capabilities [1].

At the time of the attack, it is especially difficult to identify and defend the vulnerability that attackers target to engineers who write the code so zero-day exploits. Software vulnerabilities are defects in programme design, software or operating system design, which allow you to hack into a device or network. When vulnerability in the software is identified, developers rush to fix the issue through a software update called a patch that closes the chances window. The Unidentified The "zero day" attacks that take advantage of vulnerabilities are because the developers had zero days to solve the problem. Zero-day is a vulnerability to the software or application that has not yet been patched or unknown by the seller. Find and take advantage of zero-day vulnerabilities The success rate of attacks is rising for cyber criminals. With hours, weeks, or months of hard work Attackers work on code lines to detect weaknesses or flaws. To plan the attack, the identified failure is used. Attackers will try to break the network, which allows them to execute the code secretly. This is how a zero-day attack is broken by a network.

Traditional algorithms detect flaws by signing, but zero-day signature information is unknown. As a result, detecting zero-day attacks with traditional defenses is extremely difficult. For months or even years, the vulnerability of the highly skilled attackers may remain unknown to the public. A typical zero-day attack could last up to 310 days, depending on the Fire Eye. It is obvious that it is a difficult task to deal with zero-day [2].

This time line typically follows the vulnerability window for viruses, Trojans, etc.

- The developer creates an unknown vulnerability software product.
- The vulnerability hacker will be detected before the developer.
- The hacker develops an operation while the developer is not aware of the vulnerability.
- The developer will begin to develop a fix after becoming conscious of the vulnerability.

As attackers do not report when the vulnerability has first been detected, it can be difficult to measure the vulnerability length. If the vulnerability is exploited vendor may not even know

when it is fixed, so the vulnerability cannot be recorded as a zero-day attack. For example, Microsoft confirmed that some of the versions released in 2001, declared in 2008, were vulnerable in the Internet Explorer. The first time an attacker has found the vulnerability, but in this case up to seven years could have taken the vulnerability window[3]. It's not known.

In 2016 Adobe Flash Player and Microsoft Windows were attacked with zero-day flaw (CVE-2016-4117).

The ability to keep your programmes, operating systems, and drivers up to date can prevent zero-day attacks. The delay in updating the software can threaten vulnerabilities that have been identified and fixed by developers. No matter how often you update your software to protect it against known threats, new and unknown threats will always arise. And zero-day attacks cannot be totally prevented. Instead, concentrate on remaining as safe as possible when a cyber-attack takes place. It's so important that you use a comprehensive cyber security tool — it gives you the best chance to detect and remove threats before they compromise your safety. In addition to using state of the art heuristic detection methods, AVG AntiVirus Free not only blocks and eliminates even the unknown. As new threats are identified, AVG also automatically updates. You will comfortably and confidently browse with AVG Anti-Virus FREE knowing that even the very latest threats are always fully safeguarded for your devices [4].

II. Literature Review

Yehuda Afek et al[5] The system has been developed to extract the necessary attack signatures using string-hitter algorithm. In linear time, the algorithm passes across the input. This solution is a package filtering method based on content that has good real-life performance and a mean 98% recall rate and average 98% accuracy rate. The length of the signature differs. The traffic of the attack is not known as malicious before. For this system, the space required is proportional to no heavy hitters. But we cannot identify attack signature groups and signature variability, e.g. signature may include regular expressions, do not care.

Xiaoyan Sun et al[6] The ZePro prototype system was demonstrated as a probabilistic approach to detecting zero-day attack paths. A graph is essentially a zero-day attack path. To detect a null day attack, all system calls are examined, and a dependency graph is created as a super graph for an object instance graph. In the super graph, ZePro is building a Bayesian network to extract a zero-day attack path. The Bayesian network estimates the probability that object instances are infected by

intrusion evidence. When high probability instances are connected by dependency relations, they form the zero-day attack path.

However, if the time of an attack exceeds the time of analysis, the instance graphs built may not record the entire path of zero day attacks, if some attack activities pass system call. The attack paths cannot be followed. In this case, only parts of the paths can be disclosed.

Agathe Blaisea et al[7] Proposed technique called split-and-fusion, which means that the detecting process is divided into several network segments, with distributed abnormalities only retained. (ii) Surveillance at the port level using a straightforward but effective detection algorithm based on a modified Z-Score measurement. You can plan on using an algorithm controller and multiple switches in an SDN environment for further work. Through patches of the appropriate services or network programming, for instance, the identified attack may be mitigated.

We could however detect that there wasn't a single source (mAWI-dataset), with attack and traffic in the background (the UCSD dataset).

Ruming Tang [8] Proposed unattended ZeroWall approach to efficiently detect zero-day Web attacks, which works together with a pipeline existing WAF. Historical web requests are considered benign, permitted by the current WAF based on signatures and ZeroWall uses an auto-translation machine for the trapping of syntax and semantic patterns of benign requests via recurring neural network encoders. In real time, the request for the attack for a zero-day attack that the WAF does not detect cannot be returned from the machine to its initial request and is therefore declared an attack that has not been fully grasped by an automatic translation machine. The Zero Wall detects true zero-day attacks in real world web requests which the existing wafers do not detect, reaching high F1 levels above 0.98.

Umesh Kumar Singh [9] Suggest a framework that constitutes an integrated (possibility-based) approach to zero-day attacks detection and prioritizing. Three layered architecture Framework 1.zero day detection something, 2. Attack ranks something, 3. The proposed framework uses a probabilistic approach to identify a zero-day attack route and evaluates the severity of the discovered zero-day vulnerability. It is a hybrid detection technology that detects previously undetected network failures.

Mahmood Yousefi-AZAR [10] proposed a malware detection system called Malytics, and it

does not have a specific tool and operating system dependent. It removes static characteristics from any binary file to distinguish between benign and malware. Two phases of Malytics are: extraction of features, measurement of similarity and classification. These three stages are performed by a neural network with two layers hidden and an output layer. Malytics F1 score in Android dex files is 97.21 percent and Windows PE files are 99.45 percent in applied data sets respectively.

Malytics limitation is the quantity of memory needed. The model must store all input samples as a memory batch and also a significant amount of memory is required to obtain output layer weights, of course, but only for large data. In the test phase, the layer of the kernel also has to maintain all the exercises so the memory problem is brought to light and the test process also depends directly on the training set. Malytics has a binary file in one vector and may not work with binary files that have malicious codes partially infected.

Lingyu Wang [11] K-zero day safety is a novel security method for assessing network security in the face of potential zero-day attacks. This has turned unknown vulnerabilities' unsatisfactory capability into a widely recognized barrier to safety measurement opportunity. Despite the fact that the computational problem is insoluble in general, it has demonstrated that practical security issues can be formulated and solved in polynomial time.

Huthifh Al-Rushdan[12] Within a zero-day attack on Software-defined networks, the solution proposed to protect the two parts identifies and block malware (SDNs). For the protection of client PCs, custom python code residing on the controller is used. Second, the use of UNIX-based sandbox prevents attacks on the SDN controller if the additional detection rules traffic is monitoring.

You can investigate the effects of malware size, RAM, and processor speed in future research.

III. Problem Statement

Traditional methodologies are no longer effective in protecting systems from new cyber security threats such as advanced persistent threats or zero-day attacks. On previously known malware, signature-based malware detectors can be effective. Most algorithms have limited detection and highly computational complexity of unknown threats. Traditional algorithms have not been able to detect polymorphic malware with the ability to change its symbols and new malware that has not yet been signed for. The accuracy of heuristic detectors, in turn, is not always enough to detect attacks adequately, resulting in numerous false positive and

false negatives. Thus a high spread rate of polymorphic viruses dictates the need for new detection techniques.

IV. Machine Learning for Cyber Security

The effect on real-world applications was machine learning. Cyber Space Attacks traditional machinelearning programmes:

Four main steps are taken by an ML solution:

1. Extract features;
2. Choose a suitable MI algorithm;
3. Train a model and then use different algorithms and set parameters for the most efficient model;
4. using the trained model classify or forecast unknown data [14].

Although null-day attacks are difficult to distinguish, many strategies emerge to show:

Statistics-based detection: generates a base for reliable system behaviour and uses the machine to learn to collect data from exploits already discovered. Signature-based detection: during threat scanning Signature-based detection uses existing malware databases as a reference and their behaviour. Signatures can be used for detecting vulnerabilities or attacks previously unknown.

Behavior-based detection: malware can be identified based on its interactions with the target system behaviour. In order to predict malicious attack, the solution analyses its interactions with existing software.

Hybrid detection: This method combines the above three techniques in order to benefit from their strengths and reduce their deficiencies [13].

Network intrusion detection systems (NIDS) Develop signature-based systems into systems based on anomalies that detect defects in a behaviour profile.

A. Support Vector Machines

SVM separates labeled samples with a hyper-plane, while maximizing the "boundary" from the hyper-plane to the classes. In SVM, data is typically mapped to a larger space separated by excessively wide planes. The kernel trick allows us to work in a larger space without sacrificing performance. The verification of kernel trick details can be carried out by using Lagrange multipliers. This effort is worthwhile, however, as the key to

understanding SVMs is the kernel trick [14]. [15 to 17] [15 to 17]. [19].

The mapping vectors on the side of the hyper plane space are classified into one class, and on the other side of the plane are mapped into the other class. For non-linear data points, the SVM uses kernel functions for mapping data points to larger dimension spaces that can be separated from each other. [19].

B. Decision Tree

The structure of a decision book is a tree, a test means an inner node on one object, and a trial output on each branch is a category on each node. The decision tree is a predictive model. The decision tree is the mapping of object and object values. Each node is an object, with each divergence track representing an attribute value, each leaf node representing the object's value, and the root node path to a leaf node representing that object. The decision tree has only one output so that if we want to achieve a complex output, we can set up an independent choice tree for handling different outputs. ID3, C4.5 and CART [19] are commonly used decision tree models. The drawing back to a decision tree means that it is usually not desirable in a learning algorithm to fit the training data.

C. Random Forest Algorithm

The Random Forest is a group-based approach mainly based on the decision-tab concept. In the decision tree the gain of information can be calculated as the parent node entropy below average weighted entropy. The gain of information can be measured for each feature when making a decision-tab and selecting features greedily on the basis of this measure. This means that the highest gain characteristics are closest to the root. [14] [14] [14] [19 to 23]. [19 to 23].

Random forests are average of several deep policy areas trained in the same training set and in different parts to reduce variations so as not to adapt the training sets. The process flow is as follows: The system that passes through each tree is given a new input. For category variables, the result can be a weighted average, an average of all the reached leaf nodes, or a voting majority. Unbalanced or missing data can be handled by the random forest and runtimes quite quickly. They cannot, however, predict beyond the training data if used for regression. They can also fit data sets that are particularly noisy. [24]. The estimate of multi-tree random range is relatively more appropriate for reducing distortion or over fitting, without affecting the characteristic variance [25].

V. Conclusion

One solution to this problem is relying on heuristic analyses combined with methods of machine learning that offer a high detection efficiency. Therefore taking the accuracy and leniency of using the Random Forest algorithm for future implementation at once with multiple datasets and used to characterize the large quantity of datasets we choose. It can be a state in which threats can automatically be detected and information can be transmitted immediately to the required department. The main objective of the proposal is to identify previously unknown and unseen cyber-attacks and can improve cyber detection reliability.

VI. Future Work

In future, the level of safety that will be very difficult for hackers to interfere can be achieved. The existing attack logs can be used by a good ML system and the type of future attacks can thus be predicted and avoided. In DL, the features are automatically selected instead of manually, and DL is trying to obtain more detailed data functions. We are therefore looking forward to profound learning algorithms, such as DBN, CNN, and recurring neural networks.

References

- [1] A Survey of Deep Learning Methods for Cyber Security by Daniel S. Berman, Anna L. Buczak *, Jeffrey S. Chavis and Cherita L. Corbett
- [2] A framework for zero-day vulnerabilities detection and prioritization by Umesh Kumar Singh, Chanchala Joshi, Dimitris Kanellopoulos.
- [3] <https://www.sciencedirect.com/topics/computer-science/vulnerability-window>, <https://sci-hub.do/https://doi.org/10.1016/B978-0-12-416689-9.00001-0>
- [4] <https://www.avg.com/en/signal/zero-day-attack#topic-3>.
- [5] Zero-Day Signature Extraction for High-Volume Attacks by Yehuda Afek, Member, IEEE, Anat Bremler-Barr , Member, IEEE, and Shir Landau Feibish , Member, IEEE.
- [6] Using Bayesian Networks for Probabilistic Identification of Zero-day Attack Paths Xiaoyan Sun, Jun Dai, Peng Liu, Anoop Singhal and John Yen.
- [7] Detection of zero-day attacks: an unsupervised port-based approach by Agathe Blaisea,b, Mathieu Boueta, Vania Conana, Stefano Seccic.
- [8] ZeroWall: Detecting Zero-Day Web Attacks through Encoder-Decoder Recurrent Neural Networks, Ruming Tang†‡, Zheng Yang]‡, Zeyan Li†‡, Weibin Meng†‡, Haixin Wang§, Qi Li]‡, Yongqian Sun¶, Dan Pei*†‡, Tao Weik, Yanfei Xu£ and Yan Liu£.
- [9] A framework for zero-day vulnerabilities detection and prioritization by Umesh Kumar Singh a ,Chanchala Joshi b , *, Dimitris Kanellopoulos c.

- [10] Malytics: A Malware Detection Scheme MAHMOOD YOUSEFI-AZAR^{1,3}, LEN HAMEY¹, VIJAY VARADHARAJAN², SHIPING CHEN³.
- [11] k-Zero Day Safety: Measuring the Security Risk of Networks against Unknown Attacks, Lingyu Wang¹, Sushil Jajodia², Anoop Singhal³, and Steven Noel².
- [12] Zero-Day Attack Detection and Prevention in Software-Defined Networks Huthifh Al-Rushdan¹ , Mohammad Shurman² , Sharhabeel H. Alnabelsi³ , Qutaibah Althebyan⁴.
- [13] <https://www.jigsawacademy.com/blogs/cyber-security/zero-day-attack/>
- [14] Cyber security meets artificial intelligence: a survey by Jian-hua LI.
- [15] A Survey of Machine Learning Algorithms and Their Application in Information Security by Mark Stamp.
- [16] Cristianini N, Shawe-Taylor J (2000) An introduction to support vector machines and other Kernel-based learning methods. Cambridge University Press, Cambridge.
- [17] Law M (2011) A simple introduction to support vector machines. http://www.cise.ufl.edu/class/cis4930sp11dtm/notes/intro_svm_new.pdf
- [18] OpenCV: introduction to support vector machines. http://docs.opencv.org/doc/tutorials/ml/introduction_to_svm/introduction_to_svm.html
- [19] BerwickR(2003)An idiots guide to support vector machines(SVMs).<http://www.svms.org/tutorials/Berwick2003.pdf>
- [20] Machine Learning and Deep Learning Methods for Cybersecurity by Yang Xin^{1,3}, Lingshuang Kong², Zhi Liu^{2,3}, (IEEE member), Yuling Chen³, Yanmiao Li¹, Hongliang Zhu¹, Mingcheng Gao¹, Haixia Hou¹, Chunhua Wang⁴.
- [21] Chen E (2011) How does randomization in a random forest work? <https://www.quora.com/How-does-randomization-in-a-random-forest-work> .
- [22] LiawA,WienerM(2011)Classificationandregressionby randomforest.RNews2(3):18–22
- [23] LinY,JeonY(2002)Randomforestsandadaptive nearestn eighbors,TechnicalReport1055, Department of statistics, University of Wisconsin. <https://www.stat.wisc.edu/sites/default/files/tr1055.pdf>
- [24] Breiman L, Cutler A (2001) Randomforests™,https://www.stat.berkeley.edu/~breiman/RandomForests/cc_home.html
- [25] Anomaly detection in medical wireless sensor networks using machine learning algorithms by Girik Pachauria*, Sandeep Sharma b.

A Survey on Privacy-Applicable Deep Learning Schemes in Big Data

A.Thatikonda Somashekhar

Department of Computer Science and
Engineering , Osmania University,
Hyderabad-500007, India

B.B Srinaiah

Department of Computer Science and
Engineering , Osmania University,
Hyderabad-500007, India

Abstract: Big data analytics is a burgeoning research field of computer science and various other industries worldwide. It has had much success in a variety of different applications. On the other hand, deep learning algorithms derive precise explanations automatically from a large volume of unsupervised data. These algorithms are primarily triggered by the field of artificial intelligence (AI), which aims to mimic the human brain's knowledge to recognize, investigate, research, and make decisions, particularly in the case of too complex problems. This paper gives a quick overview of the most recent research on deep learning for big data analysis that is privacy-preserving. Deep learning is a machine learning technique that relies on learning explanations. Deep understanding typically necessitates hierarchical representations and uses either supervised or unsupervised approaches to classify deep architectures. When we apply Deep Learning to Big Data, we will uncover previously unseen and useful trends. Also, we will analyze and address various Deep learning algorithms in machine learning.

Index Terms: Deep Learning, Big Data, Machine Learning, Feature Selection, Feature Extraction

I. Introduction

Deep Learning algorithms are a promising avenue of investigation into the automatic extraction of secret data descriptions (features) at high abstraction levels.

- A. Thatikonda Somashekhar is pursuing his Doctoral degree in Computer Science & Engineering at Osmania University Hyderabad, India.
- B. B Srinaiah is pursuing his Doctoral degree in Computer Science & Engineering at Osmania University Hyderabad, India (e-mail: bsrinugoud@gmail.com).

Higher level (more abstract) gatherings are defined in terms of lower-level (less abstract) characteristics, resulting in a layered, hierarchical structure for learning and understanding data. Artificial intelligence triggers the Deep Learning technique's hierarchical learning structure based on the in-depth, layered learning approach used by the primary sensorial areas of the human brain's

neocortex, which automatically extracts features and distractions from the underlying data. Deep Learning algorithms are extremely useful for determining large volumes of unsupervised data, and they usually learn data descriptions in a greedy layer-wise manner. Experiments have shown that data descriptions gathered by accumulating nonlinear feature extractors (as in Deep Learning) yield better machine learning results, such as advanced classification modeling, the high quality of individuals generated by generative probabilistic patterns, and the invariant feature of data representations. Deep Learning extracts have shown outstanding results in natural language processing, speech recognition, and computer vision, among other machine learning applications. The section "Deep learning in data mining and machine learning" provides a more detailed overview of Deep Learning. Big data refers to a wide variety of issues and methods used in applications that capture and retain large volumes of raw data to analyze a specific location. Modern data-intensive technology and increased computing resources and data storage have all aided significant data science advancement. [1].

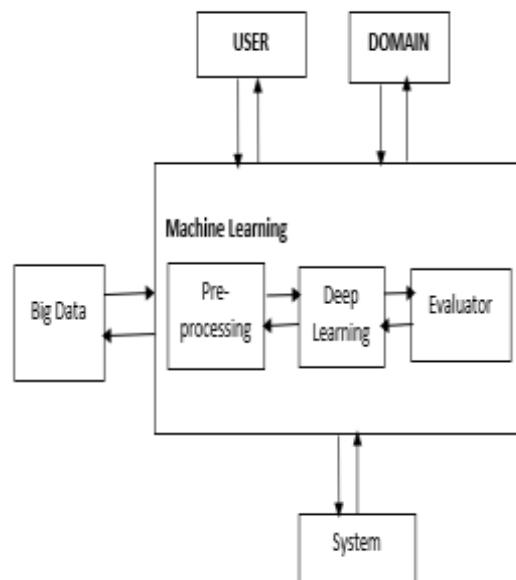


Fig 1: Architecture of deep learning using machine learning and big data

Big Data Language can handle vast amounts of data and has analytical capabilities to address the limitations of modern data processing techniques [2]. In today's digital world, the increased use of sensors,

the Internet, heavy machinery, and other technologies in a percentage of flights has resulted in an accelerated increase in data. Large data properties, such as speed and scale, have complicated data processing in computer systems. In the typical days of analyzing this variety of data, data processing frustrations, storage strategies, and approaches for analysis were all used. A distributed architectural file system manages huge data storage to address these challenges.

Text, icons, photographs, and videos in their entirety. This form of data is only going to get bigger, so it's important to organize it. If big data is obtained, it must be put to logical use or waste time, effort, and storage. Notification is the process of recording or collecting large amounts of data. Since it is a data area, big data can be used effectively. Data organization isn't enough; you really need to figure out what you can do about it. To extract necessary information from big data, ideal computing capacity, analytical abilities, and skills are required. For example, in most steps of big data problems, we can use Deep Learning, a method for understanding top abstract knowledge. However, it is preferable to require large volumes of data. We need to identify abstract trends if we want to be more effective in this competitive environment. The more style you have, the more successful you will be. In this regard, we must understand how to apply deep learning to big data and how to use it, which is the aim of this paper.

II. Literature Survey

Deep learning in big data and machine learning

Automating the extraction of representations (considerations) from data is the law for deep learning calculations. To separate complex representations, deep learning characters use a harsh measure of unsupervised data. These estimates are motivated, in a sense, by the field of erroneous information, which aims to simulate the human brain's ability to observe, interpret, learn, and choose, especially when dealing with a complicated issue. Deep learning tests that aim to imitate learning processes at various levels of the human brain have been guided by alignment with these stunning challenges. Models for removing absorptive knowledge from complex structures and assemblies in the data set, such as decision trees, support vector machines, and case-based logic, can be short in light of shallow learning schemes. On the other hand, deep learning structures can be integrated in a non-contiguous and general way, resulting in the development of diagrams and educational connections with former data neighbors [3].

A. Feature Selection

Lin Yao et al. [4] The selection of features is intended to eliminate redundant information and increase classification accuracy. This is a challenging issue, particularly when dealing with unbalanced data. Traditional feature selection approaches disregard the issue of class imbalance, skewing particular features toward the majority category while ignoring important minority characteristics. We recommend using the F scale instead of accuracy as an improvement objective in the feature selection algorithm because of the F measurement feature in the classification of unbalanced data. This article introduces a new method for selecting an SSVM-FS function based on the machine class of structural support carriers for optimal F measurement. The characteristics will be chosen based on the SSVM weight vector, which considers the imbalance problem in separation. As a result, we created an integrated property classification system that incorporates SSVM weight vectors and symmetric uncertainty. We reduce the properties to an acceptable size using the integrated score and then use the harmony quest to find the best set of properties to predict the target group's name. The suggested method's subset of features may reflect both the majority and minority categories, and they are less common. Experiments on six sets of high-dimensional unbalanced microarray data show that this approach solves unstable classification more effectively.

Xiaojun Chen et al. [5] A For weight space characteristics and high-dimensional data collection characteristics, a new technique has been proposed. According to their standard features, high-dimensional data is divided into groups of unique properties. They suggested two types of weights to calculate the effect of different categories of properties and special characteristics in each category at the same time, and they started working on a better-optimized design to explain the optimization process. To compile and optimize the optimization design, the FG-k-means algorithm was proposed.

Jianping Hua et al. [6] Using synthetic and real-life data with thousands of functions, we investigated some main feature selection techniques. Your survey aims to examine ranking output using a feature selection process that trains many features with limited sampling. They look at various approaches and confirm that some features are close to those found in real-life exams and that the association between them meets real-life instructions. Selecting properties detect patterns in activities related to particular system configurations, including sample size and the amount of heterogeneous and heterogeneous markers using this method. They also recommend that if a feature selection method is required in high-dimensional settings, the process'

output must be differentiated in the specific configuration.

Carine A et al. [7] The Impact of Assessment Trends and Similarities on Feature Selection Methodology (FS). The main goal of this survey is to determine the significance of these parameters in the FS system under consideration. For these two important parameters, this approach will be tested using eight different configurations. Many correlation measures will be used as assessment criteria, and distance measurements will be used as similarity measures.. An experimental analysis will also be conducted to examine the impact of these parameters, in which various arrangements will be tested to decide the best arrangement. Following that, the composition's best outcome will be compared to extraction methods and current property selections that have been applied to different classification problems. The findings presented in this document show that in most situations, the suggested system with the best configuration outperforms the existing arrangements..

Chen et al. [8] Provide Marginalized denoising autoencoders(MDA), MDA is measured effectively to obtain high-resolution data and graphics faster than smartphones. Its method highlights the noise in MDA training and thus eliminates the need for incremental deviations or other optimization algorithms to learn the parameters. There are secret nodes in the MDA module's layers that can be found and solved quickly. MDA also has only two free parameters, which govern the amount of noise and the number of stacks, making the model selection process much more comfortable.

B. Feature Extraction

Liying Zhan et.al.[9] One of the most challenging tasks in the field of knowledge extraction is feature extraction. The study of event extraction technology has significant theoretical implications as well as practical utility. This paper performs a survey of event extraction technologies, explains event extraction tasks and definitions, analyses, compares, and disseminates practical explanations in different fields. Then compare-contrast, and summarise the three primary methods for extracting the occurrence. These strategies each have their own set of benefits and drawbacks. The rules and template-based practices are more established, the statistical machine-based approach is the most common, and the deep-based process is the way to go in the future. At the same time, this paper summarises current problems and potential research developments in event extraction technology and the state of research and main event extraction techniques.

Hasan Dağ et.al [10] Deep learning is a machine learning subfield, and deep neural

architectures can automatically extract high-level features without engineering from natural features, unlike traditional machine learning algorithms. This article proposes a method that combines the extraction layers of convolutional neural network features with conventional machine learning algorithms, such as support vector machine, gradient increase machines, and random forests. All the proposed hybrid models and machine learning algorithms listed above are trained in three different sets of data: MNIST, Fashion-MNIST, and CIFAR-10.. The results show that when trained on raw pixel values, the proposed hybrid models outperform traditional models. This study uses the ability to extract features from deep neural network architectures to allow conventional machine learning algorithms for classification, and this learning transfer methodology inspires us.

The results show that when trained on raw pixel values, the proposed hybrid models outperform traditional models. This study uses the ability to extract features from deep neural network architectures to allow conventional machine learning algorithms for classification, and this learning transfer methodology inspires us.

Wang et.al [11] This document introduces a new tool for extracting the vibration characteristics of rotating machines to build a tool to identify different construction fluctuations. A spectrum analyzer, a signal processing circuit, and a computer make up the system. This structure offers a low-cost method of tracking and evaluating machine conditions. The study results show that training data from an acoustic spectrum analyzer can be used effectively with KNN and SVM methods to create accurate machine learning models with an accuracy of 95.8% and 97.2 percent, respectively.

Lars Hertel et al. [12] When intraclass contrast was strong, CNN-based features seemed to work best, while LBP variables produced better results for the reduced intraclass decrease. Hertel et al. made a similar discovery. They saw a small change in datasets like MNIST, CIFAR-10, and CIFAR-100 using a non-manual framework.

III.Various Deep Learning Techniques

Deep Learning (DL) techniques, especially image classification, have recently become very popular in the experimental community. These technologies will automatically learn features from non-labeled samples. The effective approaches in DL are Deep Belief Networks (DBNs), Autoencoders (AEs), Convolutional Neural Networks (CNNs), and Recurrent Neural Networks (RNNs). CNNs and RNNs have a network-wide supervised practise. DBNs and AEs, on the other hand, train one layer at a

time in an unsupervised manner, reducing the need to manage a large number of labeled samples.

Deep Belief Networks (DBNs)

Deep Belief Network is a deep learning algorithm. It's a good way to solve problems with deep-layer neural networks, such as slowness and over-adaptation in learning. DBNs are deep neural networks that are made up of several layers of a graphic model with guided and undirected edges. DBNs are a hybrid of unsupervised and straightforward systems, such as Restricted Boltzmann Machines (RBMs) or Autoencoders (AEs), in which each subnet's secret layer serves as the visible layer of the next network. It is made up of several layers of secret units, each of which is linked but the units themselves are not..

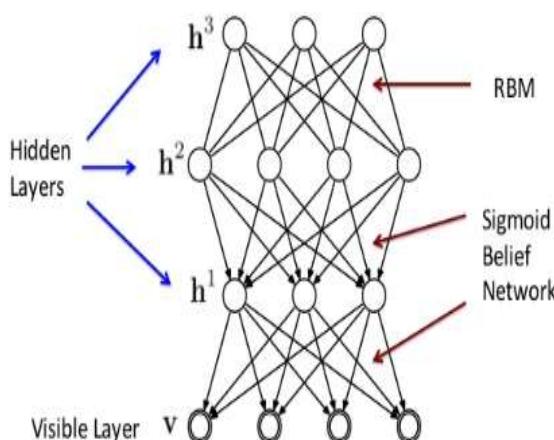


Fig 2: Deep Belief Networks model

Due to the fact that DBN is a multi-layer belief network. For the Deep belief Network, each layer is a Restricted Boltzmann Machine stacked on top of each other. The first step in DBN training is to use the Contrastive Divergence (CD) technique to learn a layer of features from the apparent units. Then, in a second secret layer, handle the activations of previously trained characteristics as visible unites and learn features. When the learning for the final hidden layer is completed, the DBN as a whole is ready.

a) Autoencoders (AEs)

Autoencoders are a form of neural network that consists of three layers: input, output, and secret. Adjust the hidden layer's weights via training to enter the input and output values as quickly as possible. As a result, the hidden layer has essential characteristics of the original signal for the unsupervised feature extraction process. Principal Component Analysis (PCA), which can minimize the data dimension, is similar to automatic codes.

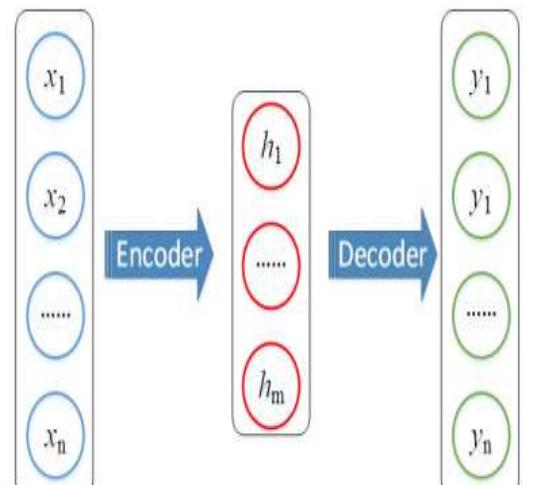


Fig 3: Autoencoders Framework

b) Convolutional Neural Networks (CNNs)

CNN networks process images across multiple layers of small groups of neurons/nuclei, each of which examines a small portion of the image and produces an output. The result may be a single class or a collection of separation options that best represent the picture. CNN networks, in general, use small convolutional cores. CNN networks, in comparison to wholly connected neural networks, have fewer parameters. The most basic CNN systems are made up of several layers. These layers may be any of the types mentioned below.:

1. **Convolutional:** The nucleus glides over all of the pixels in the input image during warp. This core/weight is a matrix with the same depth of input as the previous one. These cores can be thought of as landmark identifiers.
2. **Assembly:** The convolutional layer output is used as the input for this descending sampling layer. To minimise the number of subsequent layer parameters, reduce the cost of computation, and monitor overprocessing, the aggregation layer decreases the amount of data in the spatial domain (depth remains unchanged)..
3. **Fully Connected:** Converts a two-dimensional layer (the previous layer) to a one-dimensional layer, linking all neurons in the last layer to each neuron in the completely connected layer.

d) Recurrent Neural Networks (RNNs)

RNNs, particularly long short-term memory (LSTM), have attracted a lot of attention in the field of automatic speech recognition (ASR). Despite some success stories, RNN training remains a significant challenge, especially with limited training data. According to recent studies, a well-trained model may be used to train other children's models, with the instructor model's forecasts serving as supervision. This knowledge transfer learning is used to train simple neural networks with a complex network, allowing the final output to exceed that of normal training.

III. Conclusion

To extract better abstract information, it is now essential to connect with Big Data. Deep Learning (Hierarchical Learning), which presents higher-level data abstraction, is one suitable method for this goal. Deep Learning is a useful technique that can be applied in a Big Data environment. This paper reviewed the most recent research on Deep Learning for Big Data Analysis in terms of security and privacy. In addition, various deep learning approaches in machine learning were explained. The algorithms investigated in this paper show promise as a step forward from conventional algorithms.

References

- [1] T. Tran, S. Kiyomoto, 2017, Optimizing share size in efficient and robust secret sharing scheme for big data", 1–14.
- [2] Aisha Siddiqa, Mohsen, 2016, "A survey of big data management: taxonomy and state-of-the-Art", pp.151–166.
- [3] Dogukan Aksu, 2018, "Detecting Port Scan Attempts with Comparative Analysis of Deep Learning and Support Vector Machine Algorithms", pp.77-80.
- [4] Chunkai Zhang, Lin Yao, 2017," Feature selection for high dimensional imbalanced class data based on F-measure optimization" pp.278-283.
- [5] X. Chen, Y. Ye, X. Xu and J.Z. Huang, A feature group weighting method for subspace clustering of high-dimensional data, Pattern Recognition, 45(1),(2012), 434–446.
- [6] J. Hua, W.D, 2009, "Performance of feature-selection methods in the classification of high-dimension data", pp.409–424.
- [7] Carine A, Anne M. P. Canuto,2017, "Investigating the Impact of Similarity Metrics in an Unsupervised-Based Feature Selection Method", pp. 55-60, 2017.
- [8] Chen M, Weinberger KQ, 2012, "Marginalized denoising autoencoders for domain adaptation".
- [9] Liying Zhan; Xuping Jiang, 2019, "Survey on Event Extraction Technology in Information Extraction Research Area", pp.2121-2126.
- [10] Aykut Çayir, Hasan Dağ, 2018, "Feature Extraction Based on Deep Learning for Some Traditional Machine Learning Methods", pp. 494-497.
- [11] Jyun-Shun Liang; Kerwin Wang, 2017, "Vibration Feature Extraction Using Audio Spectrum Analyzer Based Machine Learning",pp. 381-384.
- [12] Lars Hertel, Thomas Martinetz, 2015, "Deep convolutional neural networks as generic feature extractors", pp. 1-4.

Detection of plant Disease Using Image Processing based on KNN and GLCM Algorithms.

N.S. Shivani

Department of CSE,

Chaitanya Bharathi Institute of Technology (A),
Hyderabad-500075, India
shivanisandy07@gmail.com,

M.V. Jeeva

Department of CSE,

Chaitanya Bharathi Institute of Technology (A),
Hyderabad-500075, India
jeevamaddela1@gmail.com,

Dr.R Ravinder Reddy

Department of CSE,

Chaitanya Bharathi Institute of Technology (A),
Hyderabad-500075, India
rravinderreddy_cse@cbit.ac.in

Abstract: Food is an essential human resource and the agriculture is the main source for food. Using soil, water, and other natural resources plants are grown. During this process Farmers go through many obstacles in which one of the major obstacle is plant diseases or infection. This cause's major loss for farmers. Detection of plant diseases in early stages makes it easy to decrease the loss of productivity. To overcome these kind of problems, photos of infected leaves can be made use to analyse and discover the disease in the plants. Image Refining is used to perform some operations on image and extract useful information. Plant disease detection is a technique where the picture of infected leaf is added to the process and information is extracted to detect the disease. It helps us to increase the quality of crops. In this work GLCM and KNN is implemented. K-means clustering is for the separation of colours and GLCM is used to classify based on the input images.

Keywords: Image segmentation, Plant disease detection, GLCM, K-Means, KNN.

I. Introduction

Plant infections occur usually due to infectious organisms called Pathogens. Fungi is common type of organism that causes diseases. Other bacteria, viruses and many other also cause infections. Insects, mites, pests also eat outer layer of plant leaf and for that purpose pesticides are used. Almost 85 percentage of plant diseases are caused by fungal or fungal-like organisms. Farmers try to adapt the growing practices based on local conditions like climate, plants and animals living in local, landscapes etc. Soil fertility and type of soil plays main role in farming. All farmers rely on ecosystem services.

To cultivate crops farmers need resources. Natural resources like water, land, air, nutrients and sunlight are must to grow plants. Lot of efforts are needed in case of plant cultivation. But due to some

climatic conditions or fertility of soil the plants can be infected. Detection of such infections or diseases in early stages can be beneficial and in some cases we can control its growth.

In Few rural areas farmers are unable to contact an expert or can control the growth of disease on their own. Instead plant disease detection can be helpful. The images of the leaves are analysed, then using Gray-Level Co-occurrence Matrix (GLCM) and K-Nearest neighbour (KNN) are used to detect the disease.

Image processing is done using digital cameras. Euclidean distance metric method is used K-mean clustering algorithm and clusters the image. GLCM is used in texture analysis, it uses greyscale values and constructs histogram. Picture element make an image. Each Picture elements have different intensities. These intensities simply is gray level. In GLCM grayscale values of picture are sorted in table. GLCM uses a same order matrix for calculations.

II. Literature Survey

Now a days, image processing techniques are used in various fields all around the world, such as medical field, automation, security, graphic visualization etc. here we are going talk about the plant infection in the medical field. The identification of plant infection using traditional method is replaced by image processing.

The image processing systems mainly requires the following materials such as camera, computer and necessary software. Steps involved in plant disease detection are as follows, they are image input, pre-processing of image, segmenting, draw out important features and classifying [1]. Performing picture enhancement, it increases standards and makes images more clear. Basic primary colors red, green and blue (RGB) colors combinations produce many different varieties of

colors. Hence, implementing image processing using RGB components is difficult as the range is very high. So to minimize the high range of RGB we are Converting RGB image into its equivalent gray image, it is done for easier [2]. Automated detection of plant disease using picture processing is beneficial for the farmers as it reduces large human labors and can help to detect the diseases or infection by identifying the symptoms in early stage [4]. For picture processing k-mean clustering is used for easy discovery of infection or disease and is mostly accurate. Software image processing tools are also used for detecting the disease of the plants. GLCM and KNN is used for detection of virus in the plant leaves by image processing.

More over in this paper we use Image acquisition that is performed using digital cameras. Algorithms such as K-mean clustering algorithm which uses Euclidean distance metric method and clusters the image based on the specified number of groups [3, 5]. Gray-Level Co-occurrence Matrix (GLCM) is one of the most popular methods for texture analysis. It measures the spatial distance between the pixels and produces a feature based gray level matrix for the colour image. GLCM represents the distance and angular spatial relationship of an image in a specific size. GLCM calculates how often the pixel with gray level intensity occurs. Vertically or diagonally values to adjacent pixels are labeled as 'j' and horizontally values are represented as 'i' [6, 7, 8].

The KNN approach has used by Rani Pagariya et.al,(2014) [9] to the plant diseases and plant infection detection. With enhanced technological advancements the image processing is used for the plant disease detection. The different approaches like classification techniques are used to detect the plant disease detection and provides the appropriate results. This paper mainly focused on the various diseases of cotton plants and classifies their diseases. In the Machine learning, many classification techniques are available, the following techniques are considered, such as k-means Classifier, k-Nearest Neighbor classifier, Genetic Algorithm, Probabilistic Neural Network, Support Vector Machine, PCA and neural network techniques.

This paper gives brief information for the classification of plant diseases by using following techniques those are The GLCM (gray-level co-occurrence matrices) procedure is utilized which excerpts textural features from the input image and implementation of KNN (k-nearest neighbors) algorithm for image classification, The k-mean clustering procedure is utilized for the segmentation of input images. After all those selection criteria depends upon of the input of the data and produced

classification accuracy from 70 to 75% for different inputs [10][11].

III. Methodology

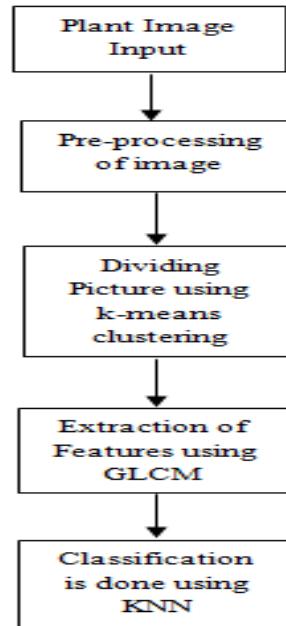


Fig 1: Methodology

a. Image Input

Taking pictures using digital camera is the first step for image acquisition.

A picture is captured using digital camera or mobile camera to use as input and analyze useful features from it.



Fig 2: Image Input [12]

b. Pre-processing of Image

Region of interest (ROI) is taken into consideration.

Pre-processing mainly deals with filtering, smoothing, enhancement, cropping etc. In this step the quality of image can be enhanced. Picture quality can be improved by smoothing the image and improving the contrast.

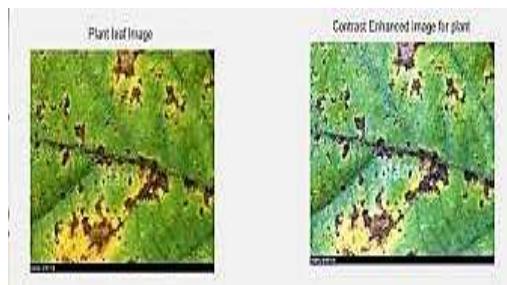


Fig 3: Image Enhancement [14]

c. Image Segmentation

As the name says, this step involves the segmentation of images i.e. the image is divided into small segments or parts for further analysis. The segmented images individually are used to extract the features of that particular region or area. K mean segmentation is applied here for the segmentation of image.

K-mean clustering – A cluster refers to a collection of data points are grouped together because of certain similarities. It is based on the closeness of pixels in the image and so it used Euclidean distance measurement.

Here the image is divided into various clusters. Data is categorized into disjoint sets. A centroid point is taken and the neighboring points that are near to the centroid are taken into consideration. Then Euclidean distance is calculated. There are also other methods that can be used to measure the distance.

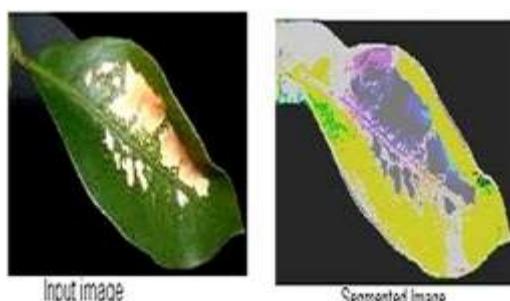


Fig 4: Image Segmentation [12]

d. Feature Extraction

The process where required features are extracted from the image is considered as Feature Extraction. Considering to the original image dimensions of Region of Interest will be smaller. Gray-Level Co-occurrence Matrix (GLCM) is used in texture analysis, it uses greyscale values and constructs histogram. Image consists of Picture elements i.e is pixels. Each pixel is composed with different gray levels.

GLCM uses same order matrix i.e square matrix where number of rows and columns are equal.



Fig 5: Feature Extraction [12]

e. Classification

Leaves are not only affected by virus, fungi etc in some cases insects also cause damage to the leaf which appears like a disease. External leaf or needle damage is caused by insects. They chew leaf from outside called as free feeding. The toxic effect of saliva results in small, circular dead spots on the leaf which appears as disease. It may be of different size and color. According to the texture of the affected area using GLCM the disease can be classified.

To classify data with only two classes Support vector Machine (SVM) is used. For more than two classes KNN can be used.

IV. Result

The Accuracy of this system identifying the disease and classifying them is 98.27% [13]. With the help of K-means clustering and GLCM the infections are known with maximum accuracy. There are different kinds of diseases in plants. Fungal disease signs are leaf rust, stem rust, sclerotinia, powdery mildew and symptoms include Anthracnose (Birds-eye spot on berries), Phytophthora(Damping of seeding), septoria brown spots(leaf spot), chlorosis (yellowing of leaves).

Table 1: Classification of Disease and Affected Area [13]

Sample No	Disease Classified	Affected Area (Percentage)
1	Anthracnose	49.88
2	Anthracnose	53.12
3	Anthracnose	66.37
4	Cercospora Leaf Spot	80.56
5	Cercospora Leaf Spot	43.25
6	Cercospora Leaf Spot	21.89
7	Bacterial Blight	30.51
8	Bacterial Blight	15.68
9	Bacterial Blight	88.76

V. Conclusion

According to this work plant disease detection using image processing is easy and efficient. It has maximum accuracy. It utilizes K-mean clustering and GLCM to analyze and detect disease. It makes easy not only for farmers but to everyone to easily detect the disease in less time. There is no need of expert, this automated system can be useful to reduce labour cost and detect disease in minimum time.

References

- [1] Pallavi.S. Marathe, "Plant Disease Detection using Digital Image Processing and GSM", International Journal of Engineering Science and Computing, April 2017, pp. 10513-15.
- [2] Vijai Singh, Varsha, A.K. Mishra, "Detection of Unhealthy Region of Plant Leaves using Image Processing and Genetic Algorithm", 205, ICACEA, India.
- [3] Gautam Kaushal, Rajni Bala, "GLCM and KNN Based Algorithm for Plant Disease Detection", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 6, Issue 7, July 2017, pp. 5845 – 5852.
- [4] Sujatha. R, Y. Sravan Kumar and Garine Uma Akhil, "Leaf Disease Detection using Image Processing", Journal of Chemical and Pharmaceutical Sciences, March 2017, pp 670 – 672
- [5] MrunalaniR. Badnakhe, Prashant R. Deshmukh, "Infected Leaf Analysis and Comparison by OTSU Threshold and K-Means Clustering, "International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 3, March 2012.
- [6] Abdolvahab Ehsanirad, Sharath Kumar Y.H, "Leaf Recognition for Plant Classification Using GLCM and PCA Methods", Oriental Journal of Computer Science & Technology, Vol. 3 (1), 2010, pp. 31-36.
- [7] Namrata K.P, Nikitha S, Saira Banu B, Wajiha Khanum, Prasanna Kulkarni, "Leaf Based Disease Detection using GLCM and SVM", International Journal of Science, Engineering and Technology, 2017.
- [8] Vijai Singh, A.K. Misra, "Detection of Plant Leaf Diseases using Image Segmentation and Soft Computing Techniques", Information Processing in Agriculture 4 (2017), pp. 41–49.
- [9] SmitaNaikwadi, NiketAmoda, "Advances in Image processing for detection of plant disease", International Journal of Application or Innovation in Engineering & Management, volume 2 issue 11, 2013.
- [10] Konstantinos P.Ferentinos, "Deep learning models for plant disease detection and diagnosis", Computers and Electronics in Agriculture, Vol. 145, 2018, pp. 311-318.
- [11] Sharada Prasanna Mohanty, David Hughes and Marcel Salathé, "Using Deep Learning for Image-Based Plant Disease Detection" Frontiers in Plant Science, Vol.7, 2016.
- [12] Vijai Singh, A.K.Misra "Detection of plant leaf diseases using image segmentation and soft computing techniques" Information Processing in Agriculture Volume 4, Issue 1, March 2017.
- [13] Dr. Sridhathan C, Dr. M. Senthil Kumar "Plant Infection Detection Using Image Processing" International journal of Modern Engineering Research ,Vol. 8 ,July 2018.
- [14] K. Elangovan, S. Nalini "Plant Disease Classification Using Image Segmentation and SVM Techniques" International Journal of Computational Intelligence Research, Volume 13, Number 7 (2017).

Music Genre Classification

A.G Naga Sujini

Department of CSE

Mahatma Gandhi Institute of Technology,
Hyderabad-500075, India
gnagasujini_cse@mgit.ac.in

Dr M Ramabai

Department of CSE

Mahatma Gandhi Institute of Technology,
Hyderabad-500075, India
mramabai_cse@mgit.ac.in3

J Sreedevi

Department of CSE

Mahatma Gandhi Institute of Technology,
Hyderabad-500075, India
jsreedevi_cse@mgit.ac.in2,

V Mounica

Department of CSE

Mahatma Gandhi Institute of Technology,
Hyderabad-500075, India
mounicavuyyuru4@gmail.com4

Abstract: Music can be categorized into different categories using genres. Our aim here is to categorize music into different genres using machine learning algorithms. The different genres have different distinguishable characteristics that can be recognized by the using machine learning by extracting features. Music has different features categorized as spectral and temporal features, which comprise of many different kinds of features which have very minute differences. Of them the features which we used are zero crossing rate, energy, spectral roll off, spectral bandwidth, chroma vector and MFCCs. These features have been selected because they are useful for our genre classification task. After extracting these features, we pass them to different machine learning classifiers to classify the genres. We used the GTZAN dataset. We genres we classified are blues, classic, country, disco, hiphop, jazz, metal, pop, reggae and rock. Now the classifiers we used are KNN, XGBoost, rbf kernelized SVM, decision trees and random forests. We compared the results obtained by these different classifiers and observed that the rbf kernelized SVM performed better than all with an accuracy of 64.67%. The XGBoost classifier performed relatively closely as that of the SVM with an accuracy of 62.33%. The decision tree classifier performed the worst with an accuracy of 44%. Since the SVM classifier performed better, we chose it for our music genre classification task.

Keywords: Music genre, Machine learning, Feature extraction, Music information retrieval.

I. Introduction

Music is a very popular source of entertainment and has become quite ubiquitous in modern life. It is a very popular medium of relaxation and is considered to be a universal language. Music has traditionally been consumed through live performances and through vinyl records, cassettes and CDs. With the advent of the digital age music has mostly been consumed digitally and electronic consumption has become the norm. Digital music is

one of the most important means of music distributed over the Internet and the digital music content is increasing Nowadays, quickly. It has become an important problem to manage and organize a large digital music database.

There are widespread highlights of music that all structures have, paying little heed to their musicality, structure, scoring or tone. One approach to order and sort out tunes depends on the class, which is distinguished by certain qualities of the music, for example, cadenced structure, consonant substance and instrumentation. Having the option to consequently group and give labels to the music present in a library, in view of classification, would be advantageous for audio streaming services, for example, Spotify and iTunes. Automatic music genre order has increased immense fame lately as there is a quick advancement of the computerized media outlet.

As a first step in the classification of genres, extraction of features from musical data will have a significant influence on the accuracy of the final classification. Music genre is a key feature of any song that can guide users into their category of choice. Many music enthusiasts create playlists based on specific genres which lead to potential applications such as recommendations for playlists and management. A classification system for the music genre is proposed in this study based on different machine learning techniques. The rationale of the study is to correctly classify these genres of a new music track given. There are many music characteristics such as the musical structure, tempo, rhythm, melody, chord, and so on that could be used to differentiate different music genres.

The data we are dealing with is music, and there are many formats for music files like mp3, mp4, aac, flac, wav, but we would be working with wav format audio files since librosa primarily deals with wav files. The dataset we will be using to train our model is the GTZAN Genre Collection dataset from MARSYAS website. The GTZAN dataset is the most used publicly available dataset in the field of A classification of the music genre. This dataset

consists of 1000 audio tracks collected from a variety of sources each 30 seconds long including personal CDs, radio, microphone recordings. These 1000 tracks are divided into 10 genres with 100 tracks each. All these tracks are in .wav format. The 10 different genres are: jazz, metal, pop, reggae, rock, hip hop, disco, classical, country, and blues.

The current models which are used for MIR systems are heavily based on extracting temporal features rather than the spectral features. They are used for content-based music searching. They can take in information regarding their systems such as matching methods, descriptions, features etc. We can distinguish two main groups of MIR systems for content-based searching, audio data search and noted music search systems. The system we are interested in building comes under the subsection for searching noted music. The current systems which we have look only at a particular paradigm for feature selection. We aim to extract both the spectral and temporal features and attributes. Of the temporal features, we extract the first 12 of them individually instead of taking their mean to get each of the representations accurately.

II. Literature Survey

“MUSICAL GENRE CLASSIFICATION USING SUPPORT VECTOR MACHINE” This paper used a multi-layered support vector machine learning model for the music genre classification problem. These SVMs were used to capture the differences between the class boundaries for different genres through the training data. The different features that were considered are beat spectrum, linear prediction coefficients, zero crossing rates, short time energy and mel cepstral coefficients. Three nonlinear support vector machines were used. This study showed that multi-layer SVMs have performed better than the traditional Euclidean distance based methods on music genre classification task [1]. **“Music Genre Classification using Machine Learning Techniques; Hareesh Bahuleyan”** In this paper two different approaches were used for the music genre classification task. The first one is using various CNN classifiers on the spectrogram of the audio signal considering it to be an image. And the second approach is by using the traditional machine learning classifiers on the time domain and frequency domain features of the audio signals. This study used logistic regression(LR), random forest(RF), support vector machine(SVM) and extreme gradient boosting(XGB), of which the XGB classifier showed better performance[3]. **“Music Genre Classification Using Machine Learning Techniques”** This paper used a neural network for the music genre classification problem and also proposed that a growing neural gas would improve the performance of the neural network. The purpose of the GNG in the

scope of this task is to reduce the complexity of the music space for the neural network by abstracting some of the more important features into model vectors associated with each genre of music [4]

“Music Genre Classification Using Frequency Domain Features” This paper utilized the spectral features in the music genre classification task. To differentiate different genres musical properties like tonality, pitch and timbre are important and for this purpose spectral features have been used. Different feature sets were formed considering the features spectral flux, spectral rolloff, spectral centroid, mel Frequency cepstral coefficients, spectral flatness measure, tonal power ratio, pitch, spectral skewness, were used. These feature sets were then trained on two different classifiers, random forests and support vector machines. This is performed on three different datasets namely GTZan, Ball Room and Uni-Dortmund. The performance was consistent irrespective of the classifier [11]. **“Automatic Music Genres Classification is using Machine Learning”** In this paper, k-nearest neighbor and support vector machine classifiers were used with and without dimensionality reduction through principal component analysis on the GTZan dataset to find a better music genre classifier. Mel frequency cepstral coefficients are the features used for this task [5]. The k-NN classifier performed better than svm for classical, rock and reggae genres, whereas svm performed better than k-NN for country hip hop and jazz genres. Overall the SVM classifier was found to be a better one between them with a better accuracy score. **“Musical Genre Classification Using Support Vector Machines and Audio Features”** This paper used a nonlinear support vector machine with different kernels applied on the different possibilities of combining various features with a k-fold cross validation. The categories of the features considered are rhythm, timbre, tonality, mel frequency cepstral coefficients (MFCC) and linear predictive coefficients (LPC), these are combined with each other with different possibilities to know which features contribute the most to the music genre classification task. These features are then passed to three different 10-fold cross validation nonlinear systems with different kernels, radial basis function (RBF), polynomial and sigmoid. Of them the polynomial kernel with the combination of MFCC, tonality and LPC features performed better with a higher accuracy than other possibilities. This study was carried out on the data mining software Weka. In the lyrics feature extraction, the chi-squared test vector and word embedding extracted by Word2vec are, respectively, used as the feature representation of the lyrics. Combining the two types of heterogeneous features selected by audio and lyrics through the classification model can improve the classification performance [12].

Seo and Huh used different classification algorithms such as random forest, DNN, and K-nearest neighbor for comparative analysis and used SVM as the best classification method [13].

Yeong-Seok Seo and Jun-Ho Huh, proposed an emotion-based automatic music classification method that can classify music with high accuracy according to commonly identified emotions for use in the development of various types of music-related emotional intelligence IoT services. The well-known circumplex model was used to identify and quantify emotions [14].

III. System Design

Architecture

The data we are dealing with is unstructured in nature. A ML model can deal with only structured data, so we need to follow the below architecture in order to apply the ML techniques. After loading the data we need to extract important features from it, which is then divided into test and train sets. We will build and train our model on the train set by applying a machine learning algorithm. After the model is built it is tested against the test set. Now when we pass a new audio (music) file to our trained model, it predicts the genre of that song.

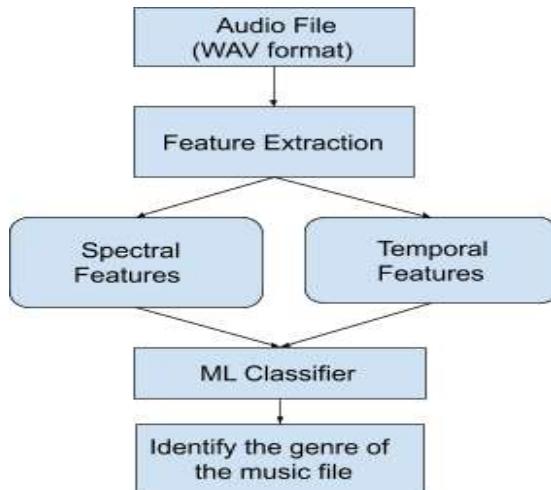


Fig 1: Architecture for music genre classification

A. Feature Extraction

Feature extraction is a dimensionality reduction process as we want to base our analytics algorithms on a relatively small number of features. The extraction of features is an important stage of the audio analysis. The sound is sizable, and thus, it is difficult to measure straightforwardly in some investigation undertaking. We in this manner necessitate changing the underlying information portrayal to a more reasonable one, by removing

sound highlights that speak to the properties of the first signals while decreasing the size of the data. We should remove the qualities of our sound sign that are generally applicable to the difficulty we are attempting to illuminate.

So we extract the following features for our task:

B. Energy

The Signal Energy relates towards the complete magnitude of that sign. For sound signals, that generally relates how noisy the Signaling is.

C. Zero Crossing Rate

The Zero-Intersection Rate (ZCR) of a sound casing is the rhythm of signal transform throughout the frame. At the end, it is nothing but the occasions A signal transforms appreciation, from positive to negative and the other way around, partitioned by the length of the frame.

D. Spectral Centroid

The spectral centroid has the crucial indication of 'gravity' of the range i.e. it demonstrates at which recurrence the vitality of a range is focused upon.

E. Spectral Bandwidth

Spectral bandwidth gauges how the range is dispersed around its centroid. It's the second central spectral moment.

F. Spectral Roll off

Spectral Roll off is distinct as the regularity underneath which an assured entitlement of the spectrum enormity distribution is strenuous (usually around 85 per cent).

G. Chroma Vector

A chroma vector (which typically encompasses all the chroma features) typically a 12-element vector indicates how much energy is present in the signal of each pitch class, {C, C #, D, D #, EF, F #, G #, A, A #, B}.

H. MFCCs

A signal's mel frequency cepstral coefficients (MFCCs) are a diminutive deposit of description (habitually regarding 10-20) that depict the overall contour of a spectral shroud in a concise manner. MFCCs are in fact a kind of cepstral signal depiction, where the regularity bands are disseminated according to the mel-scale rather than

the linearly spaced advance model building. Once we've got our features, we'll then move on to building the model. We will use the following classification techniques:

I. KNN Classifier

K-closest neighbor (KNN) characterization is one of the most essential and basic classification techniques and ought to be one of the best options for a classification study when there is nearly nothing or no earlier information about the distribution of the data. Because of its simplicity, ease of implementation and effectiveness it is an extensively used classification algorithm. It is one of the top algorithms of machine learning which has been widely applied in different fields. KNN assumes similar things are close to each other (Similar data points are near each other most of the time). KNN grasps the concept of similarity interpreted as distance between points on a graph.

J. Decision Trees

A decision tree is a decision-help contrivance which uses a tree-like graph or choice model and its potential outcomes, including outcomes of chance, asset spending, and utility. Showing a calculation which only contains restrictive control articulations is one approach.

K. Random Forest

An enormous number of individual decision trees work as a troupe, this is a random forest. Every personage tree in the random forest predicts a class and the class among the largely noteworthy choices is predicted by our replica.

L. SVM

A support vector machine (SVM) is a supervised learning representation for categorization purposes investigation of data. Every data entry is contrived as an indication in n-dimensional space (where n is the amount of description you comprise) among the value of every function being the value of an explicit coordinate. SVM aims to find the best possible decision boundary (hyper-plane) to classify the existing classes accurately and to correctly classify a new data item.

M. XGBoost

Extreme Gradient Boosting (XGBoost) is a decision tree based ensemble learning algorithm that makes use of the gradient boosting framework. So before going into XGBoost let us know what boosting is. Boosting is an all together method that converts weak learners to brawny learners by passing

the errors of the present model to the next model with different weights each until we get accurate values. Gradient boosting is exactly the same as boosting except for here This method hysterics the novel representation with novel residuals of the preceding prediction as a substitute of assigning unlike weights to the classifiers behind apiece iteration and afterwards minimizes the trouncing after accumulation of the newest prophecy. XGBoost implements this for boosting decision trees.

N. Model Testing

After building a model, we'd want to know how good our model is and ways to improve its accuracy. We'll have to look at the evaluation metrics for that. In order to find the best model that represents our data and the working of our model we go for model evaluation. Let's look at the most common method of representing various evaluation metrics, the confusion matrix.

O. Confusion Matrix

In machine learning, performance estimation is a fundamental task. The Confusion Matrix is a machine learning performance estimation model. Better the adequacy, better the performance of the model. Confusion Matrix is a recital estimate for classification problems with machine learning, where yield can be at least two classes. It is a table containing 4 distinct mixes of actual and predicted values. Confusion Matrices are extremely useful for measuring Recall, Precision, Specificity, Accuracy which are critical metrics for measuring model performance and most importantly AUC-ROC curves.

P. AUC-ROC curve

On behalf of a numeral of dissimilar entrant threshold values among 0.0 and 1.0, ROC is a plot showing the performance of a classification model. It has Two Parameters. 1. False positive rate (x-axis) 2. True positive rate (y-axis). In other words, it draws the false alarm vs. the hit rate. ROC curve is a good metric to be used when comparing various models as In general, the curves of contrasting models might be contrasting unswervingly or for dissimilar thresholds. The region beneath the value of curve (AUC) might be worn as a synopsis of the dexterity of the model.

IV. Result Analysis

The following are the results we got using different classifiers - xgboost, knn, svm, decision trees, random forests.

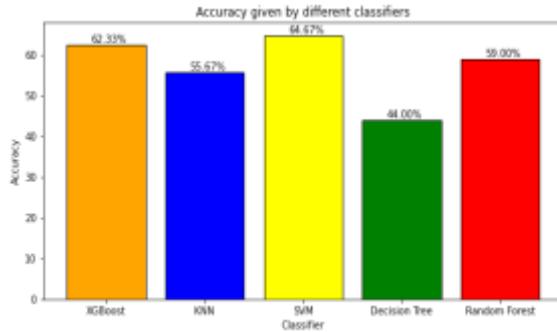


Fig 2: Accuracy of models built by different classifiers

The least accuracy was observed by the decision tree classifier with an accuracy of 44% while the accuracy given by the random forest classifier was 59%. The KNN classifier gave an accuracy of 55.67%. The XGBoost and the rbf kernelized SVM classifier performed relatively closer. XGBoost classifier's accuracy was 62.33%. The highest accuracy was observed by the rbf kernelized SVM with an accuracy of 64.67%.

Let us now look at the genre wise accuracy by different classifiers.

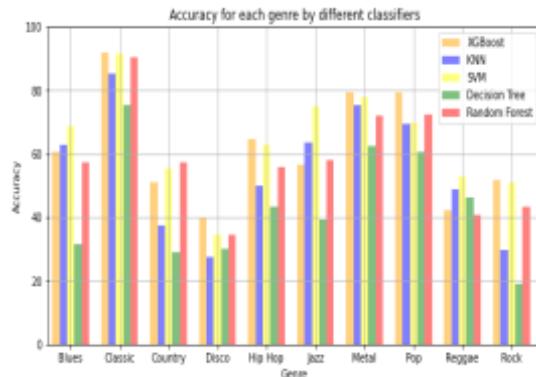


Fig 3: Performance of each model with different classifiers towards each genre

Classical genre songs were best recognized by all the classifiers with an accuracy of more than 80% whereas the disco genre songs were worst recognized by all the classifiers with an accuracy of less than 40%. The XGBoost classifier better recognized the classical, disco, hip-hop, metal, pop and rock genres than other classifiers. The rbf kernelized SVM classifier better recognized the blues, jazz, and reggae genres than other classifiers. The country genre was better recognised by the random forest classifier than the other classifiers. The XGBoost classifier and the rbf kernelized SVM classifier performed relatively closely with each other.

Since the model built with the rbf kernelized SVM algorithm gave the best accuracy (64.67%),

we'll use it for our task. The model we built will spit out a number as result; this number corresponds to which genre the audio file belongs to. The following table tells us which number corresponds to what genre:

Table 1: Output array numbers mapping with their corresponding genre

S.No	Output Array Number	Genre
1.	0	Blues
2.	1	Classical
3.	2	Country
4.	3	Disco
5.	4	Hip hop
6.	5	Jazz
7.	6	Metal
8.	7	Pop
9.	8	Reggae
10.	9	Rock

Let us try out different test cases:

1. Loading a metal song to extract the features and test for it using our model

```

x,y = librosa.load('Metallica-HighwayToHell.mp3')
temp_prestige = librosa.feature.prestige(y=y, sr=sr)
temp_centrality = librosa.feature.spectral_centrality(y=y)[0]
spectral_centroids = spectral_centroids[0]
spectral_bandwidth = librosa.feature.spectral_bandwidth(y=y)[0]
spectral_rolloff = librosa.feature.spectral_rolloff(y=y)[0]
spectral_polyrhythm = librosa.feature.spectral_polyrhythm(n_poly=3)
spectral_skewness = librosa.feature.spectral_skewness(n_fft=n_fft)
chromagram = librosa.feature.chroma_stft(y=y, sr=sr)
chroma_mean = [np.mean(x) for x in chromagram[::12]]
chroma_std = np.std(chromagram[::12])
mfcc_mean = np.mean(mfccs[0])
mfcc_std = np.std(mfccs[0])
Features = str(temp_prestige) + ',' + str(spectral_centrality) + ',' + str(spectral_bandwidth) + ',' + str(spectral_rolloff) + ',' + str(spectral_polyrhythm) + ',' + str(spectral_skewness) + ',' + str(chroma_mean) + ',' + str(chroma_std) + ',' + str(mfcc_mean) + ',' + str(mfcc_std)
Features = str(Features).replace('[','').replace(']','').replace(',',' ')
with open('test_features.csv', 'w') as f:
    f.write(Features)
f.close()

```

Fig 4: Test Case-1

Testing with our model

```

: model.predict(test_X)
: array([6])

```

Fig 5: Test Result-1

Our genres have been Label Encoded to numbers. Our model spat out 6 meaning that our model correctly predicted the song to be metal.

2. Loading a Jazz song to extract the features and test for it using our model

```

x,y = librosa.load('Resources/Jazz/Happy.mp3')
zero_crossings = librosa.zero_crossings(y, pad=False)
zero_crossings = np.array(zero_crossings)
spectral_centroid = librosa.feature.spectral_centroid(y, sr=sr)[0]
spectral_bandwidth = librosa.feature.spectral_bandwidth(y, sr=sr)[0]
spectral_rolloff = librosa.feature.spectral_rolloff(y, sr=sr)[0]
spectral_pca = librosa.pca_mfcc(y, sr=sr)
spectral_bandwidths = librosa.feature.spectral_bandwidth(y, sr=sr)[0]
spectral_bandwidths = np.array(spectral_bandwidths)
chromagram = librosa.feature.chroma_stft(y, sr=sr)
chroma_mean = [str(i) for i in chromagram.mean(axis=0)]
chroma_mean = np.array(chroma_mean)
mfcc_mean = [str(i) for i in librosa.mfcc(y=y)]
mfcc_mean = np.array(mfcc_mean)
features = str(zero_crossings) + ',' + str(spectral_bandwidth) + ',' + str(spectral_centroid) + ',' + str(spectral_rolloff) + ',' + str(spectral_pca[0][0]) + ',' + str(spectral_bandwidths) + ',' + str(chromagram) + ',' + str(chroma_mean) + ',' + str(mfcc_mean)
with open('test_features.csv', 'w') as f:
    f.write(features)
    f.close()

```

Fig 6: Test Case-2

Testing with our model

```

: model.predict(test_X)
: array([3])

```

Fig 7: Test Result-2

Our model has predicted our model to be a disco song while it's a jazz track. The confusion may be attributed to the fact there are aerophones in both songs and our model might have mixed up the both.

3. Loading a classical song to extract the features and test for it using our model

```

x,y = librosa.load('Resources/Classical/Clasic.mp3')
zero_crossings = librosa.zero_crossings(y, pad=False)
zero_crossings = np.array(zero_crossings)
spectral_centroid = librosa.feature.spectral_centroid(y, sr=sr)[0]
spectral_bandwidth = librosa.feature.spectral_bandwidth(y, sr=sr)[0]
spectral_rolloff = librosa.feature.spectral_rolloff(y, sr=sr)[0]
spectral_pca = librosa.pca_mfcc(y, sr=sr)
spectral_bandwidths = librosa.feature.spectral_bandwidth(y, sr=sr)[0]
spectral_bandwidths = np.array(spectral_bandwidths)
chromagram = librosa.feature.chroma_stft(y, sr=sr)
chroma_mean = [str(i) for i in chromagram.mean(axis=0)]
chroma_mean = np.array(chroma_mean)
mfcc_mean = [str(i) for i in librosa.mfcc(y=y)]
mfcc_mean = np.array(mfcc_mean)
features = str(zero_crossings) + ',' + str(spectral_bandwidth) + ',' + str(spectral_centroid) + ',' + str(spectral_rolloff) + ',' + str(spectral_pca[0][0]) + ',' + str(spectral_bandwidths) + ',' + str(chromagram) + ',' + str(chroma_mean) + ',' + str(mfcc_mean)
with open('test_features.csv', 'w') as f:
    f.write(features)
    f.close()

```

Fig 8: Test Case-3

Testing with our model

```

: model.predict(test_X)
: array([1])

```

Fig 9: Test Result-3

Our model predicted that the given track is a classical track while it really was classical. Our model was able to correctly predict it.

V. Conclusion

A model that classifies the songs based on their genres is built using ML techniques. The features extracted for this task are - energy of signal, zero crossing rate, spectral bandwidth, and spectral roll off, spectral centroid, chroma vector, and MFCCs. Different ML classifier algorithms like - decision trees, random forests, KNN, XGBoost, SVM have been tested to build the model for music genre classification tasks. Although most of the genres were better classified by the XGBoost algorithm than the rbf kernelized SVM algorithm, the overall accuracy of the model was obtained by the SVM classifier. The model built with the rbf kernelized SVM algorithm has performed better than others with a better accuracy of 64.67%, so we use this model for our task of genre classification.

VI. Future Enhancement

An appreciable effort has been made to start with a rudimentary retrieval system which can be improved upon with the current exercise. Although all the genres considered are closely interrelated with each other, and are sometimes difficult even for humans to wrongly classify them and yet we managed to build a build that performs appreciably. These models give the necessary features in terms of harmonics and spectral features. Further features can be extracted based on the vocal, keys and tempo of the songs. There is also scope to include a database system to the existing system to keep a track of previous records. We could further carry out our research and build more accurate models using deep learning techniques using neural networks.

References

- [1] Xu, Changsheng & Maddage, Namunu & Shao, Xi & Cao, Fang & Tian, Qi. (2003). Musical genre classification using support vector machines. 5. V - 429. 10.1109/ICASSP. 2003.11 99998.
- [2] Scaringella, Nicolas & Zoia, Giorgio & Mlynák, Daniel. (2006). Automatic genre classification of music content: a survey. Signal Processing Magazine, IEEE. 23. 133 - 141. 10.1109/MSP.2006.1598089.
- [3] Bahuleyan, Hareesh. (2018). Music Genre Classification using Machine Learning Techniques.
- [4] Elbir, A., Bilal Cam, H., Emre Iyican, M., Ozturk, B., & Aydin, N. (2018). Music Genre Classification and Recommendation by Using Machine Learning Techniques. 2018 Innovations in Intelligent Systems and Applications Conference (ASYU). doi:10.1109/asyu. 2018.85 54016.
- [5] Mutiara, Achmad & Refianti, R. & Mukarromah, N.R.A.. (2016). Musical Genre Classification Using Support Vector Machines and Audio Features. TELKOMNIKA Indonesian Journal of Electrical Engineering. Vol. 14. 1024-1034. 10.12928/telkomnika.v14.i3.3281.

- [6] Kim, Seong Hoon & Kim, Daesik & Suh, Bongwon. (2016). Music Genre Classification using Multimodal Deep Learning. 389-395.10.17210/hcik.2016.01.389.
- [7] Prabhu, Nimesh & Andro-Vasko, James & Bein, Doina & Bein, Wolfgang. (2018). Music Genre Classification Using Data Mining and Machine Learning. 10.1007/978-3-319-77028-4_52.
- [8] Lansdown, Bryn & He, Shan. (2019). Machine Learning for Music Genre Classification.
- [9] Ali, Muhammad & Ahmed, Zain. (2017). Automatic Music Genres Classification using Machine Learning. International Journal of Advanced Computer Science and Applications. 8. 10.14569/IJACSA.2017.080844.
- [10] Prabhu, N. R., Andro-Vasko, J., Bein, D., & Bein, W. (2018). Music Genre Classification Using Data Mining and Machine Learning. Information Technology – New Generations, 397–403. doi:10.1007/978-3-319-77028-4_52.
- [11] Sarkar, R., Biswas, N., & Chakraborty, S. (2018). Music Genre Classification Using Frequency Domain Features. 2018 Fifth International Conference on Emerging Applications of Information Technology (EAIT). doi:10.1109/eait.2018.8470441.
- [12] A Multimodal Music Emotion Classification Method Based on Multifeature Combined Network Classifier, Changfeng Chen and Qiang Li, Hindawi Mathematical Problems in Engineering Volume 2020, Article ID 4606027.
- [13] Y.-S. Seo and J.-H. Huh, Automatic emotion-based music classification for supporting intelligent IoT applications, Electronics, vol. 8, no. 2, p. 164, 2019.

A Review on Neuro Feedback System using Brain Computer Interface

G.Kavita

Department of CSE

Chaitanya Bharathi Institute of Technology(A),
Hyderabad-500075, India
gkavita_cse@cbit.ac.in,

Akshitha

Department of CSE

Chaitanya Bharathi Institute of Technology(A),
Hyderabad-500075, India
akshitha.n123@gmail.com

Namya Reddy

Department of CSE

Chaitanya Bharathi Institute of Technology(A),
Hyderabad-500075, India
gnamyareddy25@gmail.com

Abstract: The brain is the most important organ in the human body. Brain is divided into left and right hemispheres. These hemispheres are further divided into four lobes, called as frontal lobe, parietal lobe, occipital lobe and temporal lobe. Studies have shown that the asymmetry between left and right hemispheres causes stress and depression. The traditional way to overcome anxiety, stress, depression and other such conditions is to use medicines over a period of time. But usage of these medicines is leading to other side effects such as nervousness, weight gain, fatigue, drowsiness, vomiting etc. The alternative method is to use neuro feedback system to get around with the mentioned side effects.

The new technology called as Brain Computer Interface (BCI) can be used by people suffering with neuromuscular disorders, that is, people having problem with mobility and also by the people facing problem with listening and speaking or having visual defects. BCI acts as an interface between the human brain and computer. A differently abled person can easily and efficiently interact with the external environment by using BCI.

Considerable amount of Asymmetry between left and right brains called as differentiation of the brain function is one of the major concerns for the proper functioning of human body. This asymmetry of the brain can be monitored and analyzed by electroencephalogram signals from the scalp of the brain. Various devices are available in the market to capture electroencephalogram (EEG) signals from the human brain. Thus the Neuro feedback system uses BCI to accomplish its purpose. Neuro Feedback system helps to monitor brain waves and also to control the brain events. Neurofeedback provides immediate feedback from a computer-based program that assesses a subject's brainwave activity. There are several stimulus contents that can be used for neuro feedback training such as audio, video and games. Neurofeedback system can be used in varied applications where improvement in the efficient working of brain is desired. It can be used in treating dyslexia, Alzheimer's disease, attention-deficit/

hyperactivity disorder (ADHD) , psychotic disorders, autism, to improve concentration levels, to reduce stress or for the overall improvement of the brain functioning. In this paper, a study on neurofeedback systems is carried out.

Keywords: Brain Computer Interface (BCI), Electroencephalogram (EEG), Neurofeedback.

I. Introduction

The brain activity can be monitored and measured using invasive and non-invasive techniques. EEG is one of the non-invasive technique which places the electrodes on the scalp of the human brain to monitor and measure the brain activity whereas, invasive techniques require surgery to place the electrodes in any part of our body. Neurofeedback can be used as a interface that is used to improve the emotional disorders of a person. This method is used to find out the status of patients with mental disorders.

Brainwaves vary from one person to another. Brainwaves are classified into delta(0~4 hz), theta(4~8hz), alpha(8~12hz)and beta(12~30hz)waves. Alpha waves denotes relaxation and calm state of mind, Theta waves denotes meditation and sleepy state of mind, Low beta denotes attention and concentration state of mind, High beta denotes stress and tension state of mind. Neurofeedback is a kind of technique where brain exercises itself. Hence, brain function improves. The cognitive abilities are improved not only in patients with mental illness but also in healthy people by using this training. Neurofeedback systems have several applications like, it can be used to decrease the stress and depression, for improving the concentration of individuals and also in various medical treatments.

The paper is organized as follows. Section2 describes the literature survey on the neurofeedback system, tools and technologies used for the implementation of system. Section 3 discusses about the design of the neurofeedback system and section4 draws the conclusion and the future scope.

II. Literature Survey

1. Related Works

In [1], a neurofeedback system was used to reduce stress and anxiety. This paper concluded that there was a considerable improvement in the symmetry of left brain activity and right brain activity. In this paper, Naïve Bayesian machine learning technique was used for classification and experiment was performed for 3 weeks. The results were compared for the first and last week of the experiment which has confirmed improvement in alpha and beta waves. Here, the alpha and beta waves were increased by 21.86% and 17.41%, respectively and asymmetry of left brain and right brain was decreased.

In [2], the efficiency of different neurofeedback stimulus contents was investigated. The stimulus contents which were considered for neurofeedback training were Audio, video, and games. The alpha power and alpha asymmetry were calculated before the neurofeedback session and later compared with the values obtained after the neuro feedback session. Here, the EEG data were recorded during multiple sessions for 29 study participants. The statistical significance of the results was verified by ANOVA and post hoc testing. It was concluded that to reduce stress game was more efficient than the other stimulus contents for neurofeedback training.

In [3], To design four states BCI for a neurodegenerative person using EEG Band Power (BP) and Radial Basis Function (RBF) were used. The analysis of the performance of the wheelchair for neurodegenerative person was carried out. For four tasks an average classification accuracy of 95%, 87.50%, 92.50%, 95.00% was achieved. This paper has showed that a person with disability can control the wheelchair by converting his mental thoughts to commands with an overall classification accuracy of 92.50%.

In [4], a study was done on BCI which was presented using 6 sections. In the first section, a brief introduction of BCI was given. In the second section, all the BCI components like signal acquisition, feature identification and feature extraction by several algorithms were discussed. In the third section, BCI characteristics were described. In the fourth section, some of the BCI challenges like issues with the headsets, lack of ideal data analysis methods, eliminating artifacts, inter-subject and intra-subject differences were discussed. In the fifth section tools used in BCI research like Matlab, Scilab for offline and online mode, Octave were described. In the sixth section few applications of BCI were presented.

In [5], To preserve the spatial, spectral, and temporal structure of EEG an approach was designed. Here, the brain activities are converted into a sequence of topological images which preserves multi-spectral features. Next, a deep recurrent-convolutional network is trained. In this paper, the author compared the above approach against various classification algorithms like Support-Vector Machines (SVM), sparse Logistic Regression, and Deep Belief Networks (DBN). The preprocessing step used converts the EEG time domain data acquired from various sources into frames.

In [6], a machine learning framework was proposed. Stress was induced in this experiment by using a well-known experimental model based on the Montreal imaging stress mission. The tension was triggered, and the task success and subjective input confirmed it. EEG feature extraction, feature collection, classification using logistic regression, support vector machine and nave Bayes classifiers machine learning techniques, and tenfold cross validation were all part of this machine learning system. This system had an accuracy of 83.4 percent for multiple level stress identification and 94.6 percent for two-level stress identification. Finally, this paper introduced an EEG-based ML paradigm that has the ability to objectively measure stress at multiple levels.

In [7], the author's goal is to create a brain-computer interface (BCI) speller that uses asynchronous electroencephalogram (EEG) signals and eyes-closed and double-blinking electroencephalogram (EEG) signals. This system consists of a signal processing module and a graphical user interface with 26 English characters plus a special symbol. The "select" command is activated when a "eyes-closed" event is detected, while the "undo" command is activated when a "double-blinking" event is detected. The results showed that for multi-class classification, this method can achieve an overall accuracy of 93.8 percent.

In [8], it was considered that by using mu rhythm technique, accurate classification of Motor Imagery was difficult to achieve, Extreme learning machine (ELM) has proved to be more effective than support vector machine, which is a benchmark for MI-related EEG classification, since it was very slow and likely to be polluted by other background noises, and as an extension of the single layer feedforward network. As a result, the author proposed Motor Imagery (MI) EEG classification algorithm based on a Sparse Bayesian Extreme Learning Machine (SBELM). SBELM's efficacy is tested using a publicly accessible dataset from BCI Competition IV IIb, and it is compared to a variety of other algorithms. The SBELM-based algorithm's high classification accuracy suggested that it is a

promising candidate for improving the efficiency of a Motor Imagery BCI.

In [9], it presented a comparison study using a brain-computer interface (BCI) system between people with spastic paralysis and safe controls of various ages. The research was conducted in a qualitative manner. In Portugal and Brazil, people with spastic paralysis and healthy controls were tested. The aim of the research was to create a product assessment study to see whether people with cerebral palsy can communicate with computers and whether their output is comparable to that of healthy controls when using a brain-computer interface. There are no major variations between people with spastic paralysis in the two countries, as well as between populations without spastic paralysis, according to the findings (healthy controls). It used the NeuroSky MindWave brain-computer interface to assess the output of both classes.

In [10], a survey of all optimized methods for filtering the EEG signal was conducted, as well as a comparison of the different classification methods used to categorize the emotions. The aim of this paper was to propose an effective EEG classification algorithm based on a multimodal approach that not only considers the EEG signal for emotion classification but also verifies the result using the NLP technique to obtain more accurate results.

2. Commonly used Tools and Technologies for Neurofeedback Systems

Technologies for creating GUI: Electron, Django, Bootstrap, NodeJS, jQuery, HTML, CSS.

Technologies for Backend: Python, Java Dependencies:

1. WebSocket API: It helps to open a two-way communication session between the server and user's browser.
2. Cortex API: It is used to communicate with the Emotiv products. Since it is built on JSON and WebSockets, it makes it easy to access from different programming languages and platforms.

Software Requirements

Operating System: Windows 7 or above

Environment: Python, NodeJS/Django
Hardware Requirements

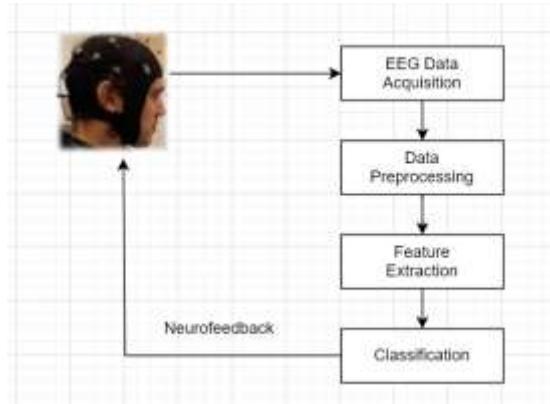
Processor: Intel core i5 or better processor
RAM: 8 GB or more

Disk Space: 500MB available disk space

EEG Headset: There are various EEG headsets available in the market such as Emotiv Insight, EPOC, EPOC+, Open BCI's Mark IV etc.

III. Design of the Neurofeedback System

1. Sequence of the activities carried out in the system.



Description: First, we collect the raw eeg data (brain waves) using Emotiv headset from the subjects. This data can be used in diverse ways depending on the application. Then preprocessing of data is done using filters. Then features are extracted, classification is done using Machine Learning, deep learning algorithms and predictions are made. Then the neurofeedback is given to the subject.

IV. Conclusions

In this paper a study on neurofeedback systems was carried out. It was found that to optimize brain function, asymmetry between the left brain and right brain must be decreased. One of the studies, concluded that games were the most effective neurofeedback stimuli content. In most of the systems the accuracy achieved from deep learning algorithms is more when compared to that from machine learning algorithms. This work presented current trends in Neurofeedback systems.

This study focused on several techniques used for feature extraction and classification for neurofeedback systems. Some of the techniques used for classification are Naïve Bayesian, Deep belief networks, KNN, Support Vector Machine, Sparse Bayesian Extreme Learning Machine (SBEML) etc. Some of the tools used in this research are GNU Octave, FreeMat, Scilab, MATLAB, EEGLab, Emotiv Apps etc. Some of the challenges faced in this field are lack of ideal data analysis methods, inter-subject and intra-subject differences.

Future research can be done with Robust patterns determined by using a 14 or 32 channel EEG headset and a high-end GPU for training the models.

A small percent of the users cannot learn how to use the system. For this the possible solution is to create interactive co-learning environment which is more user-friendly for the respective application. We can also develop a mobile application to make the systems more connected with the users. Neurofeedback system can be used in medical field for various purposes, for improving research, also in educational field for improving concentration in students. It can also be used for increasing the efficiency of researchers, doctors etc.

References

- [1] Jonghwa Choi, Sungjoong Kim, Dongmin Shin, Young-hwan You, Dongil Shin, And Dongkyoo Shin, "Neuro-Feedback System Enhancing the Level of Symmetry in Left and Right Brain Activities",2020.
- [2] Yasir Hafeez, Syed Saad Azhar Ali, Wajid Mumtaz, Muhammad Moinuddin "Investigating Neurofeedback Protocols for Stress Mitigation: A Comparative Analysis of Different Stimulus Contents", 2019.
- [3] Li Junwei, S. Ramkumar, G. Emayavaramban , "Brain computer interface for neurodegenerative person using EEG", 2018.
- [4] [Parmar Prashant, Anand Joshi, Vaibhav Gandhi, "Brain-Computer Interface Review",2015.
- [5] PouyaBashivan , Irina Rish, Mohammed Yeasin, Noel Codella," Learning Representations from Eeg With Deep Recurrent-convolutional Neural Networks", 2016.
- [6] Ahmad Rauf Subhani, Wajid Mumtaz, Mohamed Naufal Bin Mohamed Saad, Nidal Kamel, And Aamir Saeed Malik, "Machine Learning Framework for the Detection of Mental Stress at Multiple Levels",2017.
- [7] Trung-haunguyen, da-lin yang, and wan-young chung, "A high-rate BCI speller based on eye-closed EEG signal",2018.
- [8] [ZhichaoJin, Guoxu Zhou, Daqi Gao, Yu Zhang, "EEG classification using sparse Bayesian extreme learning machine for brain-computer interface",2018.
- [9] Regina Heidrich, Francisco Rebelo, Marsal Branco, João Batista Mossmann, Anderson Schuh, Emely Jensen, Iago Oliveira, "A Comparative Study: Use of a Brain-Computer Interface (BCI) Device by People with Cerebral Palsy in Interaction with Computers",2015.
- [10] K. Saranya, S. Jayanthi, "BCI based EEG Signals for Emotion Classification", International Journal of Recent Technology and Engineering (IJRTE), Volume 7, January 2018.
- [11] Michele bevilacqua , Serafeim Perdikis, and José Del R. Millán, "On Error-Related Potentials During Sensorimotor-Based Brain-Computer Interface: Explorations with a Pseudo-Online Brain-Controlled Speller", 2019.
- [12] N. Hamzah, N.A.M Syukur, N. Zaini, F.H.K. Zaman, "EEG Signal Classification to detect Left and Right Command using artificial neural networks", AJOL, Volume 9, No. 4S, 2017.
- [13] Yuanqing Li, Chuanchu Wang, Haihong Zhang and Cuntai Guan, "An EEG-based BCI system for 2D cursor control", 2008 IEEE International Joint Conference on Neural Networks (IEEE World Congress on Computational Intelligence), 2008.
- [14] Parth Agrawal, Parul Khanna, Beaulah Soundarabai P, Niju P Joseph, "Electroencephalogram based Brain Computer Interface System Analysis", IJITEE, ISSN: 2278-3075, Volume-9 Issue-3S, January 2020.
- [15] C. Hintermüller, C. Guger, G. Edlinger, "Brain-Computer Interface: Generic Control Interface for Social Interaction Applications",2011.
- [16] Xiang-Zhen Kong, Merel C. Postema, Tulio Guadalupe, Carolien de Kovel, Premika S. W. Boedhoe, Martine Hoogman, Samuel R. Mathias,Daan van Rooij, Dick Schijven, David C. Glahn6, Sarah E. Medland, Neda Jahanshad, Sophia I. Thomopoulos, Jessica A. Turner,Jan Buitelaar, Theo G. M. van Erp Barbara Franke, Simon E. Fisher1,18 | Odile A. van den Heuvel, Lianne Schmaal,Paul M. Thompson Clyde Francks"Mapping brain asymmetry in health and disease through the ENIGMA consortium" april 2020

Session-B1:
VLSI and Embedded Systems

Design and Analysis of Approximate Lower-Part OR Adder for Low Power Computations

Varala Pasula Nikhila

Department of ECE

Chaitanya Bharathi Institute of Technology (A)
Hyderabad-500075, India

Abstract: As the devices reach deep sub-micron technology, power consumption has become a major concern in the design of integrated circuits. Meeting power requirements while maintaining high performance is a complicated task in the present era. Approximate computing has evolved as a promising design approach recently which has attracted the attention of various researchers. It is a technique which enhances the performance of the circuit and reduces the energy consumption by trading it off with some loss in the output accuracy. The increasing demand for high speed, low power consumption and also the error resilience property in many applications like image processing, multimedia, artificial intelligence, biometric security and machine learning where an inaccurate result is sufficient, has motivated the development of approximate computing. Adders are one of the most essential arithmetic circuits in Digital Signal Processor (DSP) systems which are used for image and video processing and they play a vital role in determining the power consumption, speed and performance of the system. This paper focusses on the design of an approximate adder called Lower-Part OR adder (LOA) which uses OR gates and AND gates for approximate computations. A 4-bit LOA is designed using Cadence tool in 90 nm and 180 nm CMOS technologies and its power consumption is compared with that of 4-bit accurate Ripple Carry Adder.

Keywords: Approximate computing, error resilience, low power, approximate adders, Lower-part OR adder.

I. Introduction

The feature size of transistors has decreased exponentially in the past few decades, [1] following the Moore's law according to which the number of transistors on an integrated circuit gets doubled for every two years. As a result, the performance and energy efficiency of integrated circuits has been continuously improving. But as the transistor count increased and the feature size reaches nanometre realm, the benefits deriving from small transistor sizes diminished. The improvements in area, power, and delay resulting from scaling have started to see a decrease. Approximate computing has emerged as an

Dr. N. Alivelu Manga

Department of ECE

Chaitanya Bharathi Institute of Technology (A)
Hyderabad-500075, India

approach in which applications can bear some loss in the image or video quality, yielding acceptable outputs to have an energy efficient design.

The main motivation behind approximate computing is the feature of error tolerance or resilience in applications like image processing, multimedia and biometric security which can tolerate some amount of degradation in the output in terms of quality or accuracy in the computed result. There may be many sources of error resiliency [2]: (i) applications where redundant data is used in which the output can have a range of acceptable results rather than having an accurate result, (ii) in applications like multimedia, some amount of data gets unnoticed because human eye cannot perceive everything due to perceptual limitations and (iii) applications which are used to process noisy data.

Adders are the basic elements of DSP systems which are primarily used in arithmetic logic units. They can also carry out numerous other operations like subtraction, division, multiplication, shift, increment and decrement operations [3]. A number of research studies have investigated approximate computing which can be done at both software level as well as the hardware level of abstraction [4]. Some levels of algorithm are skipped or eliminated in the software level, whereas the hardware techniques involve redesigning the logic circuitry. Approximate adders are designed using hardware level approximation to obtain low area, delay and power of the entire system and to minimize the complexity of the circuit and lifetime of the carry propagation.

Approximate adders can be constructed using two approaches [5]. A single-bit approximate computing based full adder is designed by minimizing the number of transistors or gates in the first approach which results in low power dissipation, less area and high performance than the accurate adders. This approximate full adder is used in the lower significant bit positions only and in most significant bit positions accurate adder is used to ensure that the outcome of the adder is acceptable. In the second methodology, a block-based approximate multi-bit adder is designed in which the adder is divided into smaller overlapping accurate multi-bit sub-adder blocks. Here, the carry propagation chain is smaller which results in high speed, low power dissipation, and area required. The primary objective

of this paper is to analyze the Lower-part OR Adder which is designed based on the first methodology and to compare its power consumption with an accurate Ripple Carry Adder.

The rest of the paper is organised along the following lines. Section II provides a review of existing approximate adders. The lower part OR adder architecture is described in section III. In section IV, the simulation results of LOA and its comparison with RCA is presented. Finally in section V, the paper is concluded.

II. Review

A wide variety of approximate adders have been studied in detail and a great deal of research has been carried out over the past few years. In [6], five simplified versions of the widely used mirror adders are proposed by reducing the logic complexity at the transistor level. Some transistors which are connected in series are removed by ensuring that there is no open circuit or short circuit for any input combination and minimum number of errors are introduced in the simplified circuit. In [7], XOR/XNOR based 10-transistor exact full adder is approximated and three Approximate XOR/XNOR Adders have been presented. Pass Transistor Logic is used here to implement multiplexer which reduces the logic complexity by eliminating redundant transistors. [8] has proposed three inexact adder cell designs by approximating full adder circuit at gate level. This is done by approximating one of the full adder outputs while using accurate result for the other output. [9] presented two approximate adders using transmission gate-based multiplexers. They are designed by either removing some transistors from accurate full adder which is made up of three modules or by changing some of the signals for sum and carry out. In [10], an Accuracy Configurable Adder is presented that can be operated in both accurate and inaccurate modes. The output accuracy can be configured at runtime. This adder is divided into multiple sub-adders and errors can be detected and corrected using AND gates and incrementors respectively. [3] has presented an Approximate Carry Look-ahead Adder which is designed by modifying and considering only the carry propagation part in the carry-out expression of accurate Carry Look-ahead Adder

III. Lower-Part or Adder

In the lower-part-OR adder (LOA), addition of n bits is divided into two smaller parts: nh -bit and nl -bit such that $nh+nl=n$ where ' h ' represents higher bits and ' l ' represents lower bits [11] as shown in figure 1. In the upper part of LOA, a sub-adder which is a smaller accurate adder is available to calculate the precise values of the ' nh ' most significant bits of the output. It also has OR gates which are used to

compute the approximate values of the ' nl ' least significant bits of the result in the lower part which is done by bitwise OR operation of the corresponding input bits. For sub-adder in the upper part, carry-in is generated using an extra AND gate when MSBs of both inputs of lower part are one. This is used to decrease the imprecision of adder by considering the carries from lower part to upper part of the LOA. The sub-adder can have any precise structure like Ripple Carry Adder or Carry Look-ahead Adder. If more efficient precise adders are used as the sub-adders, it directly results in a more efficient LOA. For an LOA which has a constant word length (' p '), as the value of ' nl ' or Lower-Part Length increases, the area, power consumption and delay of the LOA decreases and imprecision increases. The error due to approximation is in the LSB part because the carry is not considered in the lower part of the adder and hence approximation is limited to the lower bits.

For a single bit LOA, sum is calculated using OR gate and carry is calculated using AND gate. Its truth table is shown in Table I. In a single bit approximate adder, sum has 4 errors whereas carry has 2 errors compared to accurate adder. A ripple carry adder can be implemented with Lower-part OR Adder architecture by varying the length of lower part. For a 4-bit adder, four approximate LOA adders can be designed. For the first approximate adder, LOA-1, the full adder in the LSB position is replaced with the OR gate to generate sum (S_0) and AND gate to produce carry-in for the accurate adder. In other 3 bits' positions, the precise full adder is used for the sum and carry generation. LOA-2 has two OR gates in the two LSB bit positions to generate sum (S_0, S_1) and AND gate in the LSB to generate carry-in. In the other 2 bits' positions, the precise full adder is used for the sum and carry generation. Similarly, LOA-3 has three OR gates in the three LSB bit positions to generate sum (S_0, S_1, S_2) and AND gate in the LSB to generate carry-in. In the other 1-bit position, the precise full adder is used for the sum and carry generation. LOA -4 has four OR gates to generate sum (S_0, S_1, S_2, S_3) and one AND gate to generate carry-out ($Cout$).

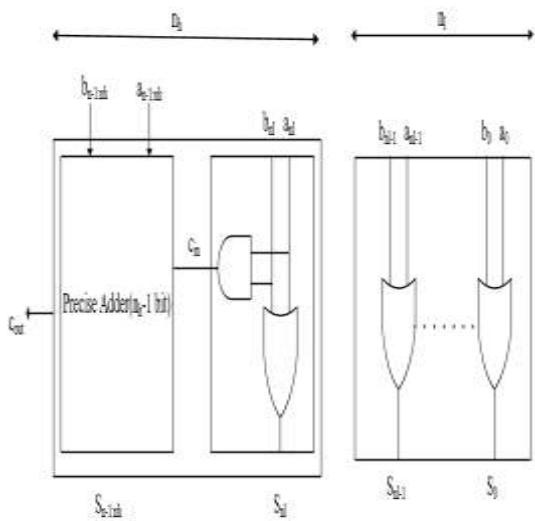


Fig 1: Architecture of Lower-Part OR Adder (LOA)

Table I: Truth Table of 1-bit Full Adder and 1-bit LOA

Inputs			Precise Adder		Approximate Adder	
A	B	C_{in}	Sum	C_{out}	Sum	C_{out}
0	0	0	0	0	0	0
0	0	1	1	0	0	0
0	1	0	1	0	1	0
0	1	1	0	1	1	0
1	0	0	1	0	1	0
1	0	1	0	1	1	0
1	1	0	0	1	1	1
1	1	1	1	1	1	1

Table II: Transistor count, total power consumption of LOA and percentage improvement with respect to RCA

Adder	Transistor Count	90nm Technology		180nm Technology	
		Power Consumption (nW)	Improvement in Power Consumption (%)	Power Consumption (uW)	Improvement in Power Consumption (%)
RCA	20	665.9	-	431.5	-
LO A-1	17	504.4	24.25	404.9	6.16
LO A-2	13	395.4	40.62	267	38.12
LO A-3	9	237.8	64.28	94.71	78.05
LO A-4	5	151.8	77.20	94.71	78.05

IV. Results

4-bit accurate Ripple Carry Adder and Lower-part OR Adders are designed, implemented and simulated using Cadence virtuoso tool with 90nm and 180nm technologies. These approximate adders are designed by applying Lower-part OR Adder architecture to Ripple Carry Adder and varying the length of lower part. For 90nm technology, 1 V is used as standard supply voltage (VDD) and for 180nm technology, 1.8 V is used as VDD. Table II shows the transistor count, total power consumed by RCA and LOA and the percentage improvement with respect to RCA. The number of transistors in LOA has greatly reduced compared to total number of transistors in RCA which is 20. LOA-1 has the greatest number of transistors which is 17 whereas LOA-4 has the least which is 5. Hence, LOA-4 has the simplest structure and LOA-1 has a complex structure. The maximum power consumed by approximate adder is 504.4nW and 404.9uW for LOA-1 in 90nm and 180nm technologies respectively. The minimum power consumption is 151.8nW for LOA-4 in 90nm technology and 94.71uW for LOA-3 and LOA-4 in 180nm technology. The improvement in power consumption ranges from 24.25% to 77.20% in 90nm technology and 6.16% to 78.05% in 180nm technology.

V. Conclusion

Approximate computing is a recently emerging design paradigm which is gaining prominence for the implementation of error-resilient systems. It is based on the idea that high performance and energy efficiency can be attained in digital systems through fair negotiation with the correctness of the result. This means that, by putting less efforts to deliver an accurate and correct result, other design metrics are enhanced. A Lower-part OR Adder which computes accurate results in upper part and approximate results in lower part has been designed and analyzed for 4-bit addition in this paper. It uses OR gate to generate the sum and carry-in which is given as input to the precise adder in the upper part is generated using an AND gate. By comparing LOA with an accurate RCA it is clear that by sacrificing a very little precision, it is possible to obtain considerable savings in power consumption and transistor count. Simulation results show that there is 24.25% to 77.20% power savings in 90nm technology and 6.16% to 78.05% power savings in 180nm technology.

References

- [1] Antonio G. M. Strollo; Darjn Esposito, "Approximate Computing in the Nanoscale Era", International Conference on IC Design & Technology (ICICDT), 2018.

- [2] Jie Han and Michael Orshansky, "Approximate Computing: An Emerging Paradigm for Energy-Efficient Design", IEEE European Test Symposium (ETS), 2013.
- [3] Jayeeta Barman and Vinay Kumar, "Approximate Carry Look Ahead Adder (CLA)for Error Tolerant Applications", 2nd International Conference on Trends in Electronics and Informatics (ICOEI), 2018.
- [4] Honglan Jiang, Cong Liu, Leibo Liu, Fabrizio Lombardi, Jie Han, "A Review, Classification and Comparative Evaluation of Approximate Arithmetic Circuits ", ACM Journal on Emerging Technologies in Computing Systems, 2017.
- [5] K. Varnika, "Approximate Adder: Lower-part OR Adder," International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2020.
- [6] Vaibhav Gupta, Debabrata Mohapatra, Anand Raghunathan, "Low-Power Digital Signal Processing Using Approximate Adders", IEEE Transactions on Computer-aided Design of Integrated Circuits and Systems, 2013.
- [7] Zhixi Yang, Ajaypat Jain, Jinghang Liang, Jie Han and Fabrizio Lombardi, "Approximate XOR/XNOR-based Adders for Inexact Computing", IEEE International Conference on Nanotechnology , 2013.
- [8] Haider A.F.Almurib, T. Nandha Kumar and Fabrizio Lombardi, "Inexact Designs for Approximate Low Power Addition by Cell Replacement", Design, Automation & Test in Europe Conference & Exhibition (DATE), 2016.
- [9] Zhixi Yang, Jie Han and Fabrizio Lombardi, "Transmission Gate-based Approximate Adders for Inexact Computing", Proceedings of the 2015 IEEE/ACM International Symposium on Nanoscale Architectures, 2015.
- [10] Andrew B. Kahng and Seokhyeong Kang, "Accuracy-configurable adder for approximate arithmetic designs", DAC Design Automation Conference, 2012.
- [11] H. R. Mahdiani, A. Ahmadi, S. M. Fakhraie, and C. Lucas, "Bio-Inspired Imprecise Computational Blocks for Efficient VLSI Implementation of Soft-Computing Applications", IEEE Transactions on Circuits and Systems, 2010.

Implementation of FPGA based Image Processing Algorithm Using Xilinx EDK

Aruna Kokkula

Assistant Professor

ECE Department

Matrusri Engineering College

Hyderabad- 500059, India

kokkulaaruna@gmail.com

P.Amulya

BE Student

ECE Department

Matrusri Engineering College

Hyderabad- 500059, India

amulya.parasara@gmail.com

B. Indira Priyadarshini

Assistant Professor

ECE Department

Matrusri Engineering College

Hyderabad- 500059, India

priyadarshini414@gmail.com

B. Charan Supraj

BE Student

ECE Department

Matrusri Engineering College

Hyderabad- 500059, India

charansupraj@gmail.com

Abstract: One of the important purposes of digital image advancement techniques is increasing the quality of photographic images. This paper majorly describes image enhancement techniques especially at spatial domain. The images are processed with reference points when images are undergone different stages such as manipulation of brightness and contrast, negative images, threshold, Logarithmic transformation, intensity-level slicing, gamma correction and edge detection. The image is processed through different hardware software co-simulation platforms such as Xilinx Platform Studio (XPS). For better operation, this one implemented through C/C++ instead of Verilog HDL.

Keywords: Image Enhancement, Xilinx Platform Studio, FPGA, MATLAB JTAG and UART.

I. Introduction

There was huge rise at digital images which is generated from computer. People interested to click high quality images from different cameras and then stored at different memory devices. Individuals need to impart the pictures to loved ones by means of web (Facebook, WhatsApp). Picture improvement is the process that is made out of various strategies used to accomplish the presence of a picture in visual or picture is changed over to a more qualified structure for investigation by a human being or machine.

Picture Enhancement manages handling of a picture with the end goal that subsequent picture is more appropriate than unique. It manages separating data from picture, which can't be seen by natural eye. So determination of a picture improvement strategy relies upon the information picture to be prepared. The enhancement techniques of pictures are sorted into different strategies such as frequency domain and spatial domain. In this paper we have concentrated on spatial space methods. In Spatial

space, Image Enhancement Techniques (figure 1) are named.

Brightness Adjustment: An expansion or abatement in splendour coming about either from making an improvement discontinuous, or when a surface is encircled by a dim zone, when contrasted with when it is encircled by a light region.

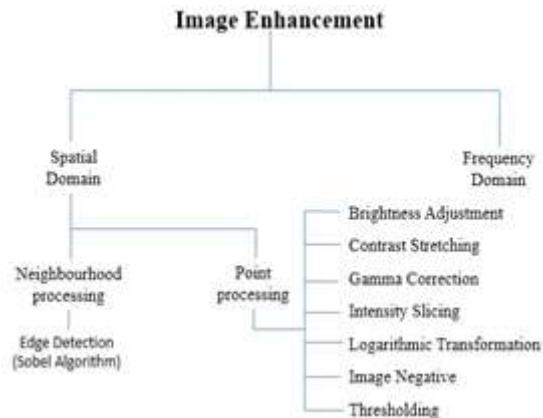


Fig 1: Classification of Image Enhancement Techniques

Contrast stretching: Contrast stretching additionally called standardization is a straightforward picture upgrade procedure that endeavors to improve the differentiation in a picture by 'extending' the scope of force esteems it contains to traverse an ideal scope of qualities.

$$P_{out} = (P_{in} - c) \left(\frac{b - a}{d - c} \right) + a$$

Pout= Output value of the pixel

Pin= Pixel value of the image

A =0 (Min value of 8bit pixel)

B =255 (Max value of the 8bit pixel)

C = Desired min value of the pixel

D = Desired max value of the pixel

Gamma Correction: Gamma correction work is a capacity that maps radiance levels to repay the non-direct glow impact of show gadgets.

$$V_{\text{out}} = A V_{\text{in}}^{\gamma}$$

V_{out} =The pixel value after processing

V_{in} =The Pixel value of the Image

A=Constant

γ =Gamma Value

Intensity Level Slicing: Intensity level slicing (Fig 2) methods featuring a particular scope of forces in a picture. As such, we fragment certain dim level districts from the remainder of the picture. In this sort of preparing we set a scope of pixel esteems and upgrade them in like manner.

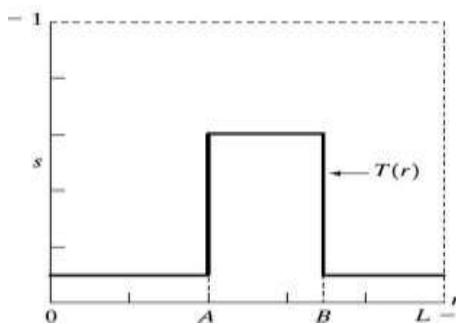


Fig 2: Intensity Level Slicing

Log Transformation: Logarithm transformation (Fig 3) is a non-direct picture handling activity. Accepting that the picture $f(x, y)$ is certain esteemed, the logarithmic point activity is characterized as

$$S = C \cdot \log(1+r)$$

Where $r \geq 0$ and c is a constant. Adding solidarity to the picture keeps away from the chance of taking the logarithm of zero. The state of the log bend in Fig 3 shows that this change maps a restricted scope of low dark levels. The entirety of the dark level is compacted to the range $[0, \log(L)]$.

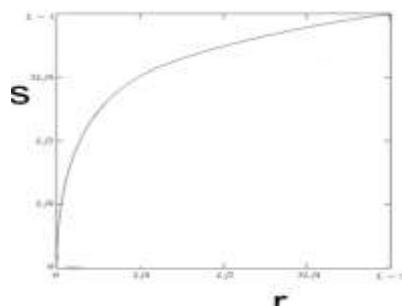


Fig 3: Logarithmic transformation

Image Negatives: The negative of a picture (Fig 4) with dark level in the range $[0, L-1]$ is acquired by utilizing the negative change, which is given by the articulation

$$S = L - r - 1$$

Image Negatives are only turning around the powers of each pixel.

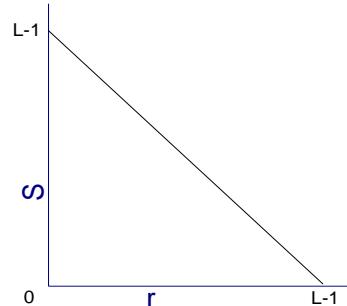


Fig 4: Image negative Transformation

Image Thresholding: In this procedure, the pixels underneath edge esteem are relegated dim scale esteem 0 or more limit esteem is doled out dark scale esteem 255. The choice procedure is typically called thresholding.

$$\begin{aligned} S &= 0 && \text{if } r < m \\ &= 255 && \text{if } r \geq m \end{aligned}$$

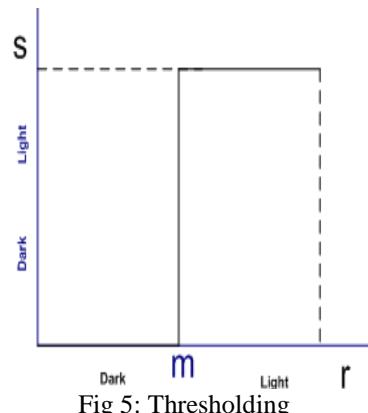


Fig 5: Thresholding

Instances of thresholding applications are record picture (Fig 5) investigation, where the objective is to extricate printed characters, logos, graphical substance or melodic scores, where lines legends and characters are to be discovered scene preparing, where an objective is to be distinguished. The yield of the thresholding activity is a twofold picture.

Edge Detection (Sobel Operator): The edge identification or edge detection might be founded on assessing the pace of progress of forces in the pixel neighbourhood. In the discrete picture portrayal, the fractional subordinates are approximated by directional contrasts (Fig 6).

The gradient at (x, y) for a function $p(x, y)$ is defined as two dimensional column matrix

$$\mathbf{p} = \begin{bmatrix} \frac{\partial y}{\partial x} \\ \frac{\partial x}{\partial y} \end{bmatrix}$$

$$\nabla_p = \text{mag}(\nabla_p) = [G_x^2 + G_y^2]^{1/2}$$

The ∇_p is approximated as

$$f = |G_x| + |G_y|$$

The masks for Sobel operator are:

$$G_x = \begin{bmatrix} +1 & 0 & -1 \\ +2 & 0 & -2 \\ +1 & 0 & -1 \end{bmatrix} * A \quad \text{and} \quad G_y = \begin{bmatrix} +1 & +2 & +1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix} * A$$

Fig 6: 3×3 Gradient (Sobel) masks

With reference of original image, processed image measured different quality points.

The list of Image Quality measures implemented includes:

1. **Structural Content (SC):** The Structural Similarity Index (SSIM) likewise called as Structural content is a perceptual metric that evaluates picture quality corruption brought about by handling. It is a full reference metric that requires two pictures from a similar picture catch for example a reference picture and a handled picture
2. **Mean Square Error (MSE):** The mean square error defined as error between original and cumulative squared compressed image. The lower the MSE value the better the quality.
3. **Peak Signal to Noise Ratio (PSNR):** It is used to measure the peak error in dB. The high quality images have high PSNR.
4. **Normalized Cross-Correlation (NCC):** The Normalized cross connection coefficient (NCC) is the used to compute the closeness of two clusters in the scope of 0....1 (equivalent to 0....100%).
5. **Average Difference (AD):** This term calculates the average difference of the input and output image pixel values.
6. **Maximum Difference (MD):** This term finds the maximum altered pixel value of output compared to input.
7. **Normalized Absolute Error (NAE):** NAE is normalized error by averaging of actual value.

II. Literature Survey

M. Ownby et.al (2003) described actualizing approach for current DSP applications and presented results when it is implemented on Xilinx system generator with MATLAB. To improve the plan of complex framework, they proposed rationale reconfigurable technique which is targeted effective learning. The DSP structure models of proposed work are implemented on Xilinx system generator. As of late, the complexities of equipment plans have expanded fundamentally. The on-time consummation became more difficult in terms of understanding of plan ventures because of shortage of skilled fashioners and cycle of diminishing structure. The created technique tends to the accompanying issues like deciding the structure details, planning a framework in Simulink using System, Simulating the plan in Simulink, MATLAB system generator software works on VHDL/ Verilog code in Xilinx/ Modelsim. A DSP application selected to show the time delay and frequencies between two sine waves by structural approach.

S. R. A. S. J.C.Moctezuma et.al (2008) clarifies the design for channels pixel by pixel and districts channels for picture preparing utilizing software. It offers an extra option such as consolidations of MATLAB, XSG and Simulink. It also provides significant angles for equipment when it is implemented. The treatment of advanced pictures has become in on-going decades a subject of across the board enthusiasm for various territories. We may refer to heaps of models where picture handling assists with dissecting, construe and decide. The fundamental target of picture handling is to increase the nature of the pictures for this work and the handling pixel of a picture and in the adjustment of pixel neighbourhoods and obviously the change is to be implemented to the entire picture or just an incomplete district. The need to process the picture progressively, prompting the execution level equipment and parallelism. Accordingly essentially decreases the preparing time is chosen for this work. Xilinx System Generator is a graphical interface in the Matlab Simulink, based squares which makes it exceptionally simple to deal with as for other programming for equipment portrayal.

III. Methodologies

The algorithm is proposed in MATLAB to process a image requires methods in picture improvement (spatial domain) process. Summoning this header record in MATLAB with XPS-EDK. The header is recorded at client who includes configuration of coordinated venture menu. It combines both sources cache tab and header tab at C/C++ domain. The calculation of plan determination is incorporated with header documents.

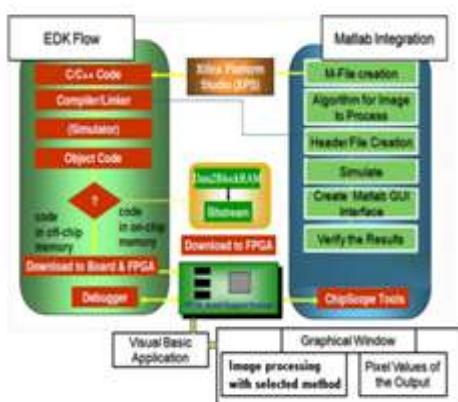


Fig 7: Design Flow of EDK

The equipment module was created alongside XPS in EDK Design Environment. Conjuring Header record and incorporated with Software module and blended a mythical person document was produced. Fig 7 presents an assessment of equipment displaying plan for picture upgrade procedures utilizing FPGA through Xilinx Platform Studio.

IV. Proposed System

The proposed framework has Xilinx stage studio (XPS) in the spot of Xilinx System generator (XSG) of the current framework.



Fig 8: Flow chart of XPS

Furthermore, in the Xilinx framework generator Simulink squares are utilized to make the calculation, where as in the current framework we

have to compose a C/C++ code and afterward download it to the FPGA

In the above stream diagram fig 9, as we can watch we have to physically build up the code for the necessary method. In the wake of building up the code we download/program it to the FPGA for the necessary yield. And furthermore there is a distinction that there is another code in MATLAB to see the yield showed through UART correspondence.

V. Results

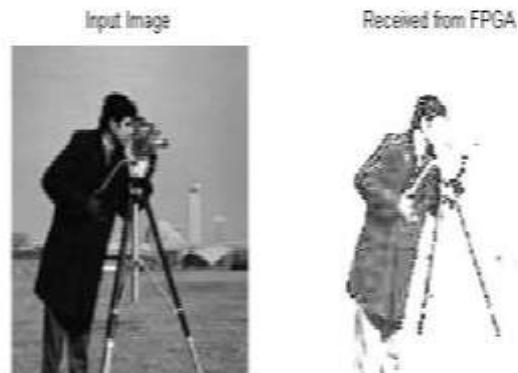


Fig 9: Brightness enhancement (I+100)



Fig 10: Brightness suppression (I-100)



Fig 11: Logarithmic Transformation

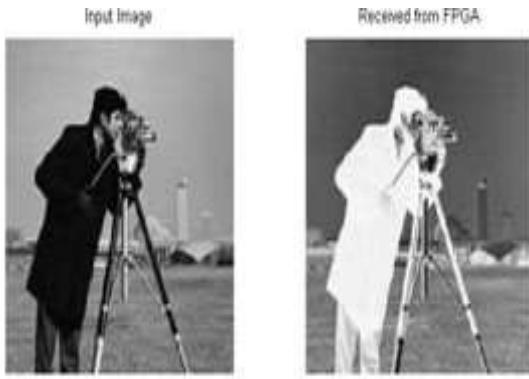


Fig 12: Image Negative

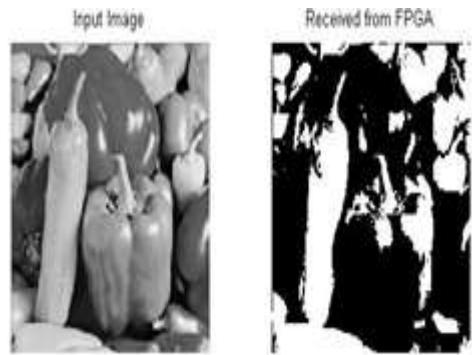


Fig 16: Thresholding Image ($t>150$)

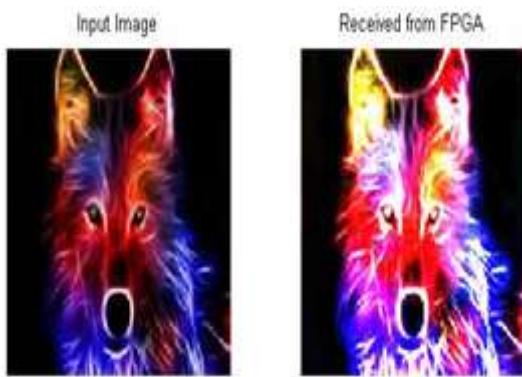


Fig 13: Contrast Stretching($c=2$)



Fig 17: Edge Detection

Table 1: Parameters of the results obtained from
FPGA



Fig 14: Intensity level Slicing



Fig 15: Gamma Correction ($\text{gamma}=2$)

S no	Parameters	Brightness enhancement	Brightness suppression	Contrast Stretching	Intensity-level Slicing	Gamma Correction	Logarithmic Transformation	Thresholding Image	Image Negative	Edge Detection
1	SC	0.33	9.50	0.36	1.00	0.13	482.61	1.45	4.74	6497
2	MSE	58.43	54.01	10.11	13.13	71.09	75.93	1.32	16960	61.12
3	PSNR(dB)	29.77	30.89	39.08	34.48	29.69	33.32	38.92	3.02	39.19
4	NCC	1.74	0.22	1.04	0.82	1.46	0.02	0.77	0.04	0.09
5	AD	0.71	0.63	0.38	0.04	0.53	0.24	0.12	0.56	0.48
6	MD	75.88	99.99	66.92	173.93	168.43	251.11	96.36	255	173.38
7	NAE	0.39	0.63	0.36	0.49	1.44	0.90	0.32	1.41	1.00

VI. Conclusion

The main aim of this work is to exhibit the utilization of Xilinx Platform Studio for actualizing the computerized picture preparing calculations on a FPGA. The Xilinx Platform Studio apparatus is an application in picture handling, and offers a well-disposed condition structure for the preparing, in light of the fact that the channels are planned by C/C++ codes. This apparatus bolster programming reproduction. However, orchestrate of FPGA is the most important aspect for parallelism, speed and

powerful. The picture preparing is the basic process of picture. Hence, this work explained image enhancement techniques such as edge detection, image brightness and image negative. The quality of image extended by following methods such as Image logarithmic transformation, Image Contrast Stretching, Image thresholding, gamma correction and Intensity level slicing.

VII. Future Scope

The future extent of this venture is to actualize progressively complex picture preparing calculations. Range Highlighting Transformation, Parabola change, and so forth. Additionally in our paper we utilized leading body of 50MHz, consequently by expanding the clock frequency of the load up we have the extent of speeding up utilized alongside increasingly productive elite calculations and diminished cost cuttings. Also we can introduce parallel communication which increases the speed to the maximum possible extent.

References

- [1] Uk, Ijeacs. (2017). A Review on Image Enhancement Techniques. International Journal of Engineering and Applied Computer Science (IJEACS). 02. 232-235. 10.24032/ijeacs/0207/05.
- [2] Rahman, Shanto& Rahman, Md. Mostafijur& Shah, Khaled &Shoyaib, Mohammad. (2014). Image Enhancement in Spatial Domain: A Comprehensive Study. 2014 17th International Conference on Computer and Information Technology, ICCIT 2014. 10.1109/ICCITechn.2014.7073123.
- [3] N. Kehtarnavaz and S. Mahotra, "FPGA implementation made easy for applied digital signal processing courses," Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on, vol., no., pp.2892-2895, 22-27 May 2011.
- [4] Mohammed Alareqi1, Rachid Elgouri1, Khalid Mateur and LaamariHlou, "Real Time Hardware Co-Simulation for Image Processing Algorithms Using Xilinx System Generator", International Journal on Electrical Engineering and Informatics - Volume 7, Number 4, Desember 2015.
- [5] Zuloaga, J.L. Martin, U. Bidarte, J.A. Ezquerra - "VHDL test bench for digital image processing systems using a new image format", ECSI, 2007.
- [6] Mandeep Singh Narula and NishantSingla, "FPGA Implementation of Image Enhancement Using Verilog HDL", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 05 Issue: 05| May-2018.
- [7] Deepthi, V & Prasad, Surya. (2016). Medical Image Fusion using Xilinx System Generator in FPGA. International journal of VLSI system design and communication systems. 0410. 990-993.
- [8] E. A. B. da Silva,E. Andreas and C. L. Pagliari .Multiscale image fusion using the undecimated wavelet transform with spectral factor-ization and nonorthogonal filter banks[J]. IEEE Trans. Image Process, vol. 22, no. 3, pp. 1005–1017, Mar. 2013.
- [9] Ankita gupta , HimanshuVaishnav and Himanshu Garg, " Image Processing using Xilinx System Generator (XSG) in FPGA", Volume II, Issue IX, September 2015 IJRSI ISSN 2321 – 2705.
- [10] T. Saidani, D. Dia, W. Elhamzi, M. Atri and R.Tourki, "Hardware Co-simulation for Video Processing Using Xilinx System Generator," Proceedings of the World Congress on Engineering, vol.1, Jun 2009. London, U.K
- [11] Alba M. Sánchez G., Ricardo Alvarez G., Sully Sánchez G.; FCC and FCE BUAP, "Architecture for filtering images using Xilinx System Generator", INTERNATIONAL JOURNAL of MATHEMATICS AND COMPUTERS.
- [12] Matthew Ownby and Dr. Wagdy H. Mahmoud, "A Design Methodology for Implementing DSP with Xilinx System Generator for Matlab", Proceedings of the IEEE, vol.1, Jun 2009. London, U.K.
- [13] Raman Maini and Himanshu Aggarwal, "A Comprehensive Review of Image Enhancement Techniques", JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, MARCH 2010, ISSN 2151-9617.
- [14] S. M. Pizer, et al., "Adaptive Histogram Equalization and its Variations," Comput. Vision, Graphics and Image Processing, Vol. 39, pp. 355-368, 1987.
- [15] N. Kehtarnavaz and S. Mahotra, "FPGA IMPLEMENTATION MADE EASY FOR APPLIED DIGITAL SIGNAL PROCESSING COURSES", Department of Electrical Engineering, University of Texas at Dallas, Richardson, TX 75080, USA.
- [16] VarshaS.Surwase and S.N.Pawar "Vlsi implementation of image processing algorithms on fpga", IJEEE volume 3, number 3 (2010), pp. 139-145.
- [17] B.Muralikrishna, G.L.Madhumati, Habibulla Khan, K.GnanaDeepika, "Reconfigurable Edge Detection Processor Using Xilinx Platform Studio", 2014 2nd International Conference on Devices, Circuits and Systems (ICDCS).
- [18] Ostu N.A. Threshold Selection Method from Gray – Level Histograms. IEEE Trans on Systems. Man and Cybernetics, SMC - 9, 1979, 9(1):62-66FLEX Chip Signal Processor (MC68175/D), Motorola, 1996.

Trust Computational Methodology for an Internet of Things

M Rajendra Prasad

Department of ECE

Vidya Jyothi Institute of Technology
Hyderabad-500075, India
rajendraresearch@gmail.com

D.Krishna Reddy

Department of ECE

Chaitanya Bharathi Institute of Technology
Hyderabad-500075, India
dkreddy@cbit.ac.in

Abstract: The immense growth of Internet of Things (IoT) and it is widely effecting our daily lives. In IoT based applications security, privacy and trust plays a vital role of implementation of IoT. To enhance security and trust for an IoT a novel Trust Computational Methodology (TCM) for Internet of Things is developed to evaluate and analyze the customized hardware system performance on Unix/Linux/POSIX operating systems targeted for any wireless applications. It is also used to investigate various issues related to hardware and firmware of an IoT device. This paper describes the execution of TCM to improve the network performance of packet transmission and reception of Power PC based IoT (PPC_IoT) device also presents the detailed process of packet capturing and optimizing technique to transmit/receive packets in the results. For low budgetary benefit of transmission and reception channel path cost, PPC_IoT is designed which is a compact indoor base station used for high-density multi-band base stations that accommodate IP transmission lines. There are many issues involved in the development of an IoT based computing platform for PPC_IoT such as packet loss in transmission & reception, the time interval between 2 consecutive uplink/downlink timeslot packets. TCM not only increases the system level performance but also helps to meet the telecom application constraints.

Keywords: Mobile Station, Time Slot Packets, Trust Computational Methodology, Internet of Things, Power PC

I. Introduction

Trust Computational Methodology is considered as an efficient methodology to tackle the complexity of modern IoT devices for wireless or telecom application design. The firmware running on dedicated hardware is gaining attention as it addresses the augmenting need for feature-rich solutions. Hence, integrating embedded software and co-simulation into a low level system design flow is desirable. It is becoming challenging to design a computing platform for IP based IoT applications due to their complex requirements and design specifications. Many of such wireless applications running on dedicated hardware have great effect on the performance of their underlying computing systems. Studies based on general features of such

embedded telecom computing systems and design of an appropriate architecture for a given telecom application have therefore become an extensive research area. In this paper TCM is applied for a case study wireless application running on IoT to evaluate system level performance. It also explains how to improve system level performance if it is not matching the system level parameters like packet loss. IoT system for mobile applications is the recent and upcoming field of Electronics and Communication Engineering domain. The whole concept of IoT system arises for real-time wireless applications that are computationally intensive like wireless sensor network nodes are slow and do not meet the real time processing constraints in a processor based IoT based platform. Such an wireless application running on IoT nodes can be speeded up by executing it on a customized IoT system, but at the same time cost factor also increases. So, an intermediate approach is taken in which a part of application is executed in software and hardware is synthesized for the other part.

II. Related Work & Literature Review

The concept of trust and its management for Internet of Things has been assessed and addressed by many researchers in geographical areas. J. Lopez, R. Roman, I. Agudo and C. Gago presented best practices which are essential for developing a good trust management system for Wireless Sensor Node [1]. Performance analysis and improvement of trustworthiness of an IoT node plays a vital role for telecom application developers for IoT devices to identify early issues. Metropolis is a system-level design framework based on the principles of IoT platform-based design from UC Berkeley. F. Balarin and his team described the toolset to develop an IoT device simulation and analysis [2]. The Compaan approach is developed by Leiden University, NL, and the input of the design flow is synthesized as hardware and software for IoT . T. Stefanov, C. Zissulescu, A. Turjan, B. Kienhuis, and E. Deprettere presented an efficient system design approach based on programming problem [2]. Andreas Gerstlauer, Christian Haubelt , Andy D. Pimentel , Todor P. Stefanov , Daniel D. Gajski , JÜrgen Teic developed and proposed a novel classification for electronic system level synthesis tool [3]. Zhuosheng & Simin presented a technique for a chaotic map-based real time performance of secured video communication system using ARM processor based IoT [4]. Y. Jiang,

H.Zhang & Z.Li developed a frame work to design a control system to capture the behavior of multi clocked embedded systems [5]. M.Rajendra & D.Krishna described a methodology that deals with a powerful micro benchmarks are used to evaluate latency and bandwidth measurements for IoT nodes in the realtime. This methodology is also used to characterize the early system performance of the IoT processor board and Real Time Operating System (RTOS) on of ARM920T processor [6]. This paper describes TCM to investigate the system performance related issue identification and its solution. This methodology used to analyze the system level performance of packet transmission and reception as case study of IoT application running on Power PC known as PPC_IoT.

III. Trust Computational Methodology

Trust Computational Methodology (TCM) for Internet of Things for any telecom application is shown in the figure 1 . This paper describes the implementation procedure for TCM which decreases the complexities, motivates the usage of high-level system design approaches such as System Level Design tools and methodologies. Trust Computational Methodology is a promising solution to meet constraints for telecom application designers at early stage of implementation [13][14].

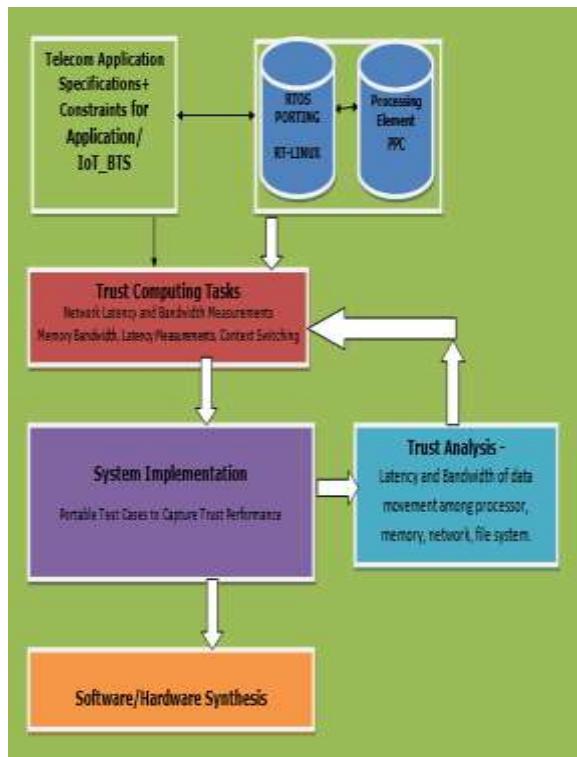


Fig 1: Trust Computing Methodology

The main concept of TCM is to reduce design complexity by modeling systems at a high

abstraction level, i.e., at system level. A powerful and enhanced performance of micro benchmarks automated tool is developed to evaluate latency and bandwidth measurements for IoT systems in an experiment with the results [15] [16]. As a result after applying this methodology MPC 8548E processor is selected to implement Internet Protocol based Base Transceiver Station (BTS) know as IoT_BTS application. This paper focuses on the performance improvement of IoT_BTS application on MPC 8548E processor board. It contains an embedded processor which executes the software partner's access point. This product also includes various digital, RF, and analog hardware. A basic block diagram is shown in figure 2. The core computing part of the IoT_BTS is MPC 8548E Processor Board which is known as embedded processor which is also depicted in the figure 2. The processor board consists of MPC8548E PowerPC Processor 1.3GHz from Freescale with DDR, two flash banks and SDRAM for storage and two 10/100M Ethernet RJ-45 (DM9000) for communication interfaces connected to A field-programmable gate array (FPGA). IoT_BTS application comprises different software modules and it is responsible for channel encoding/decoding, multiplexing/de-multiplexing, call establishment, speech communication through full rate speech channel, transmission of speech through Real-Time Protocols (RTP) to support short circuited call, transmission & signaling over TCP/IP on Abis interface. IoT_BTS software provides the physical connection of a Mobile Station (MS) to the network in the form of Air-interface.

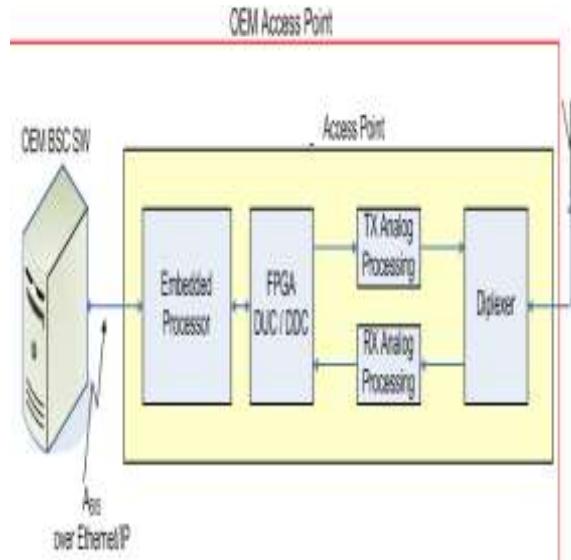


Fig 2: Block Diagram of IoT_BTS

On the other side Base Transceiver Station (BTS) is connected to Base Station Controller (BSC) via the Abis-interface. The software part of IoT_BTS consists of the following protocols and modules as shown in the figure 3.

These protocols can be viewed as independent layers, each performing different functions. IoT_BTS Controller will be responsible for IoT_BTS startup, over all controlling and monitoring of complete IOT_BTS and IoT_BTS shutdown. The overall architecture of the IOT_BTS Software Block and inter layer and component communication is as shown in figure 3. This module is responsible for startup and initialization of all the layers in coordination with OAM module. It will be the first task created after the operating system is up. It will then start and initialize other layers and components to bring up the complete IoT_BTS. Before implementation of IoT_BTS Software block the proposed TCM is applied to investigate issues related to IoT_BTS application on different processor boards.

The input specification of IoT_BTS application for wireless sensor network nodes only describes the overall functionality of the designed system and includes the imposed constraints like timing, power consumption, cost of network requirements. Starting from such a telecom application system for WSN node specification, the proposed research work supports the automatic and interactive exploration or customization of a large design space which leads to high performance and cost effective IoT solutions for IoT nodes [8][9]. Thus, the proposed research work benefits IoT telecom application developers and designers. By analyzing the system level performance of these IoT platforms at the early stages, a WSN developer can decide which processor board is suitable for their IoT applications for WSN nodes. Telecom application developer can reduce the time and cost by investigating the performance of processor boards and by increasing the performance quality of IoT system testing for different telecom applications using this Methodology. An experiment with the three processor boards comprises of MPC 8548E, ARM920T and ARM1176JZF-S is set up and technical approach of the experiment is depicted to evaluate and analyze the performance of these IoT boards known as WSN nodes for IoT networks as depicted in the figure 3 and the technical specifications of these processor boards are listed in figure 4. The MPC8548E is a networking/telecom processor and an ideal choice for enhancing and implementing security protocol and it is processing in 2.5G/3G/4G/5G wireless sensor network nodes. [9][10][11]. Samsung's S3C2440 is a 32-bit ARM based mobile application processor that has been widely used for wireless Sensor Network node implementation such as 2.5G/3G baseband stations and used as Bluetooth equipment for its high performance [10] [24]. Raspberry pi is an ARM1176JZ core processor incredibly small single-board linux computing system targeted for cellular

networking connectivity and executing a wireless sensor networking application on the board [10].

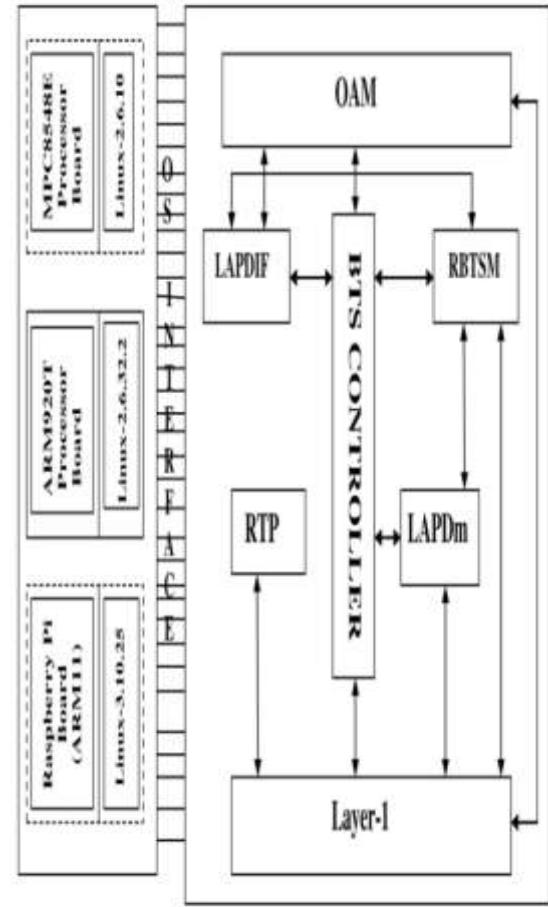


Fig 3: Block Diagram of IoT_BTS

	MPC 8548E	ARM920T	Raspberry Pi
CPU	Freescale MPC8548E PowerPC Processor 1.3GHz	Samsung S3C2440 arm920t 405MHz With 3.5 inch touch screen LCD	700 MHz ARM1176JZ F-S (ARM11 family, ARMv6 instruction set)
Memory	DDR2- 256 MB BootFlash-32 MB UserFlash-32 MB 2 serial EEPROMS.	SDRAM- 64MB, 1GB of NAND flash and 2 MB of NOR flash with BIOS, one SD card socket.	SDRAM- 256 MB or 512 MB (shared with GPU), onboard memory storage- SD/MMC- slot.
Ethernet	Two 10/100 Ethernet ports	10/100M Ethernet RJ- 45 (DM9000)	10/100 Mbit/s Ethernet (8P8C) USB adapter on the third port of the USB hub
Operating System	Linux-2.6.10	Linux- 2.6.32.2	Linux- 3.10.25

Fig 4: Customized Processor Boards Specifications

Highest level linux kernel versions of operating systems supported by the three boards are selected and are successfully transplanted and tested [12] [24].

A. Hardware specifications of MPC8548E Processor Board:

- The customized hardware comprises to assembly with MPC8548E PowerPC processor from free scale and it is adjustable to MPC8548E and MPC8543E processors.
- The custom board has two serial EPROMS as Board ID EEPROM and Boot sequencer EEPROM.
- It has a DDR-2 SODIM slot which can fit standard DDR-SODIMM memory modules for multiple vendors.
- It consists of 256MB on board memory.
- The serial EEPROMs are 8KB and are connected through the processor I2C bus.

B. Software Design Modules of IoT_BTS

- **IoT_BTS Controller:** This module is responsible for startup and initialization of all the software layers in coordination with OAM module. It will be the first task to create after the operating system is booted up. Then it will start the other layers and components to bring up the complete IoT_BTS.
- **OAM:** OAM acknowledges its creation and informs IoT_BTS Controller about its denying of software download request from BSC. It also indicates to IOT_BTS Controller that the new software downloaded is saved in the flash memory. OAM sends configuration parameter to IoT_BTS Controller, and also sends reset request to IoT_BTS Controller. IoT_BTS Controller indicates the initialization of all the layers to OAM. IoT_BTS Controller confirms the shutdown of all the layers to OAM and indicates error information through OAM.
- **LAPDm:** It performs the establishment of data links on a Dm channel and information transfer is unacknowledged with window size equal to 1. Segmentation and reassembly of Layer 3 message is in the acknowledged mode, the length exceeds the maximum number of octets in the information field of a frame.
- **LAPDIF:** This layer is responsible for transmission and reception of radio signaling messages, OAM messages and RTP Request/Response messages across A-bis interface. The main tasks performed by this layer are: Transmission and reception of

OAM messages on OML using TCP/IP and Transmission and reception of radio signaling messages using TCP/IP. Transmission and reception of RTP signaling messages over RTP Request/Response socket using TCP/IP.

- **RTP:** This module is responsible for transmission and reception of RTP packets containing TRAU frames across A-bis interface. RTP functionality will run under Layer 1 task [16][23].
- **Linux 2.6.10 Operating System Interface:** The OS interface module provides various packages to build images of u-boot, kernel and ram disk file system that are to be supported on processor board to boot along with IoT_BTS software and other modules. [17].
- **Boot Loader:** U-boot is used as a boot loader to transplant operating system images and application software on to flash memory.
- **Layer 1:** Layer 1 is the physical layer in the IOT_BTS GSM protocol architecture and represents the functions necessary to transfer bit stream data on the air interface. It includes functions such as channel coding/decoding, interleaving/de-interleaving, burst mapping/de-mapping and measurement functions such as transmission/reception of raw packets. The raw socket packets will contain the Trx configuration data, network data (signalling or speech) and IoT_BTS testing data. FPGA will send the packets to Layer 1 at each timeslot interval. There are different types of packets that are defined for various purposes. To perform this task, Layer 1 will transmit the Register Write Command packet. This packet contains the configuration/non-gsm (control/status) data along the register address on which this data will write onto FPGA[17].

This paper describes the on Layer1 issues that are improved by the TCM as shown in the figure 1. The packet type will indicate Register Write/Read Command as shown in the figure 5. The Write Address field contains the Register Address, Data field contains configuration/non-gsm (control/status) data. FPGA sends response of each received packets from Layer 1, with modified source and destination address, copy of the Tag field, R bit set and any error flags. Rest of the fields will be same as in the received packets. In order to handle the lost Register packet, retry mechanism will be used [18][19][25]. There will be no retry mechanism for Timeslot packets. The Layer 1 communicates with FPGA through raw socket over Ethernet. The raw socket is created during the Layer 1 startup.

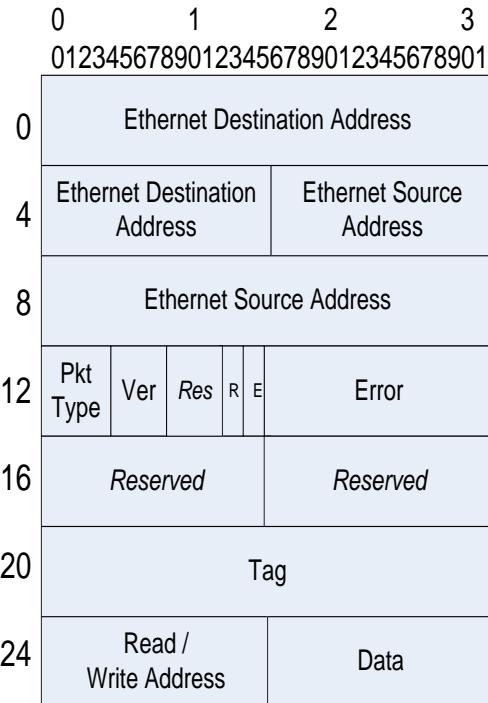


Fig 5: Packet format of Register Write/ Read Command

Reception of non-GSM data from FPGA refers to control/status data. For extracting any data from FPGA, Layer 1 will send Register Read Command packet. GSM data refers to network signaling/speech. Timeslot packets format will be used for transferring network data as shown in the figure 6[20].

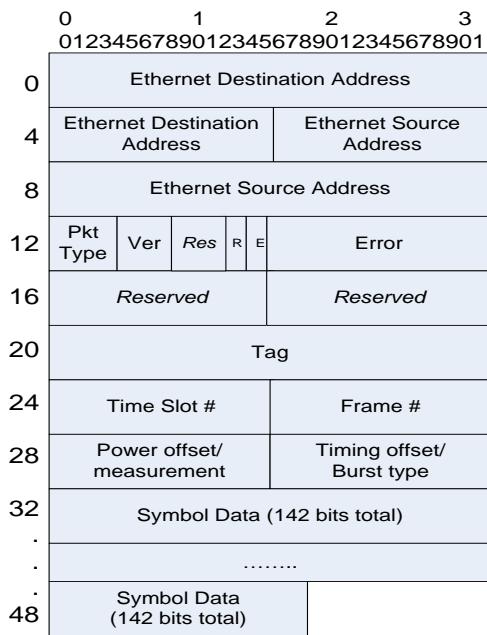


Fig 6: Packet format of Timeslot Packet

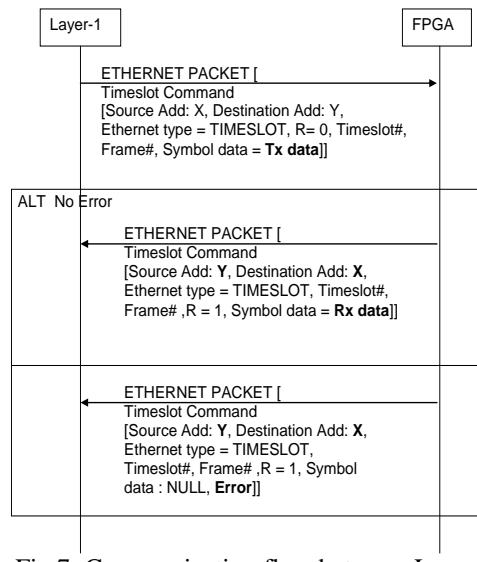


Fig 7: Communication flow between Layer1 and FPGA

The communication flow between Layer1 and FPGA is described in figure 7. The packets contain the description of timeslot, frame number and power offset. Symbol data will contain the burst data which will be transmitted over air interface [21].

IV. Results and Discussions

TCM is implemented and applied to analyze the performance of three IoT platforms whose technical specifications are described in the previous sections are evaluated by an system level automated tool [22].

MPC8548E	ARM920T	Raspberry Pi(ARM11)
Sample syscall: 0.2011 microseconds	Sample syscall: 0.3011 microseconds	Sample syscall: 0.4900 microseconds
Sample read: 0.3013 microseconds	Sample read: 1.8303 microseconds	Sample read: 1.0281 microseconds
Sample write: 1.3221 microseconds	Sample write: 1.5568 microseconds	Sample write: 1.0741 microseconds
Sample stat: 1.3272 microseconds	Sample stat: 18.4819 microseconds	Sample stat: 1.2634 microseconds
Sample fstat: 0.7364 microseconds	Sample fstat: 4.1817 microseconds	Sample fstat: 1.5791 microseconds
Sample open/close: 2.3649 microseconds	Sample open/close: 26.9803 microseconds	Sample open/close: 15.2151 microseconds
Select on 10 Gb/s: 1.7766 microseconds	Select on 10 Gb/s: 6.4029 microseconds	Select on 10 Gb/s: 3.4004 microseconds
Select on 100 Mb/s: 8.8091 microseconds	Select on 100 Mb/s: 45.7514 microseconds	Select on 100 Mb/s: 14.5254 microseconds
Select on 250 Mb/s: 21.3750 microseconds	Select on 250 Mb/s: 101.3969 microseconds	Select on 250 Mb/s: 33.8037 microseconds
Select on 500 Mb/s: 41.3946 microseconds	Select on 500 Mb/s: 251.1038 microseconds	Select on 500 Mb/s: 66.9654 microseconds
Signal handler installation: 0.8074 microseconds	Signal handler installation: 1.4564 microseconds	Signal handler installation: 1.3222 microseconds
Signal handler overhead: 3.2036 microseconds	Signal handler overhead: 12.4493 microseconds	Signal handler overhead: 8.1478 microseconds
Protection fault: 0.0882 microseconds	Protection fault: 2.6942 microseconds	Protection fault: 0.9127 microseconds
Pipe latency: 4.5429 microseconds	Pipe latency: 381.5772 microseconds	Pipe latency: 42.3736 microseconds
AF_UNIX socket latency: 8.0043 microseconds	AF_UNIX socket latency: 1041.0791 microseconds	AF_UNIX socket latency: 69.4000 microseconds
Process fork+exit: 108.1379 microseconds	Process fork+exit: 1009.5519 microseconds	Process fork+exit: 2247.6667 microseconds
Process fork+execve: 371.2857 microseconds	Process fork+execve: 6388.0000 microseconds	Process fork+execve: 6388.0000 microseconds
Process fork+bind < 2502.3333 microseconds	Process fork+bind < 2779.9256 microseconds	Process fork+bind < 1447.0000 microseconds
Process fork+bind > 2502.3333 microseconds	Process fork+bind > 56117.5889 microseconds	Process fork+bind > 1447.0000 microseconds

Fig 8: System level Latency measurement values.

Fig 9: Simple system level function latency measurements.

Table 1 Test Cases for Time slot Packet Issues

The latency measurement values of system calls, signal handler installation & overhead, stream socket latencies processes latency values are evaluated as shown in the figure 8 and graphically described in figure 9. After analyzing the system level values, MPC 8548E is suitable for IoT_BTS application. The behavior with respect to system level parameters are evaluated by using TCM and IOT_BTS network radio interface is tested by connecting a serial cable from the PowerPC based target system board to the serial port of the linux host system. By using TCM, as described in the figure 1, is applied to test whether constraints are matching according to the requirement of network telecom applications. Using this methodology, the performance of IoT_BTS is receiving the packets at constant rate 600 micro sec and some time the packet arrives at 1100 us [23] [25]. This is not matching our requirement defined in the specifications of IoT_BTS. This improvement technique is also included in the TCM and its computational algorithm is shown in the figure 10 [26]. Time stamp measurement of packet arrival rate from FPGA to layer1 is measured using Oscilloscope with Test1 and Test2 as shown in the Table 1[28].

To improve the performance, the dependency code for the number of packets to be handled in one call poll function (gfar_poll) in linux2.6.10 kernel source (This is the highest kernel source code supportive for customized board) is identified in gianfar.h and gianfar.c.

A. Identification of dependent code in kernel source for Performance Improvement of eTSEC (enhanced Three Speed Ethernet Controllers)

These two files describe the device driver for the Triple Speed Ethernet Controllers (TSeC) on the Free Scale 8540/8560 integrated processors as well as the Fast Ethernet Controller on the 8540 used as an IoT nodes .Interrupt coalescing is a feature implemented in IoT boards or custom-boards which allows a reception of a group of network frames to be notified to the operating system kernel via a single hardware interrupt, thus reducing the interrupt processing overhead, particularly at high packet rates in IoT application packet processing mechanism. However, the delays introduced by interrupt coalescing can result in significant TCP throughput degradation. To avoid degradation of packets we have customized device driver code. Poll function (gfar_poll) is modified according to our requirements and to handle all packets within the 577us as shown in the figure 11. The above changes are made

accordance with the kernel source code, a new kernel image is built and flashed on custom processor board and booted successfully. After performing Test1, Test2 and Test 3 as specified at table 1, we conducted the test for Network detection at Mobile with modified kernel image and we are able to see network 12345. Simultaneously we probed the Ethernet MAC PHY using Oscilloscope at FPGA, both downlink and uplink are at 577 us as shown in the figure 11 [29].

Table1: Test cases for packet time slot packet issues

Test1	Ethernet packets were sent from FPGA stub at rate of 1ms. Time stamping is logged at Layer1.
Result1	Consecutive packets are received at a time gap of 8090 us and 3rd packet is received after 2ms.
Observation 1	<ol style="list-style-type: none"> OS is generating an interrupt after 2 Ethernet packets are received. Due to this buffering at OS, Layer1 receives 2 packets with time gap of 8090us and a third packet is received after 2ms and after 4 ms. It seems, not to be a packet processing issue at OS. If it had been a processing issue, by slowing down the packet rate, packets should have been received at 1ms.
Test2	Ethernet packets were sent from FPGA stub at a rate of 2ms. Time stamping is logged at Layer1.
Result2	All consecutive packets are received at constant time gap of 2ms.
Observation 2	As per understanding, the triggering of received packets at OS is governed by the timeout of Ethernet specific timers.
Test3	Layer1 stub without logging was used to verify the uplink and downlink timeout of packet timings using Oscilloscope.
Observation 3	The time interval between 2 consecutive uplink timeslot packets is 577us as measured at the Oscilloscope. The time interval between 2 consecutive downlink timeslot packets is 577us as measured at the Oscilloscope.
Observation 3	The packet timing for both uplink and downlink is 577us. Oscilloscope images are captured at both RX_DV and TX_EN pin of Ethernet MAC PHY of RF/FPGA board and MPC8548 board.

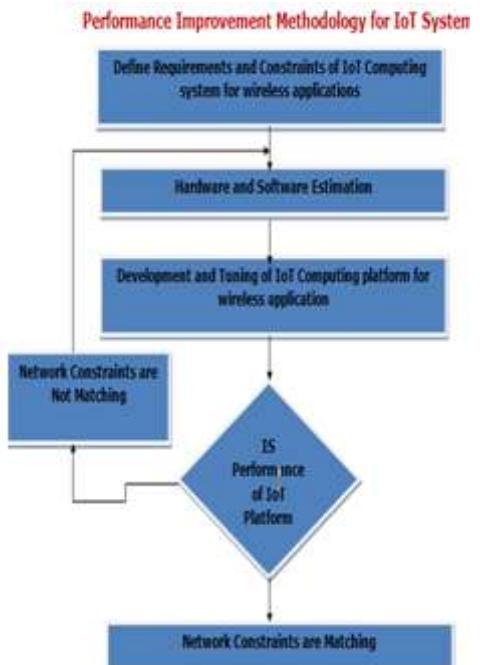


Fig 10: Performance Improvement Technique using TCM

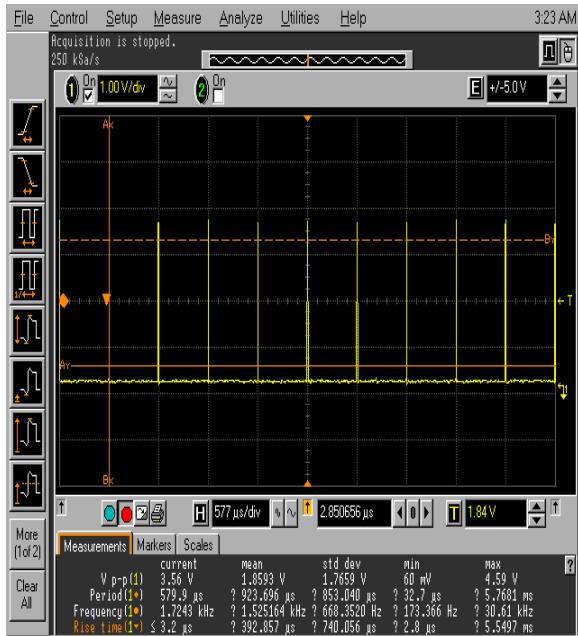


Fig 11: Oscilloscope time interval values 2 consecutive uplink/downlink packets.

V. Conclusion

In this paper a Trust Computing Methodology is developed to analyze the performance of IoT based computing platform and compared with the required specifications or constraints are matching for IoT_BTS telecom application. If the performance related to telecom requirements and constraints are not matching, a TCM is applied with case study results are discussed. This paper also discussed the procedure to identify and resolving the issues related to mismatch of requirements and constraints. By this way we can improve the performance of IoT computing system as per our specifications or requirements. From the results, PowerPC processor based IoT system is developed from the scratch and we can apply this methodology to any telecom applications to tune the performance as per the specifications at very beginning stages. This methodology is very much useful for telecom application developer to find out and fix the different problems at the early stages of the application.

VI. Acknowledgment

We would like to thank Principal and Director of Vidya Jyothi Institute of Technology for their continuous support in publishing this paper.

References

- [1] J. Lopez, R. Roman, I. Agudo, C. Fernandez-Gago, “Trust management systems for wireless sensor networks: Best practices”, Computer Communications , pp 1086-1093, 2010.
- [2] F. Balarin, Y. Watanabe, H. Hsieh, L. Lavagno, C. Passerone, and A. Sangiovanni-Vincentelli. Metropolis: An Integrated Electronic System Design Environment. Computer, pages 45-52, 2003.
- [3] T. Stefanov, C. Zissulescu, A. Turjan, B. Kienhuis, and E. Deprettere. System Design Using Kahn Process Networks: The Compaan/Laura Approach. In Proceedings of the Conference on Design, Automation and Test in Europe (DATE'04), pages 340-345, 2004.
- [4] A. Gerstlauer, C. Haubelt , A.Pimentel , T.Stefanov , D. Gajski , J.Teic, “Electronic System-Level Synthesis Methodologies”, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Volume:28 , Issue: 10 ,Page(s): 1517 – 1530, 2009.
- [5] Z.Lin, S.Yu, J.L'u, , S.Cai, and G.Chen, “Design and ARM-EMBEDDED Implementation of A Chaotic Map-Based Real-Time Secure Video Communication System”, IEEE Transactions on circuits and systems for video technology,pp.1203-1216,2015.
- [6] Y.Jiang, H.Zhang, Z. Li, Yangdong Deng, Xiaoyu Song, MingGu, and Jiaguang Sun Design and “Optimization of Multi clocked Embedded Systems Using Formal Techniques” IEEE Transactions on industrial electronics, Vol. 62, NO. 2, pp..1270-1278, 2015.
- [7] M.R.Prasad, D.K.Reddy, A.Sindhija, G.Sravanti, “Performance analysis of ARM Processor Based Embedded System for Telecom Application”, Technology Spectrum, Journal of JNTU Hyderabad, pp.82-89,, ISSN:0974-6854, August 2014.
- [8] M.R.Prasad,D.K.Reddy”Development of System Level Computational Platform for IP-BTS Telecom Application” IEEE International Advance Computing Conference (IACC-2017).
- [9] J.Sun, F.Zou, S.Fan, “A token-ring-like real-time response algorithm of Modbus/TCP message based on μC/OS-II”, International Journal of Electronics and Communications (Elsevier), 2016,
- [10] S.Y.Shin, “Throughput analysis of IEEE 802.15.4 network under IEEE 802.11 network interference”, International Journal of Electronics and Communications (Elsevier), 2013.
- [11] M.R.Prasad , S.R.Reddy, V.Sridhar, “Framework to port linux kernel on PowerPC based embedded system used for telecom application – IPBTS,” International Journal of Software Engineering & Applications(IJSEA), vol. 2, no.4, pp. 127-139, 2011.
- [12] F.Bohr.“Model Based Statistical Testing of Embedded Systems,” IEEE Fourth International Conference on Software Testing, Verification and Validation Workshops, pp. 18-25, 2011.
- [13] S.Wang, G.Duan, “On the characterization and optimization of system-level vulnerability for instruction caches in embedded processors”, International Journal of Microprocessors and Microsystems (Elsevier), 2015.
- [14] S. Gal-On,M. Levy, “Measuring Multi Core Performance,” Computer, IEEE Computer Society, Vol. 41, Issue 11, pp. 99-102, 2008.
- [15] M.H.Jamal,G.Mustafa,A.Waheed,W.Mahmood,“An extensible infrastructure for benchmarking Multi-core Processors based systems,” Performance Evaluation of Computer and Telecommunication Systems, Vol. 41, pp. 13-20, July 2009.

- [16] M.R.Prasad, D.K.Reddy, “Design Methodology for IP secured Tunnel Based Embedded Platform for AAA Server” International Journal of Mobile Network Communications & Telematics (IJMNCT) Vol. 3, No.6,pp. 49-60,2013
- [17] J. Chen, “A new design of Embedded IPv4/IPv6 dual stack protocol”, International conference on network computing and information security(NCIS), vol.2, pp.163-167, 2011.
- [18] A.En-Nouary, F.Khendek, R.Dssouli. “Testing Embedded Real-Time Computing Systems,”Seventh International Conference on Real-Time Systems and Applications (RTCSA), pp. 417-424, 2000.
- [19] A.Sung and B.Chi. “An Interaction Testing Technique between Hardware and Software in Embedded Systems,” Software Engineering Confererence,Ninth Asia-Pacific, pp. 457-464, 2002.
- [20] C.Sachin, G.Talmale, “The Design and Development of low cost Voip device Using Linux,” International Journal of Engineering Research and Applications, pp. 96-98, 2014.
- [21] S.Yanpeng, P. Peng, Z.Yuan, “ Linux Transplantation Based on The Processor S3C2440,” in the nineth International Conference on Electronic Measurement & Instruments, pp. 2-306-2.309, 2009.
- [22] J.Park, J.Jun, and B.Chi, “ IoT Convergence Research Department, Electronics and Telecommunications Research Institute, 218 Gajeong-ro, Yuseong-gu, Daejeon, Korea ,“A Method of connecting battery less devices to the IP networks”, pg:22-27, 978-1-4799-6786-5/14/\$31.00 ©2014 IEEE
- [23] A.Rawoof, K.C.Ray,“ARM based implementation of Text-To-Speech (TTS) for real time Embedded System”, p.192-196, 2013
- [24] V.Prashant, Joshi, “Analysing and Improving the Performance of SoftwareCode for Real Time Embedded Systems”, IEEE conference on Devices, Circuits and Systems (ICDCS), p.1-5, 2014
- [25] G.Wang,X. Xuan “Design and Implementation of an Embedded Router with Packet Filtering”, IEEE Symposium on Electrical & Electronics Engineering (EEESYM), IEEE ,p.285-288, 2012
- [26] H.T. Ngo, R.W.Ives, R.N. Rakvic, R. P. Broussard, “Real-time video surveillance on an embedded, programmable platform”, International Journal of Microprocessors and Microsystems (Elsevier), 2013.

A Prototype Wi-Fi Controlled Car using NodeMCU

T. Satya Sai Kiran

ECE, Chaitanya Bharathi Institute of Technology,
Hyderabad-500075, India,
tskiran13@gmail.com

Abstract: In this paper, we developed a remote-controlled car using the latest IoT modules. Low cost IoT modules are popular in terms of availability and re-programmability. This paper focused on hardware and software requirements for developing the remote-controlled car with low-cost modules. The developed prototype embedded car is useful for several research applications like data collection in long corridor or indoor/office smooth surface environments.

Keywords: IoT, NodeMCU ESP8266, Wi-Fi Car

I. Introduction

In recent years, the applications of developing remote controlled cars are one of the popular toy products in the market[1]. To draw the research results from traditional remote-controlled cars like using single chip microcomputer is not possible. Because of not having storage capabilities and data computation facilities. In order to develop scientific attention, the remote-controlled car could be used for more realistic problems, such as distance measurement, data collection for indoor channel modeling, hospitals ventilation monitoring etc., Internet of Things is the latest emerging internet technology and has got its origin from home automation. The basic difference between standard home automation devices and IoT devices is that the IoT devices can transfer and share data over the existing network framework. Also, IoT devices are capable of being controlled remotely over the internet [2]. In the recent days, applications like developing Wi-Fi based smart car for toxic gas monitoring in large-scale petrochemical plants (Shu et al., 2015), and data collection of various environments plants in industries (Zhiqiang et al., 2015) are coming. In this paper, we used NodeMCU ESP8266 Wi-Fi transceiver for the purpose of distance measuring for data collection applications. Similar kind of prototype module is developed by wang et al., (2014) with Arduino microcontroller using Bluetooth system.

II. Prototype Design and Development

The overall developed work consists of user with a smart phone, NodeMCU ESP 8266, L298N Motor Driver and Dual Shaft DC Motors and wheels. A program is developed in Arduino Integrated Development Environment (IDE) and is installed in Node Microcontroller Unit (Node MCU) to receive

T. Sridher

ECE,Chaitanya Bharathi Institute of Technology,
Hyderabad-500075, India,
tsridhar_ece@cbit.ac.in

the controls from the smart phone. Later on, Node MCU sends corresponding digital signal to the motor driver module (L298N) for smooth functioning of the car in different directions. The technical specifications of NodeMCU and L298N Motor Driver are presented in Table I and II.

Table I: Specifications of NodeMCU

S. No	Parameter	Value
1.	Input Voltage	3.3V
2.	Digital Input/Output Pins	16
3.	ADC Pin	1
4.	Flash Memory	4MB

The required supply voltage for NodeMCU is 3.3V, giving from externally Lithium-Ion Batteries of 3 no's each one of rating 4V. Therefore, nearly the remote car could be operated up to 2 hours continuously. The pin configuration of NodeMCU is shown in Fig.1[5].



Fig 1: NodeMCU ESP8266 module

Table II: Specifications of L298N Motor Driver

S. No	Parameter	Value
1.	Motor Supply voltage	5V
2.	Motor Supply Current	2A
3.	Maximum Power	25W
4.	Logic Voltage	5V
5.	Logic Current	0-36mA

The L298N is a dual-channel H- Bridge motor driver capable of driving a pair of DC motors. It can control both speed and spinning direction of four tyres of car.

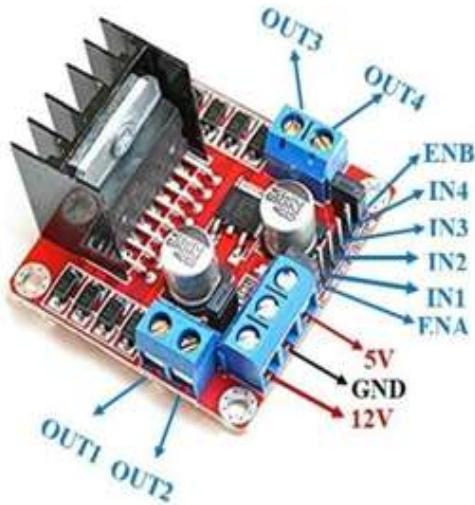


Fig 2: Motor Driver controls tyres direction

We install our own developed matLAB into Arduino IDE Software and installed into the NodeMCU. The connections for developed prototype module is shown in Fig.3

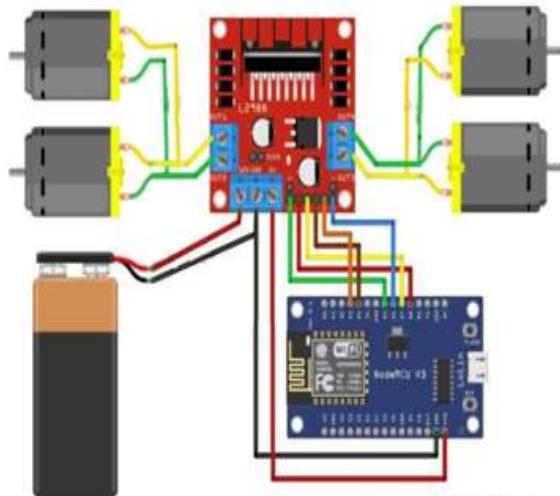


Fig 3: Complete sketch of Node MCU with L298N motor driver, battery, and necessary connections.

The rover is controlled by Node MCU placed to module in above the surface of ground by Rover. The screenshots of working model is presented with the help of mobile APP.

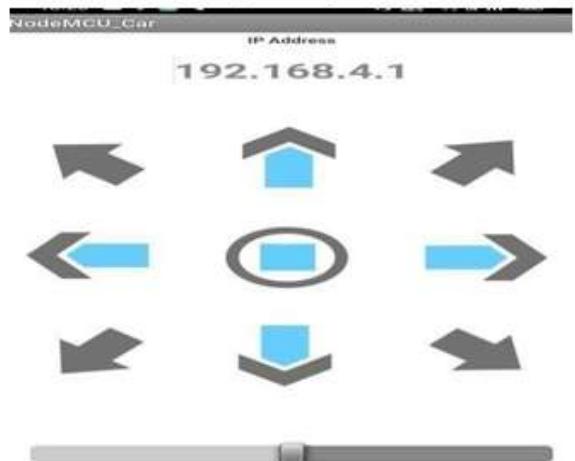


Fig 4: Display in mobile APP.

III. Results & Discussion

The developed prototype module is shown in the figure.5. Car is tested on various tracking paths. The figures of tested wirelessly controlled car is shown in figure 6.



Fig 5: Working model of Wi-Fi CAR



Fig 6.a: Car moving in a test track



International Workshop on Mobility and MiddleWare Management in HetNets, pp. 3, 2015.

[5] ESp8266 data sheet

Fig 6.b: Car moving in a test track

Fig.6 a & b are the wirelessly controlled car in test track giving instruction from mobile app (NodeMCU_Car). It is observed that the preliminary prototype wirelessly controlled car with the help of NodeMCU is moving in indoor corridor at a distance of 4.5m. It is noticed after the 4.5m that Wi-Fi car is not controlled appropriately with the help of mobile app. It may be due to poor Wi-Fi connectivity between the mobile app and node MCU.

IV. Conclusions

In our work, we have concentrated on the application of node MCU module. We developed wirelessly controlled car using NodeMCU ESP 8266 Wi-Fi module. Assessed the possibility of developing the car using this module. It is observed that, these modules are controlled up to the distance of 5m from mobile app. Further, work can be extended to take the Received Signal Strength (RSS) measurements using these modules at each increments of 0.25m internally for indoor corridor data experiments.

References

- [1] D.Mukhopadhyay, S.Karmakar, A.Meshram and A.Jadhav, "A Prototype of IoT based Remote Controlled Car for Pentesting Wireless Networks," 2019 Global Conference for Advancement in Technology (GCAT), Bangalore, India, 2019, pp. 1-7, doi: 10.1109/GCAT47503.2019.8978354.
- [2] Nazirah Ahmad Zaini Norliza Zaini Mohd Fuad Abdul Latip and Nabilah Hamzah "Remote monitoring system based on a Wi-Fi controlled car using Raspberry Pi" IEEE Xplore: 08 May 2017; 2016 IEEE Conference on Systems Process and Control (ICSPC).
- [3] L.Shu et al., "WI-FI-based smart car for toxic gas monitoring in large- scale petrochemical plants," 2015 IEEE International Conference on Consumer Electronics - Taiwan, Taipei, Taiwan, 2015, pp. 200-201, doi: 10.1109/ICCE-TW.2015.7216854.
- [4] Zhiqiang Huo, Lei Shu, Zhangbing Zhou, Yuanfang Chen, Kailiang Li, Junlin Zeng, "Data Collection Middleware for Crowdsourcing-based Industrial Sensing Intelligence", Proceedings of the ACM

Deep Learning in Sensing and Detecting Modulation Scheme in Cognitive Radio

P Ravinder Kumar

Associate Professor,
ECE Department,

Jayaprakash Narayan College of Engineering,
Mahabubnagar -509001, INDIA
1ravinderpalem@gmail.com

Sandeep V M

Professor and Dean,
ECE Department,

Jayaprakash Narayan College of Engineering,
Mahabubnagar -509001, INDIA
svmandr@yahoo.com

Subhash S Kulkarni

Principal and Professor,

PESIT – Bangalore South Campus, Bengaluru
sskul@pes.edu

Abstract: The scarce spectrum utilization is done by Cognitive Radio technology. CR senses the channel allocates to Secondary User when free. If we know the modulation feature of CR, except that feature SU may communicate with any one modulation scheme from 11. So, the opportunity increased by 11-fold. For this we build two CNN models that classify the modulations.

Keywords: Cognitive Radio, Deep Learning, CNN

I. Introduction

Spectrum is limited and allocated for all applications, as the technology is increasing the need of spectrum is also increasing to fulfil the needs the CR technology is introduced. CR senses the empty Spectrum and allocates the channel to the secondary user (SU). [2] represents different sensing methods for getting the channel. Energy detection method is used to check whether the primary user (PU) is available or not. The primary user is free then we transmit else waits for the channel. In the improvement of technology, we know some features of the PU, SU may work accordingly. If modulation scheme of PU is known then SU uses the channel without using that modulation scheme. For implementing this Deep learning (DL) methods [9] are used. The neural network that uses convolution is used for feature extraction. Modulation recognition of PU is done by using Convolutional Neural Networks (CNN). In CNN, first build the model and training is done then predicted the data. Worked with 11 modulation schemes, so 11-fold opportunity is increased to SU.

The rest of this paper is organized as follows. In Section II, we included the details of the dataset generation and background. Section III shows the DL Models for signal detection and modulation recognition. Section IV confirms our experiment results. Finally, our conclusions and directions for further research are given in Section V.

II. Background

The classification of wireless signals received is a useful tool for both civilian and military applications. RadioML2016.10a, a GNU Radio-based data set generation tool, was introduced in [1][3]. Algorithms based on signal amplitude frequency and phase have been widely used for the recognition of automatic modulation [6]. Degraded significantly under low SNR conditions. High-level statistical algorithms [3-5], such as cyclic spectrum and high-order signals, have outstanding capabilities of anti-noise. The complexity of such methods is low relatively, but the features selection relies too much on expert experience [3][7-8]. It is difficult to acquire features that could be adapted environments of non-ideal.

In particular, when there are a number of modulation formats to be classified, it is difficult to set the decision threshold [9].

Developing a technique thus leverages deep learning efficient signal detection and is still a challenge [9-10]. Some work on the DL-based modulation classification, including [3][11], has been published. For example,[3][12] researchers used the signal IQ waveform as a data representation and used CNN to learn the sample.

Data Representation

In this work, we have carried out several experiments on the RADIOML 2016.10A dataset [1]. The data set includes IQ samples from 11 modulation classes (3 analog and 8 digital) over 20 SNR values from -20 dB to +18 dB. Each stream of the IQ sample has the shape of the (2,128). Modulation schemes are WBFM, PAM4, QAM16, QAM64, 8PSK, AM-DSB, BPSK, AM-SSB, BPSK, GFSK, CPFSK. IQ samples of 11,000 streams for each class stored in a dictionary with keys representing values and tuples providing the corresponding IQ samples are in dataset. In the first stage of data pre-processing, rearranged the

dataset into a dictionary made up of a single key describing the entire dataset. Initially, all labels have been digitised, transformed into one-hot encoding vector. In this vector, an element with an index value equal to the class number is set to 1 while the rest of the elements are set to 0. The transformation is to provide a compatible input for the objective function. The new dictionary contains all the data points of each class and the SNR value stored in the list.

III. Our Work

In Cognitive Radio Primary user is present or not checking done by sensing. If PU is present use the channel else waits until the PU is free. This reduces the opportunity of PU channel utilization by SU. Instead of checking PU is free or busy, if we can find which modulation method is used for transmission by PU, when PU is busy. We avoid of using that modulation scheme. We propose this method by using deep learning modulation recognition method. For doing this we build two models of Deep Learning CNN Network.

CNN has widely used in recognizing tasks involving time domain signal such as voice picture and video. In CNN, neurons in one layer are linked to all neurons in the next layer. Convolutional Neural Network consists of an input layer, a hidden layer, an output layer. The convolution layer reduces the number of free parameters to allow the network to be deeper. The flattened matrix passes through a fully connected layer. We propose two models: first one is three convolution layers with two dense layers. And another one is four convolution layers and 2 dense layers. In first model, two convolution layers has filters of 256 and kernel size of (1,5), third convolution layer has 80 filters with kernel size of (1,3) and two dense layers. SoftMax is used after dense layer. Model uses loss function categorical Cross entropy and Adam optimizer. Another model with four convolution layers and two dense layers. Two convolution layers has filters of 256 and kernel size of (1,5), third and fourth convolution layer has 80 filters with kernel size of (1,3) and two dense layers. SoftMax is used after dense layer. Model uses loss function categorical Cross entropy and Adam optimizer.

Model: 1

Layer (type)	Output Shape	Parameters
reshape_1 (Reshape)	(None, 1, 2, 128)	0
zero_padding2d_1 (Zero Padding)	(None, 1, 6, 128)	0
conv1 (Conv2D)	(None, 1, 4, 256)	98560
dropout1 (Dropout)	(None, 1, 4, 256)	0
zero_padding2d_2 (Zero Padding)	(None, 1, 8, 256)	0
conv2 (Conv2D)	(None, 1, 6, 256)	61520
dropout2 (Dropout)	(None, 1, 6, 256)	0
Conv3 (Conv2D)	(None, 1, 6, 80)	61520
dropout3 (Dropout)	(None, 1, 6, 80)	0
flatten1 (Flatten)	(None, 480)	0
dense1 (Dense)	(None, 256)	123136
dropout4 (Dropout)	(None, 256)	0
dense2 (Dense)	(None, 11)	2827
activation1 (Activation)	(None, 11)	0
reshape2 (Reshape)	(None, 11)	0
Total Parameters:		347563

Model: 2

Layer (type)	Output Shape	Parameters
reshape_1 (Reshape)	(None, 1, 2, 128)	0
zero_padding2d_1 (Zero Padding)	(None, 1, 6, 128)	0
conv1 (Conv2D)	(None, 1, 4, 256)	98560
dropout_1 (Dropout)	(None, 1, 4, 256)	0
zero_padding2d_2 (Zero Padding)	(None, 1, 8, 256)	0
conv2 (Conv2D)	(None, 1, 6, 256)	61520
dropout2 (Dropout)	(None, 1, 6, 256)	0
Conv3 (Conv2D)	(None, 1, 6, 128)	61520
dropout_3 (Dropout)	(None, 1, 6, 128)	0
Conv4 (Conv2D)	(None, 1, 6, 80)	61520
dropout4 (Dropout)	(None, 1, 6, 80)	0
flatten1 (Flatten)	(None, 480)	0
dense1 (Dense)	(None, 256)	123136
dropout5 (Dropout)	(None, 256)	0
dense2 (Dense)	(None, 11)	2827
activation1 (Activation)	(None, 11)	0
reshape2 (Reshape)	(None, 11)	0
Total params:		409083

IV. Results

In order to evaluate the performance of our model, we look at the performance classification of the test data set. We trained approximately 2 million samples using 50% of training and 50% for testing.

These samples are uniformly distributed in signal to noise ratio (SNR) from -20 dB to +18 dB. We build two models and the results are shown for each model. For the CNN model with three convolution layers and setting Adam optimizer, we train the model for 100 epochs with GPU as runtime. Then predict the model with testing data and plot the confusion diagram. From figure 1, Digital modulation schemes are well classified and analog modulation schemes of misclassified. 8PSK, AM-SSB most of the time misclassified. QAM16, QAM 64, QPSK are also confused as QAM64, because QAM16 and QPSK phases are available in QAM64. To improve this, take the normalized data, then predict the output. When normalization is done, most of the data selected is with better signal-to-noise ratio. So, the results are improved in figure 2 and the problem of AM-SSB is solved, but the 8PSK, QAM16, QAM64 and QPSK problem is not solved.

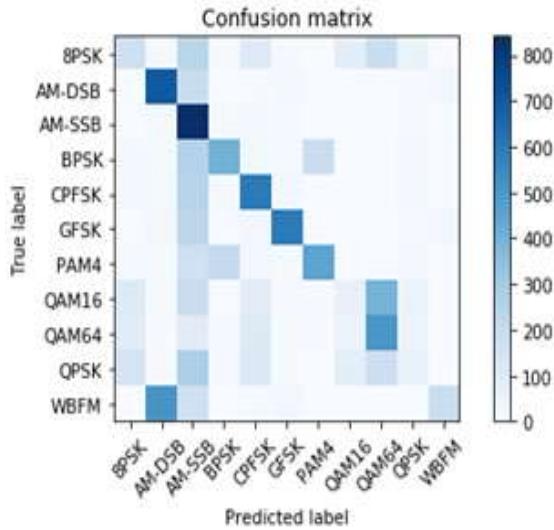


Fig 1: Confusion Diagram with trained model for Model-I

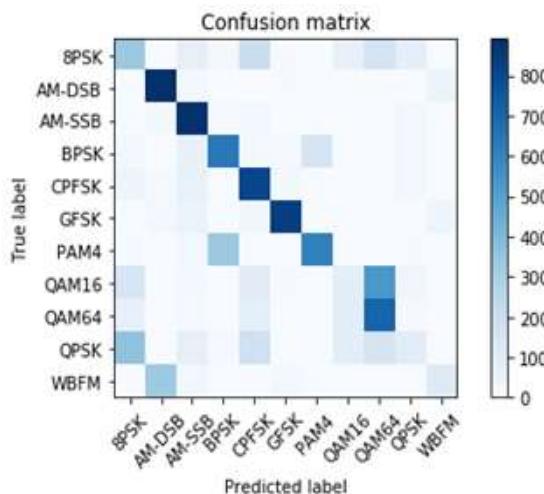


Fig 2: Confusion Diagram after normalization for Model-I

To improve model added one more convolution layer as fourth layer. Train the model with actual data set portioned as 50% training and 50% testing. GPU as run time for 50 epochs. And plotted the graph for training loss Versus validation loss. Validation loss and training loss or decreased in each epoch as shown in figure 3. For prediction 50% testing data is used. For every sample data the maximum of predicted data is stored and plotted confusion diagram (figure 4). The results are very much improved.

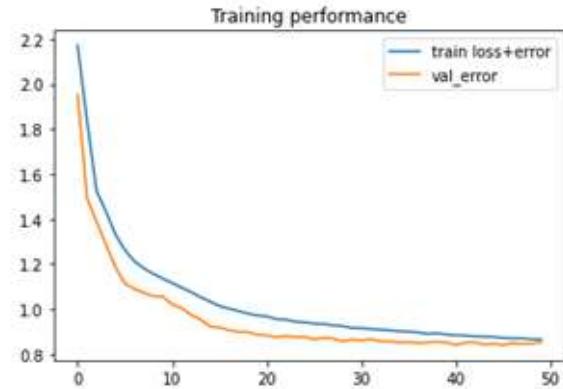


Fig 3: Training loss versus validation loss

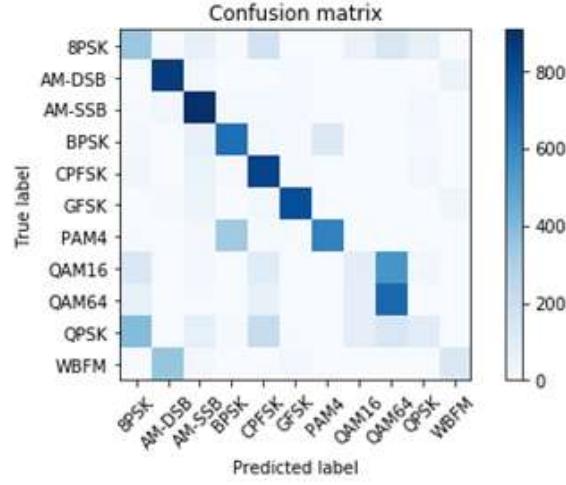


Fig 4: Confusion Diagram with trained model for Model-II

From the figure 4 digital modulation schemes are well recognized and analog modulation schemes are miss classified sometimes. To improve this, take the normalized data then predict the output with normalized data. When normalization is done most of the data selected is with better SNR. So, the results are improved as shown in figure 5. Almost 8PSK, AM-SSB problem is solved by using 4-layer model. Still some confusion with QAM16 this to corrected.

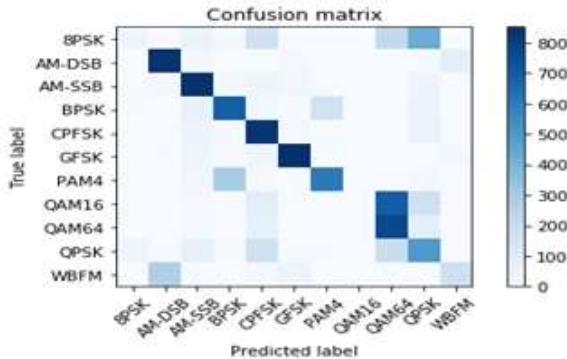


Fig 5: Confusion Diagram after normalization for Model-II

V. Conclusions

We used two deep neural networks to recognise radio modulation schemes by extracting its features. CNN offers the highest degree of precision of classification. These two models achieve satisfactory accuracy for the role of classification. In the future, we are planning to explore more models that are considered to be effective to understand the impact of different layers and modulation recognition tasks.

References

- [1] Timothy J. O’Shea and Nathan E. West. Radio machine learning dataset generation with gnu radio. 2016.
- [2] Ranjan, A.; Singh, B. Design and analysis of spectrum sensing in cognitive radio based on energy detection in Proceedings of the International Conference on Signal and Information Processing, Vishnupuri, India, 6–8 October 2016; pp. 1–5..
- [3] XiongZha, Hua Peng, Xin Qin, Guang Li, Sihan Yang. "A Deep Learning Framework for Signal Detection and Modulation Classification", Sensors, 2019.
- [4] S. S. Soliman and S. .Hsue. Signal classification using statistical moments. IEEE Transactions on Communications, 40(5):908–916, May1992.
- [5] A. K. Nandi and E. E. Azzouz. Modulation recognition using artificial neural networks. Signal Process., 56(2):165–175, January 1997.
- [6] T. J. O’Shea, T. Roy, and T. C. Clancy. Over-the-air deep learning based radio signal classification. IEEE Journal of Selected Topics in Signal Processing, 12(1):168–179, Feb 2018.
- [7] X. Liu, D. Yang, and A. E. Gamal. Deep neural network architectures for modulation classification. In 2017 51st Asilomar Conference on Signals, Systems, and Computers, pages 915–919, Oct 2017.
- [8] Timothy J. O’Shea, Johnathan Corgan, and T. Charles Clancy. Convolutional radio modulation recognition networks. In Christina Jayne and LazarosIliadis, editors, Engineering Applications of Neural Networks, pages 213–226, Cham, 2016. Springer International Publishingand.
- [9] XiongZha, Hua Peng, Xin Qin, Guang Li, Sihan Yang. "A Deep Learning Framework for Signal Detection and Modulation Classification", Sensors, 2019.
- [10] K. Karra, S. Kuzdeba, and J. Petersen. Modulation recognition using hierarchical deep neural networks. In 2017 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), pages1–3, March 2017.
- [11] Kir, safTekbiyik, Ali Ekti, Ali Görçin, GunesKarabulut Kurt, and CihatKeçeci. Robust and fast automatic modulation classification with cnn under multipath fading channels. 11 2019
- [12] Kumar, K.S.; Saravanan, R.; Muthaiah, R. Cognitive Radio Spectrum Sensing Algorithms based on Eigenvalue and Covariance methods. Int. J. Eng. Technol. 2013, 5, 595–601.

Session-A2:
Electrical Power Engineering

Optimal Shunt Capacitor and Distributed Generator in Radial Distribution System Using Particle Swarm Optimization

P.Sree Lekha

PG student, Department of EEE,
Chaitanya Bharathi Institute of Technology,
Hyderabad-500075, India

Dr.P.Venkata Prasad

Professor, Department of EEE,
Chaitanya Bharathi Institute of Technology,
Hyderabad-500075, India

Abstract: This paper provides a novel technique in order to allocate the shunt capacitor(SC) banks and distributed generators(DG) optimally in radial distribution system(RDS) to decrease power losses, improve voltage profile, increase the voltage stability index, and acquire great energy savings .To find the optimal size and site of DG and SC banks, Particle swarm optimization (PSO) technique is modified with constriction factor and is applied to IEEE 33-bus system. The result shows the efficiency of the proposed method.

Keywords: Constriction factor particle swarm optimization, Distributed Generation, Radial distribution system, Shunt Capacitors bank, Voltage Profile, Voltage stability index.

I. Introduction

The sizing and siting of distributed generations(DG) units in distribution network is very crucial because optimally and strategically placed DG reduces system losses . Distributed generations may be positioned directly to shrink both real power(Ploss) and reactive power loss (QT), improve the voltage stability index(VSI), diminish the total voltage deviation (TVD) and revamp the consistency of the network. For optimal sizing and siting of DG in distribution systems different methods are proposed in the literature. PSO is a robust stochastic optimization technique which is based on movement and intelligence of swarm. A significant amount of power loss in the system is presented , in order to that of 10-13% of the output is also generated. High distribution loss implies system voltage inefficiency and poor control occurs. Locally mounted distributed generations and bypass shunt capacitor (SC) banks added to the network can increase network capacity and power quality . Small production units ranging from 1KW to 50MW are connected near the user side in DG technology[1]. Distributed generation can be conventional and non- conventional energy sources[2]. Due to the restriction of fossil fuels, non-conventional distributed generation has become a major option. To use the advantages of the distributed generation technology it is necessary to know the optimal site and size of the distributed generations in distribution system otherwise it may cause some unfavorable effects, such as increase in losses, low voltage profile and increase costs. The implementation of the distributed generation into the

distributed systems is a great choice. as it provides more accuracy, reliability, better power quality and green house gas emission reduction[3]. Since the last decade, researchers have shown interest in finding the proper size and site of shunt capacitors and distributed generator in the radial distribution distribution system. A thorough review of number of state of art literatures which have been focused on best choice of size and site of DGs and SC banks radial distribution system is presented in Table1 for reference.

Table1: Upper and lower limits of DGs and SC bank

CASES	DG _{MIN}	DG _{MAX}	SC _{MIN}	SC _{MAX}
I	0.5	1.5	0.2	1.5
II	0.5	1.5	0.2	1.5

The PSO algorithm for particle swarm optimization often agonizes over the issue of premature convergence. The constriction factor was introduced into the PSO algorithm by cleric[6] and called as the PSO constriction factor to circumvent this problem. In relation to the rapid change of position, this aspect regulates the speed of the particles. Thus, steady and stable convergence is acquired. The Cf-PSO algorithm is used for transmission system problems, congestion management and economic load dispatch, and the results obtained shows advantage over the other algorithms [4,14 5]. From the survey it is clear that Cf-PSO algorithm has not been employed so far for allocation of shunt capacitor banks and distributed generator in radial distribution system. In view of this main contributions are,

- To achieve the optimal size and site of distributed generation and shunt capacitor banks, to include the credibility of the constriction factor-PSO algorithm.
- To analyze the impact of the allocation of distributed generation and shunt capacitor banks to justify the efficiency of the adopted IEEE 33-bus system with regard to Ploss, Qloss, TVD and VSI.
- To scrutinize the effect on operational cost and net savings.

II. Problem Formulation

2.1. Assumptions

The key assumptions considered before the formulation of the problem are presented below

- a. The source bus is not considered as the site for shunt capacitor banks and distributed generations placement .
- b. Loads are typically characterized as constant PQ loads
- c. Upper and lower limits of shunt capacitor banks and distributed generation are provided in Table2.

2.2. Load flow analysis

Perfect RDS single line diagram (SLD) in figure 1 where i is the sending end node and j is the receiving end node, Y_i and Y_j are respectively shunt node i and j capacitors, representing leakage current between conductance. Shunt conductance is assumed to be negligible in calculation as the distribution system capacitance is extremely small[9]. To analyze the multi-objective function, RDS load flow analysis is conducted using the backward forward sweep method. This method is adopted for its low memory requirement, flexibility, robustness, superior speed and efficiency of convergence[8].

2.3. Formulation of objective function (OF)

The different components of the OF is discussed below.

- **Minimizing active power loss (f_1):** The function f_1 for reducing actual power loss(PL) is defined in (1)

$$f_1 = \text{Minimise}(PL)$$

$$\text{Where } P_L = \sum_{ij=1}^{n-1} P_{\text{loss}}(ij) \quad (1)$$

The value of $P_{\text{loss}}(ij)$ for RDS is given by(2)

$$P_{\text{loss}}(ij) = R_i * (P^2 + Q^2) / |V_i|^2 \quad (2)$$

- **Minimizing reactive power loss (f_2):** The function f_2 for reactive power loss(QL) is defined in (3)

$$f_2 = \text{Minimise}(QL) \quad (3)$$

$$\text{Where } Q_L = \sum_{i=1}^{n-1} Q_{\text{loss}(ij)}$$

The value of $Q_{\text{loss}(ij)}$ for the RDS is given in (4)

$$Q_{\text{loss}(ij)} = X_{ij} \times P_i^2 + Q_i^2 / |V_i|^2 \quad (4)$$

- **Minimizing TVD (f_3):** The function f_3 for minimizing the TVD is stated in (5)

$$f_3 = \text{Minimise} \left(\sum_{i=1}^N |(V_n - V_i)|^2 \right) \quad (5)$$

- **Improving VSI(f_4):** The f_4 for improving VSI is defined in (6)

$$f_4 = \text{Maximising} (VSI_i) \quad (6)$$

The value of VSI is calculated by (7).

$$VSI_i = |V_j|^4 - 4[P_i X_{ij} - Q_i R_{ij}]^2 - 4[P_i R_{ij} + Q_i X_{ij}]|V_j|^2 \quad (7)$$

Formulation of objective function: The most frequently used method to optimize a multi objective function is the weighted sum method.In this Method,each single objective function will be renovated Into multi objective function by multiplying it with a weighting factor.All these weighted objective functions will be added to form a multi objective function(OF).

$$OF = y_1 \times f_1 + y_2 \times f_2 + y_3 \times f_3 + y_4 \times f_4 \quad (8)$$

Where

$$\sum_{i=1}^4 y_i = 1$$

The values of weighting factors are taken in this as

$$y_1=0.4, y_2=0.2, y_3=0.2 \text{ and } y_4=0.2.$$

Here, f_1 is the active power loss defined in eq(1), f_2 is reactive power loss stated in eq (3), f_3 is the TVD eq(5)and f_4 is the VSI eq(7) .

2.4. Constraints

The above OF is subject to the following equality and inequality constraints.

- **Inequality constraints**

Voltage limit: Magnitude of voltage must be between minimum and maximum limits i.e;

$$V_{\min}^i \leq V^i \leq V_{\max}^i \quad (9)$$

Where, $V^i_{\max} = 1.05 \text{ p.u}$, $V^i_{\min} = 0.95 \text{ p.u}$

Real power limit of DGs: Actual power produced by DGs(P^i_{DG}) must be between lowest and highest limits

$$P^i_{DG,\min} \leq P^i_{DG} \leq P^i_{DG,\max} \quad (10)$$

$$P^i_{DG,\min}=0.5 \text{ MW}, P^i_{DG,\max}=2.5 \text{ MW}$$

Reactive power limit of SCs: Reactive power produced by SCs (QSC) must be between 0.5MVAr and 1.5MVAr

$$Q^i_{SC,\min} \leq Q^i_{SC} \leq Q^i_{SC,\max} \quad (11)$$

- Equality Constraints:** The total sum of active power and reactive power produced by DGs and SCs must be less than sum of total demand excluding slack bus

$$\sum_{i=2}^{NDG} P^i_{DG} \leq [\sum P^i_D + P_L] \quad (12)$$

$$\sum_{i=2}^{NSC} Q^i_{SC} \leq [\sum Q^i_D + Q_L] \quad (13)$$

III. Cf-Pso Application to Solve Optimal Sizing and Siting Problem of Dg Units in Rds

Optimization is a technique that provides some satisfactory solution that meets the minimum/maximum value of the objective function. Single objective or multi objective results in the method of optimization. To figure out the best outcome that can decrease an objective function of the single objective optimization of the network provided. Multi objective requires more than one or more optimal solutions..Although ,the objective of optimizing multi-objectives are often conflicting that means objective cannot be improved without making one or more objectives.

The Cf-PSO algorithm has the following advantages

- simple to implement ,
- has higher efficiency and chance to find global optima,
- converges fast and takes less computational time,
- efficient for solving problems presenting tough to find precise mathematical problems
- has few parametes to adjust.

By updating velocity and position of particles

$$V^{t+1}_i = K \times (w \times v^t_i + c_1 \times \text{rand1} \times (p^{best,i} - X^t_i) + c_2 \times \text{rand2} \times (g^{best,i} - X^t_i)) \quad (14)$$

$$K = 2 / |2 - C - \sqrt{C^2 - 4C}| \quad (15)$$

Where $c=c_1+c_2$ and $c>4$

$$W^{t+1} = W_{\max} - (W_{\max} - W_{\min}) / t_{\max} \times t \quad (16)$$

$$X^{t+1} = X^t + v^{t+1} \quad (17)$$

Where V^{t+1}_i and X^{t+1} be updated velocity and position of the particles, W^{t+1} is the inertia weight which keeps the balance between local and global exploration. W_{\max} and W_{\min} values are taken as 0.9 and 0.4 .

Here, rand1 and rand2 are two random numbers independently generated in range [0,1].Constants c_1 and c_2 are acceleration factors,that pulls each particle towards p best and g best positions.But ,Clerc[6]has proposed to pressure values of c_1 and c_2 as 2.05 instead of 2.0 to avoid issue of local convergence .For acercleration constants c_1 and c_2 constriction factor is considered as $k=0.729$

Algorithm

Step1: Read the system data (load data and line data), population size, maximum number of iterations, number of real power distributed generations and shunt capacitor banks to be incorporated in radial distribution system.

Step2: Calculate voltages at each node and power losses (real and reactive),TVD,VSI of the RDS using backward and forward sweep load flow method .

Step3: Set iteration iter=1.

Step4: By upper and lower operating limits size of DGs and SC banks are generated randomly within their limits (18)-(19)

$$PDG(i)=P_{min,DG}(i)+\text{rand} \times (P_{max,DG}(i)-P_{min,DG}(i)) \quad (18)$$

$$QSC(i)=Q_{min,SC}(i)+\text{rand} \times (Q_{max,SC}(i)-Q_{min,SC}(i)) \quad (19)$$

Step5:Generate random position and velocity for each particle .

Step6:Calculate power losses ,TVD and VSI using (1),(5) and (7).

Step7:Update position and velocity of each particle using (14) and (17).

Step9: If maximum iteration reaches then stop iteration process or else increase the iteration by one and go step 2

Step10: Display results such as power losses (real and reactive), TVD,VSI.

IV. Results

The algorithm has been programmed using MATLAB and run for 30 independent runs having 100 iterations and 50 as population size for each case .Parameters of Cf- PSO are listed in Table 2.network performance before DGs and SC banks installation are also tabulated in Table 3.For IEEE 33 bus results are described as technical and commercial benefit analysis by using algorithms.

Table 2: Cf-PSO, PSO algorithm parameters

Algorithm	Population size	Maximum size	c1	c2	r1	r2
Cf-PSO	50	100	2.05	2.05	1	1
PSO	50	100	2.0	2.0	1	1

Table 3: Target value of objective function before allocation of DGs and SC banks

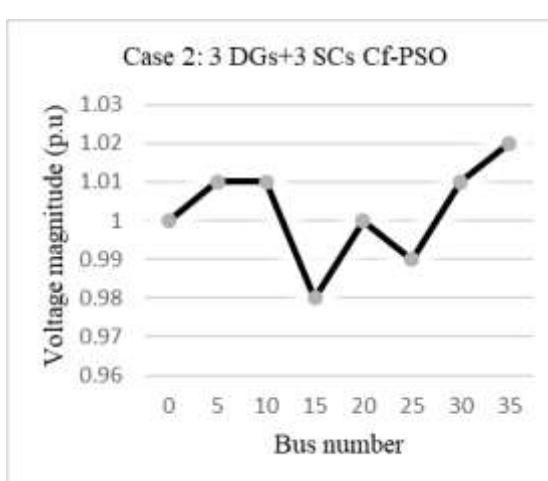
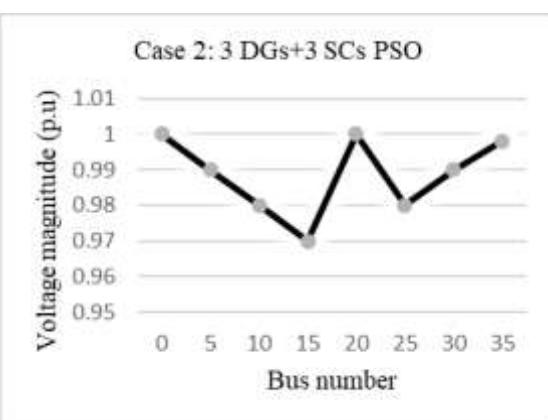
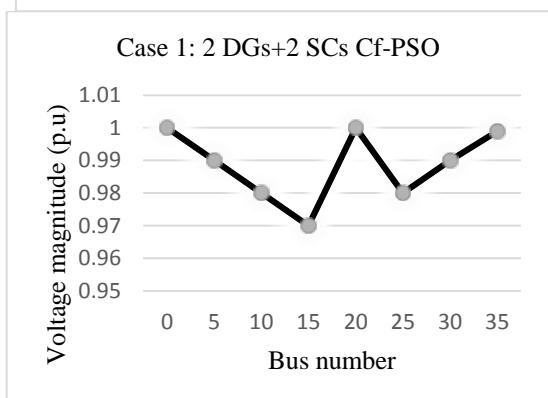
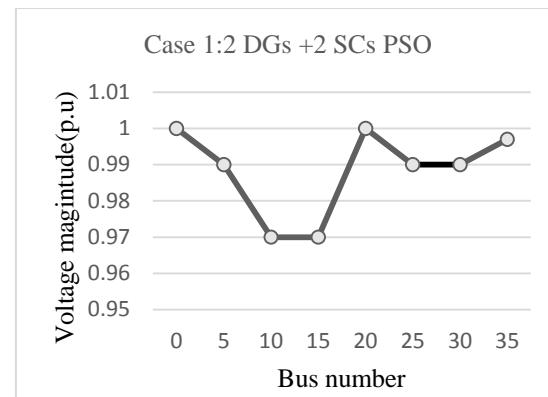
Test	f ₁	f ₂	f ₃	f ₄
IEEE-33 bus system	0.211	0.143	0.1338	0.6673

Case 1: Two DGs operating at unity power factor (UPF) and two SC banks are installed at their optimal location.

Case 2: Three DGs operating at UPF and three SC banks are installed at their optimal location.

IEEE 33-BUS RDS Test:

At first system has 12.66 KV with 1 MVA base.Consisting 33 nodes and 32 branches,total load on this network is shown in Figure(1) (3.72+j2.3)MVA .The active and reactive losses of network and performance analysis using PSO and Cf-PSO alogorithm for different cases listed .Figure exhibits bus voltage level of each bus before DGs and SC banks installation and after installation for case 1 and case 2 ,it is observed that proposed algorithm yields better voltage profile for case 2 .



V. Conclusion

This paper has multi objective optimization to define the size and site of SC banks and DGs with combining factors active ,reactive losses,TVD,VSI.Cf-PSO algorithm for RDS like IEEE 33 bus system is considered and is able to determine suitable size and position of DGs and SC banks while reducing active and reactive power loss,minimizing TVD and improving VSI .

References

- [1] Ackermann T , Anderson G, and Soder L.Distributed generation:definition.Electric power systems research.2001;57(3):195-204
- [2] Ghosh Sudipta ,Ghoshal S.P, and Ghosh Saradindu.Optimal sizing and placement of distributed generation network system.Electrical power and Energy system.2010;32(8):849-856
- [3] Singh B,Mukherjee V, and Tiwari P.A survey on impact assessment of DG and FACTS controllers in power systems .Renew.Sustain.Energy Rev.2015;42:846-882
- [4] Biswas S,Mandal K.K ,and Chakraborty N.Constriction factor based particle swarm optimization for analyzing tuned reactive power dispatch.Frontiers in energy .2013;7(2):174-181
- [5] Raha S,Som T ,and Chakraborty N.Constriction factor based particle swarm optimization applied to reactive power dispatch in transmission system.International conference on sustainable energy and intelligent systems (SSEISCON).2011
- [6] Clerc M .The swarm and the queen:towards a deterministic and adaptive particle swarm optimization.In proceedings ICEC.USA,Washington DC.1999:1951-1957.
- [7] Gopiya Naik S,Khatod D.K, and Sharma M.P.Optimal allocation of combined DG and capacitor for real power loss minimization in distribution networks.International Journal of Electrical Power and Energy Systems.2013;53:967-973.
- [8] Bompard E,Carpaneto E,Chicco G,Napoli R.Convergence of the backward/forward sweep method for the load flow analysis of radial distribution systems.International Journal of Electrical Power and Energy Systems.2000;22(7):521-530.
- [9] Ahmet Dogan,Mustafa Alci.Simultaneous optimization of network reconfiguration and DG installation using heuristic algorithms.Elektronika Ir Elektrotehnika.2019,25(1).
- [10] Biswas P,P.Suganthan P.N, and Amaratunga G.A.Optimal sizing and placement of distributed generations and capacitor in RDS.Computer Science and Information Technology.2017:27-37
- [11] Saonerkar A.K, and Badge B.Y.Optimized DG placement in radial distribution system with reconfiguration and capacitor placement using Genetic algorithm.In Advanced Communication Control and Computing Technologies. 2014:1077-1083
- [12] Biswas Partha P,Mallipeddi R,Suganthan P.N, and Amratunga A.J.A multi objective approach for optimal placement and sizing of distributed generations and capacitors in radial distribution network.Applied soft computing. 2017;60:268-280
- [13] Zeinalzadeh A,Mohamamadi Y, and Moradi M.H.Optimal multi objective placement and sizing of multiple DGs and SC banks simultaneously considering load uncertainty via MOPSO approach. International Journal of Electrical Power and Energy2015;67:336-349.
- [14] V.V.S.N. Murthy, and Ashwani Kumar, Comparison of optimal DG allocation methods in radial distribution systems based on sensitivity approaches. Electrical power and energy systems 2013;53:450-467.
- [15] Kennedy J,Eberhart RC.Particle swarm optimization. Proceedings of IEEE International conference on neural networks. Piscataway, NJ.1995:1942-1948.
- [16] Baddu Naik B,Padmanabha Raju Ch, and Srinivasa Rao R.A constriction factor based particle swarm optimization for congestion management in transmission systems .2018;10(2)

Figures:

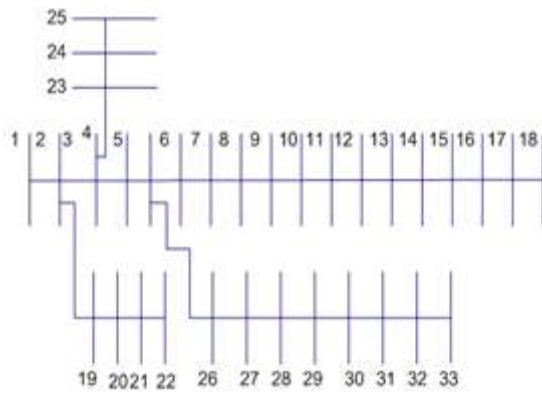


Fig.1.Single Line Diagram of the IEEE 33-bus RDS

AI based Cyber-attack Resistant Microgrid System with IRNSS Synchronization

M Balasubbareddy

Department of EEE,

Chaitanya Bharathi Institute of Technology,
Hyderabad-500075, India.
balasubbareddy79@gmail.com

Saini Varshini

Department of EEE,

Chaitanya Bharathi Institute of Technology,
Hyderabad-500075, India.
varshiniraosaini@gmail.com

P Venkata Prasad

Department of EEE,

Chaitanya Bharathi Institute of Technology,
Hyderabad-500075, India.
pvprasad_eee@cbit.ac.in

A D Sarma

Department of ECE

Chaitanya Bharathi Institute of Technology,
Hyderabad-500075, India.
ad_sarma@yahoo.com

Abstract: smart grid is next-generation power infrastructure that is being used to remodel the traditional grid in order to increase its security and performance. Unfortunately, malicious cyber-attacks on the smart grid will cause serious economic, social, technological, and control issues in power system operations. This proposal examines the cyber-security of micro grid systems and makes recommendations. To combat cyber-attacks, new cyber resilient control strategies are being created. A new AI-based approach for detecting cyber-attacks in micro grids and identifying the distributed energy resource (DER) device that was attacked is demonstrated. The approach is time series based analysis and neural network called nonlinear auto-regressive exogenous (NARX) model. To calculate the DC voltage output, use the formula below. We need to train NARX neural networks to understand distributed energy resources and currents.

A prototype will be built to verify the experimental findings presented during the grid connected and isolated modes. The DGs are synchronized using an IRNSS-based scheme. The use of a GPS-based synchronization system to create a standard time reference for synchronizing distributed generation modules is demonstrated. For optimum output and consumption, Deep Learning Optimization Technique is used.

Keywords: DC micro grid, DERs, cyber-attacks, cyber-security, power flow control strategy.

I. Introduction

In order for the country to develop, the electric sector must play a significant role in various sectors such as healthcare, industry, irrigation, and communication. Continuous power is an essential component of any nation's growth. Recent cyber-attacks have pushed energy sector resilience in the forefront of national research priorities. The report

published by a private cyber security firm in United States, months after the Galwan valley clash in June, in which soldiers from both countries were killed, has indicated that Chinese cyber operation targeted India's power grid. The firm's report raises questions about whether, outage of power in Mumbai last year is caused by a Chinese party.

In 2005, the EU proposed smart power networks based on business demands and environmental protection [1]. Our society is so dependent on electric power. During blackouts areas no emergency stand by generation, communication systems failed to operate [2]. India was in the third place at electricity producing across the world and even though it is facing power deficiency in the upcoming years power demand increases with the economy as there is a very strong relation between them [3]. A design topology and the technical specifications are discussed below of PV power plant [4]. To handle with the requirement of peak watt of zone all the time inverter should be large enough. Inverter size must be 25–30% larger than total wattage of machines and load appliances [5].

II. Synchronization Technique with IRNSS

IRNSS receiver is have the ability of tracking and obtaining of L5, S and GPS L1 signals. Under an MoU, an IRNSS receiver is installed at Navigation and Communication Research Centre (NCRC) laboratory of CBIT Hyderabad in the dept. Of ECE. The IRNSS User Receiver (IRNSS UR) obtains, changes and demodulates obtained satellite signals combined at L5 (1176.45MHz) and S1 (2492.028MHz) band frequencies. The receiver is also capable of processing GPS (L1 C/A) signals centered at 1575.42MHz and generates the computations with reference to the internal or external trigger. The receiver position can be computed using any of the seven modes i) IRNSS L5 only ii) IRNSS S1 only iii) GPS L1 only iv) IRNSS L5 and S1 dual frequency only v) Combined IRNSS

L5 and GPS L1 vi) Combined IRNSS S1 and GPS L1 only and vii) Combined IRNSS dual frequency and GPS L1 only. The IRNSS receiver consists of a suitable antenna which is capable of receiving extremely weak satellite signals on both, L5 (1176.45MHz) and S1 (2492.028MHz) frequencies. The output power signal is close to 165dBW. A antenna is accompanied by the RF front end, the signal is amplified by Low Noise Amplifier (LNA) from 15dB to 20dB. A RF front end contains an High Frequency (HF) filter which reduces effect of an interference signal. An IRNSS signal amplified is then combined with frequency of an Local Oscillator (LO) for generating Intermediate Frequency (IF) signals. A Intermediate Frequency signal filtered is then maintained at an amplitude level constant across the Automatic Gain Control (AGC) unit. The IRNSS user receiver functions are shown in Fig. 1.

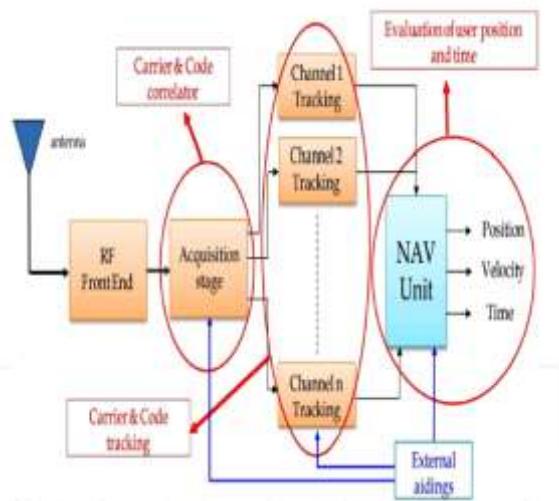


Fig 1: IRNSS receiver functions scheme.

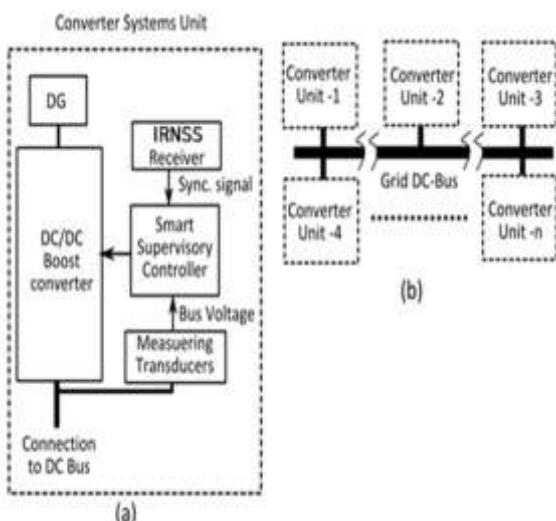


Fig. 2. block diagram proposed (a) one unit of the converter system including the controller (b) the DC Bus connected across the n-unit converter system.

A. Receiver functions

The IRNSS RF signals of Satellite Vehicles (SV) in the view is obtained through antenna that is Right Hand Circularly Polarized (RHCP) that is nearly hemispherical (i.e., upon the local horizon) coverage gain, The low noise preamplifier (preamp) amplifies the RF signals, that effectively sets figure of the noise of receiver (Keplan and Hegarty, 2006). IRNSS user's receiver particularly has four functions that are important. That is decoding, tracking, acquisition and the position solution.

A proposed system, is shown in Fig. 2, is made up of many converter distributed systems that are attached to main DC bus is shown in Fig. 1a. Each converter system is made up of a standard DC/DC boost converter is attached to its own local controller. To synchronize various distributed converter systems, an IRNSS receiver receives IRNSS signals from the satellite system.

III. Synchronization Using Irnss System

To better understand IRNSS synchronization, the definition of IRNSS technology will be presented first. The IRNSS is the navigation system in orbital six planes it contains 24 satellites. Every satellite has the atomic clock on board, which provides the exact reference time. The IRNSS satellites send out the microwave signal, which is picked up by an IRNSS receiver on the ground. The IRNSS receiver decodes signals from the two or many satellites then calculates current time and location with great precision. The measured time is output as the serial stream or a one pulse per second (1PPS) reference time signal by receiver. The satellite atomic clock provides the 1PPS output with a few tens of nanoseconds of precision In order to generate the high-frequency clock from the reference low-frequency (1 Hz)

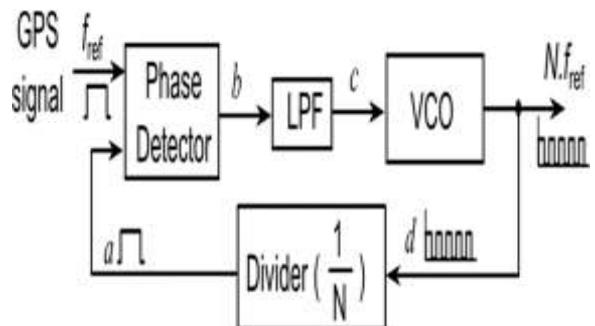


Fig 3: Frequency multiplier with the phase locked loop (PLL).

in the case of the IRNSS reference), the loop must have a large division factor. Figure 3 shows a frequency multiplier with a phase locked loop (PLL).

The proposal uses digital PLL (DPLL) as an effective answer and well-stabilized method to perform multiplying frequency to address the obstacle. Figure 4 displays the block diagram for proposed DPLL.

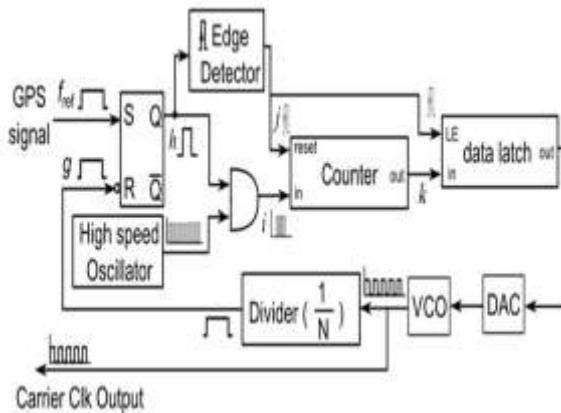


Fig 4: Frequency multiplier using DPLL.

Identify applicable funding agency here. If none, delete this text box.

IV. Simulink Model with Deep Learning

Fig.5 shows the process of deep learning optimization algorithm. In this optimization algorithm the inputs are building end use load data, Electricity tariff data, and distributed energy resources (DER) technology data are given to the deep learning optimization algorithm subjected to satisfy the minimize cost, minimize CO₂ emission and reliability after process the outputs are optimal DER capacities and optimal DER operation schedule. Fig.6 shows the input, output parameters of proposed optimization algorithm.

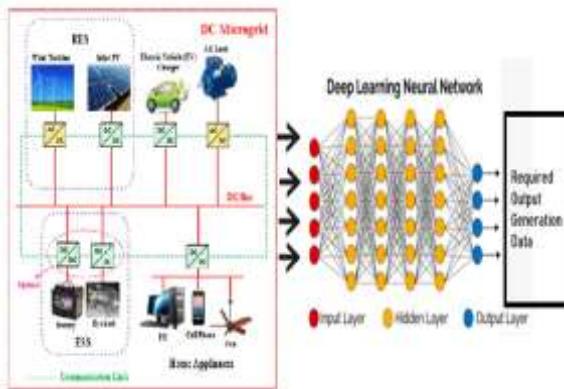


Fig 5: Deep learning Optimization algorithm.

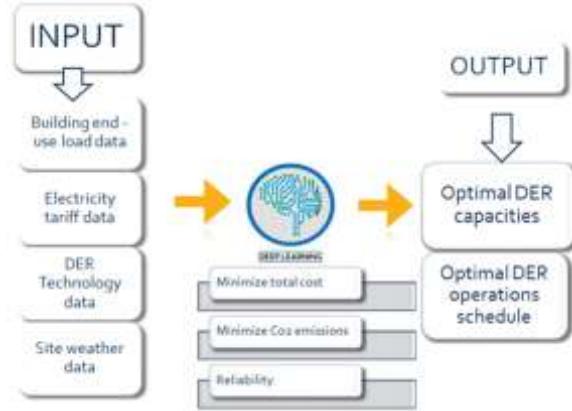


Fig 6: Input and output parameters of Deep learning optimization algorithm.

V. DC Microgrid Prototype System

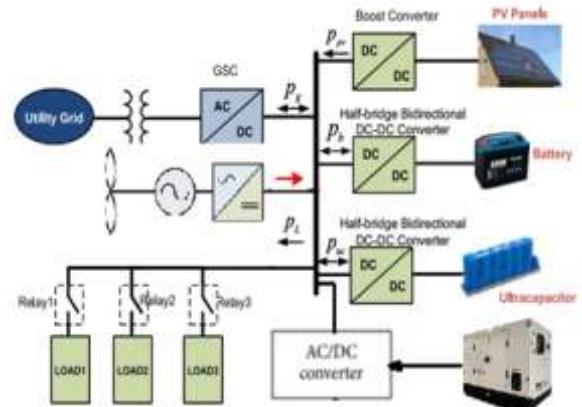


Fig 7: Grid interactive DC micro grid structure.

It is also easy to combine renewable energy sources and the energy storage systems using the DC distribution network. As modern load appliances can also be supplied dc not changing load, any of them are supplied directly through the AC grid, losses associated with conversions from AC to DC can be avoided. Figure 7 depicts the grid interactive DCMG system proposed in the proposal. It consists of a PV source attached to DCMG via a unidirectional boost converter that eliminates the need for a series diode in addition to the PV source, lowering the additional cost and losses compared to a buck converter. As maximum power point (MPP) voltage do not change with isolation, voltage control is used instead of current control to obtain maximum power from the PV. Voltage control also provides more benefits such as accurate measurement, fast tracking and faster regulation.

VI. Observation of Fault Injection of Data and Cyber-Attacks in DC Micro Grid

ANN is executed in several applications in smart grids. NARX network-based application executed to evaluate state of charge (SoC) of lithium-ion batteries.

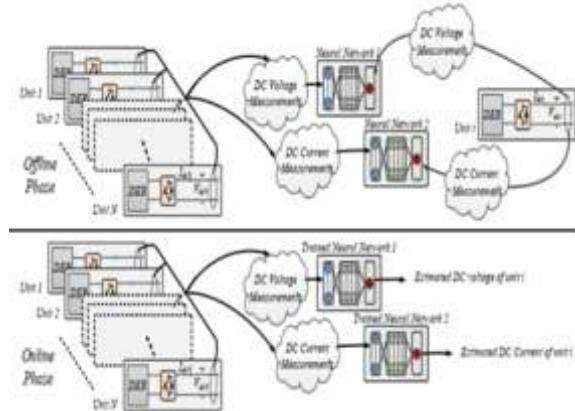


Fig 8: Exploiting and training neural NARX networks for the cyber-attacks detection the DC micro grids.

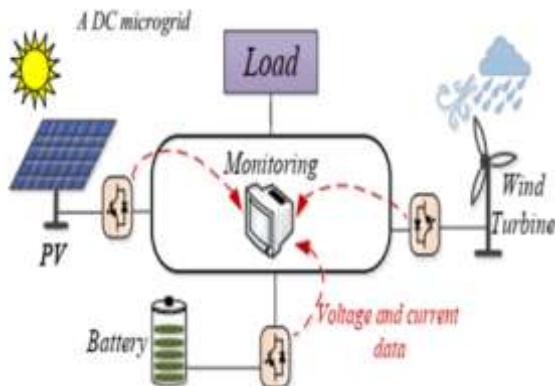


Fig 9: Exchange of data section between monitoring and DER.

VII. Conclusion

In this paper discusses and developed a methodology for designing resilient micro grids and mitigating cyber-attacks in the micro grids. Proposed power electronic distributed converter synchronization technique with IRNSS. This paper also presented Simulink model with Deep Learning Optimization Technique for optimal production and consumption.

References

- [1] Li Fusheng, Li Ruisheng and Zhou Fengquan, "Microgrid Technology and Engineering Application", China Electric Power Press Co., Ltd. (book).
- [2] T.E. Del Carpio Huayllas, D.S. Ramos, R.L. Vasquez-Arnez , "Microgrid systems: Current status and challenges", 2010 IEEE/PES Transmission and Distribution Conference and Exposition: Latin America, pp: 7-12.
- [3] Tripathi, Bhasker (26 March 2018). "Now, India is the third largest electricity producer ahead of Russia, Japan". Business Standard India. Retrieved 27 September 2019.
- [4] P. Sanjeev, Narayana Prasad Padhy, and Pramod Agarwal, "Peak Energy Management Using Renewable Integrated DC Microgrid", IEEE TRANSACTIONS ON SMART GRID, VOL. 9, NO. 5, SEPTEMBER 2018.
- [5] Ashok Jhunjhunwala and Prabhjot Kaur, "discussed Solar Energy, dc Distribution, and Micro grids", IEEE Electrification Magazine / DECEMBER 2018.

Power Quality Concerns in Implementing Smart Distribution Grid Applications

S. Swathi

Research Scholar

Electrical Engineering

University college of Engineering Osmania,
Hyderabad-500007, India
eee.swathi48@gmail.com

Dr. B. Suresh Kumar

Associate Professor

Electrical and Electronics dept
Chaitanya Bharathi Institute of Technology,
Hyderabad-500075, India
bskbus@gmail.com

Dr. J. Upendar

Assistant Professor

Electrical Engineering

University college of EngineeringOsmania,
Hyderabad-500007, India
dr.8500003210@gmail.com

Abstract: Now a day the power demand increasing every passing day. The main duty of the power system is to supply their consumers with an Uninterruptable power supply but in practice, it is not happening. In the grid-like stability problem or Power Quality issues that need to be resolved. Investigation of Power Quality may be performed for each stage of the facility system at an occasional voltage level square measure principally originated from nonlinear. In the case of high voltage level, the disturbances are originated from load Variabilities in the grid.

In this project, we use renewable energy sources for better energy saving. Lots of projects are being undertaken which are able to harness power from renewable energy sources like sun and wind are considered in this paper. The compensating devices such as Distribution Static Compensator (DSTATCOM) and Dynamic Voltage Restorer (DVR) are used in this project for improving the Power Quality in Smart Grid. DSTATCOM and DVR are the devices that are a fast, flexible and efficient solution for Power Quality problems.

Keywords: Bi-directional dc-dc converter, smart grid, Battery, DSTATCOM

I. Introduction

A Smart Grid is defined as the electric grid which uses the Technology of information as well as Technology of communication to collect the data and function on information about behavior of the suppliers and the consumers in an mechanized fashion [1]. Smart Grids will provide more electricity to meet rising demand, increase the reliability, availability, and efficiency of the power grid and also able to integrate carbon-free energy sources into

power networks. A grid uses computer technology in order to



Fig 1: Block Diagram Of Smart Grid

improve communication and automation by connecting various components to the networks [3]. As an example of bulk transmission of power gathered from different generation plants shown below fig(1).

Brilliant conveyance network applications can possibly improve the exhibition of the electric force framework and furthermore offer a similar presentation for existing

So as to improve the productivity of the framework and furthermore vitality which is requested by the heap, the Smart Grid comprises of in excess of two vitality sources [5]. Photovoltaic exhibit combined with a breeze Generator is considered as one of the instances of Hybrid vitality framework. At the hour of winter, wind turbine makes more vitality, during summer the sun-based board delivers a high measure of vitality. The Energy framework (Hybrid) utilizes the corresponding idea of every one of these sources.

A. Analysis and Mitigation of Power Quality

Advancements. In this context of Smart Grids, if the interaction happens in the supply demand side changes will occur in actual amount, the power flows and the energy distributed in between the supply and demand side.

These changes are characterized by a shift from unidirectional power flow firstly in the Alternating current (AC) to bidirectional power flows in both DC and AC forms in much wider frequency ranges. Maintaining the Power Quality levels in this scenario is a critical task. The Power Quality (PQ) monitoring describes and check the compatibility between the grid i.e., supply side and customers side.

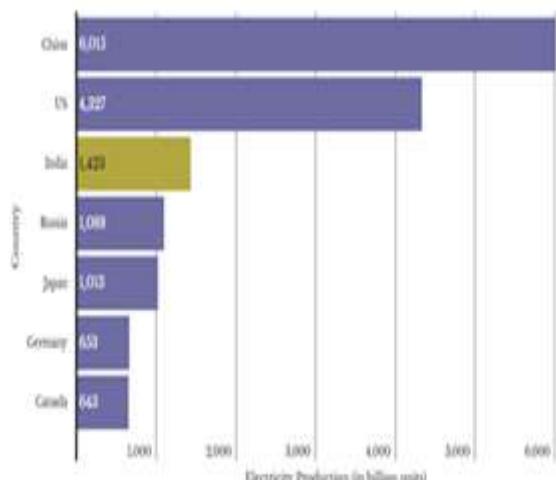


Fig.2. world's leading electricity producers in 2016

Improved Power Quality (PQ) exhibitions are one of the essential parts of future electrical systems. Shrewd Grid innovation can possibly improve the presentation of intensity framework. The levels and nature of supply demand interactions may affect in future. When not managed correctly. This can be managed by using Smart Grid distribution system can rectify some of the issues which occur in the power system i.e., voltage sag, swells and interruptions. Adding a advance techniques, distribution static compensator and Dynamic voltage Restorer.

II. Review of Literature

"In producing and consuming electricity in the world, India is the third largest electricity". India has generated around 368.79 GW till the year of 2019. Share of the renewable energy of 17.3%. Share of the fossil fuel energy of 79.8%. In India 2018-2019, the electricity which was generated by the utilities in India was 1372 TWH. Average electricity used is 1181 KWH/capita. Electricity sector in India has installed the capacity of 237.742 GW till the year

of 2014. Electricity generated around 1160.1 billion units of the electricity in 2017, and growth of 4.72% from previous year 2016. Non-renewable power plant consists of 87.55% of installed capacity. Renewable energy constitutes of 12.45% of total installed capacity. [15]

According to the survey of our project we gathered some information regarding the Electricity producers across the world and India. In figure 2 shows about the world Electricity producers for the year 2016.

III. Power Quality Issues

1. **Voltage sag**-It is the 10-90% decrease in the RMS voltage for 0.5 to 1 minute cycle.
2. **Very short interruption**- It is the total interruption of electric supply for millisecond.
3. **Long interruption**-It is the total interruption of electric supply for 2sec.
4. **Voltage spike**-It is defined as very fast variation of voltage.
5. **Voltage swell**- It is the momentary increase of voltage at power frequency.
6. **Harmonic distortion**-It is caused when voltage waveforms or current waveforms assumes non sinusoidal shape.
7. **Noise**-imposition of high frequency signals on wave forms.
8. **Voltage unbalance**-A variation of voltage in three phase system, when three magnitudes of voltage or differences in phase angle between them is not equal.

IV. Distributed Staticcompensator (Dtsatcom)

The most vital factors in up the facility quality is that the technique of voltage unbalance and compensation of reactive power within the power distribution system to the top user. The unbalance caused by numerous masses within the distribution system and also the reactive power is stipendiary by employing a custom power device that may be a distributed static compensator connected in shunt with the load.

A. Working Principles Of DSTATCOM

DSTATCOM combination of a Voltage Source Converter (VSC), DC capacitor, coupling transformer and controller, as appeared in Figure 4.0.

It is a shunt type gadget which gives a compelling answer for voltage guideline and pay of the receptive force

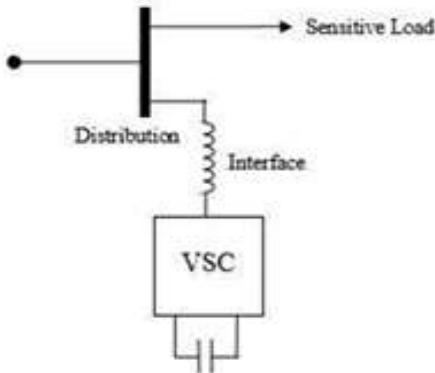


Fig 3: DTSATCOM

V. Simulation Models of DSTATCOM

B. DSTATCOM with no capacitor

The DSTATCOM is controlled in a mean way that it trades receptive force with the framework when it is associated with the network through the coupling inductor at the Point of Common Coupling (PCC) by infusing the current in quadrature with matrix voltage.

The DSTATCOM is operated in the capacitive mode when the magnitude of the grid voltage (V_s) is lesser than the DSTATCOM voltage (V_c) i.e $V_c > V_s$. Refer figure 5.1.

The DSTATCOM absorbs the reactive power from the grid when the DSTATCOM voltage (V_c) is less than the grid voltage (V_s) $V_s > V_c$ and it operates in inductive mode. Refer figure 5.2 Power and it is operated in floating mode $V_c = V_s$. Refer figure 5.3

When the magnitudes of both DSTATCOM (V_c) and grid voltage (V_s) are equal then there is no exchange of reactive

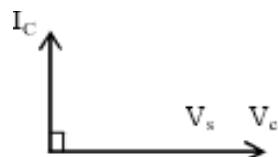


Fig 4.1

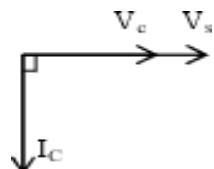


Fig 4.2



Fig 4.3

Fig. 4.4 DSTATCOM connected to a power system without capacitor

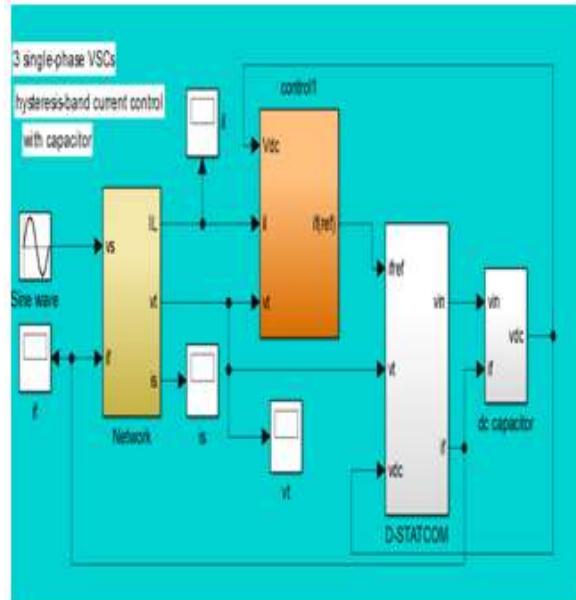


Fig 4.5: DSTATCOM connected to a power system without capacitor

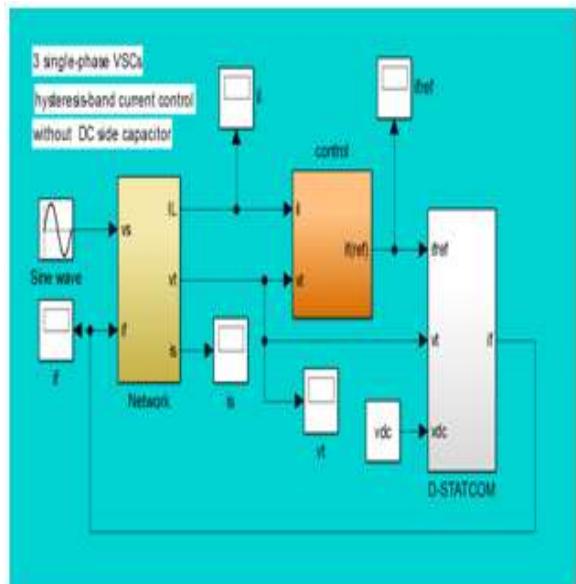


Fig 4.6: DSTATCOM connected to a power system with capacitor

DSTATCOM With capacitor PWM model

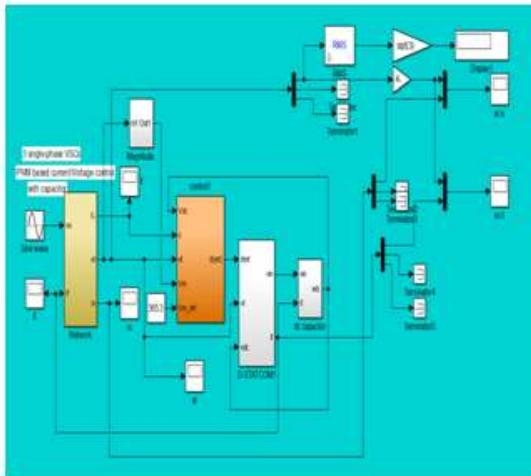


Fig 4.7: DSTATCOM connected to power system with PWM model

VI. Dynamic Voltage Restorer

The process involves injection of active/reactive power from DVR to distribution feeder [21].

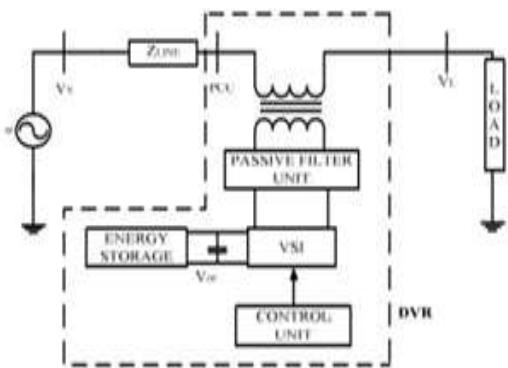


Fig 5: Basic Structure Of DVR

A. Dynamic Voltage Restorer Simulation

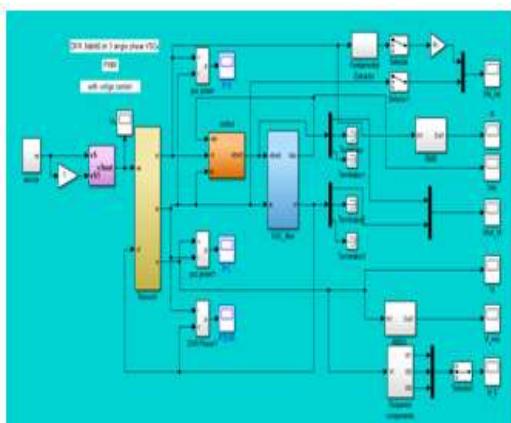


Fig 5.1: simulation of DVR connected to power system with voltage source converter filter

Source Specifications

$$\begin{aligned} f &= 50 \\ T &= 1/f \quad w = 2\pi f \quad L_s = 40e-3 \\ R_s &= w \cdot L_s / 8 \end{aligned}$$

Load specifications

$$\begin{aligned} R_1 &= 50 \quad R_2 = 50 \quad R_3 = 50 \quad L_1 = 200e-3 \quad L_2 = 200e-3 \\ L_3 &= 200e-3 \end{aligned}$$

DVR specifications

$$\begin{aligned} V_{dc_ref} &= 500 \quad C_d = 5000e-6 \quad R_d = 6000 \\ F_s &= 100*f \quad T_s = 1/f_s \quad PLL \\ K_p_pll &= 15000 \quad K_i_pll = 60000 \end{aligned}$$

DC voltage control

$$\begin{aligned} K_p_dc &= 40 \quad K_i_dc = 80 \quad k_i_inph = 7 \quad K_p_vc = 10 \quad K_i_vc = 40 \quad tstep = 0.2 \quad R_f = 0.1 \quad C_f = 4.2e-6 \quad L_f = 9.6e-3 \\ f_n &= 1/(2\pi\sqrt{L_f \cdot C_f}) \\ V_{lref} &= 400 \quad w_n = 2\pi \cdot 30 \quad \zeta = 1/\sqrt{2} \quad num = w_n^2 \\ den &= [1 \ 2\zeta w_n \ w_n^2] \end{aligned}$$

VII. Results

In this section, simulation results of promising control topologies used in three phase STATCOM. The objective of the simulation is to study different performance aspects on 3 phase uses hysteresis band current control with Dc capacitor and Without Dc capacitor based D- STATCOM.

Observing the variation between with and without capacitor of D-STATCOM

Reference with Capacitor:

D-STATCOM manages the framework voltage dependent on a characterized reference (VREF). In the event that the Voltage of the framework is lower than the reference voltage (VREF). D-STATCOM works with in capacitive mode and if Voltage of the framework is higher than the reference voltage, D-STATCOM works in inductive mode.

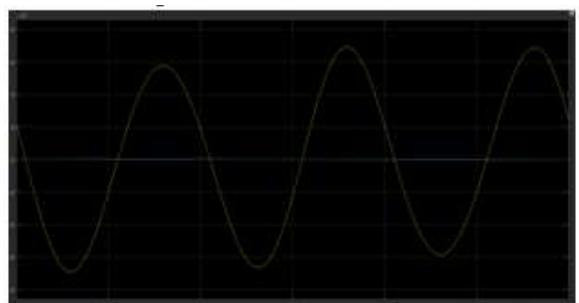


Fig 6: shows the V reference chart with capacitor.

Voltage and Current with Capacitor

In V-I characteristics if control voltage of the controlled point by adjusting the measure of infused or assimilated receptive force as long as the trade responsive force remains inside the most extreme and least restricts, the voltage is directed. V-I characteristics with capacitor are appeared in Figure 6.1

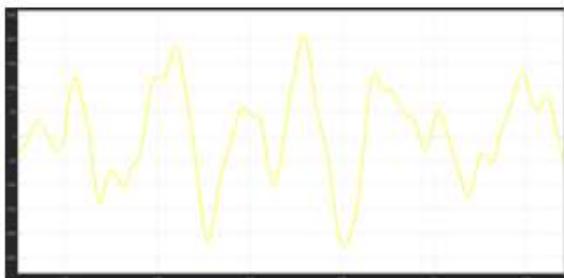


Fig 6.1: V-I characteristics with capacitor

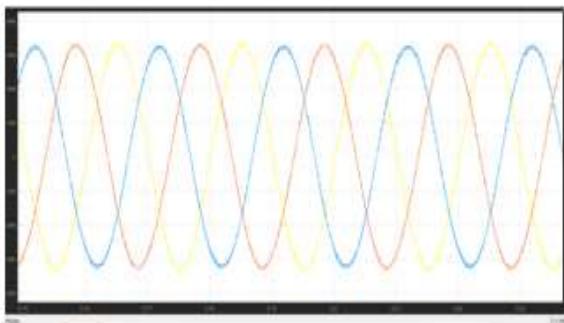


Fig 6.2: Three phase supply Voltage with capacitor using D- STATCOM

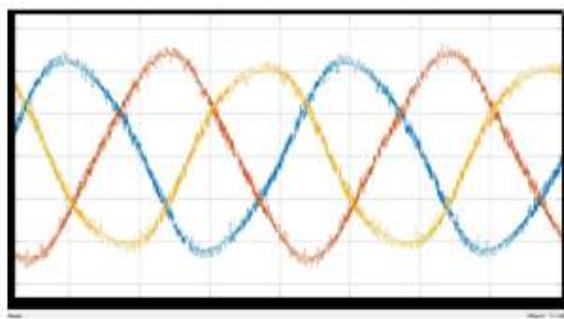


Fig 6.3: Three phase supply current with capacitor using D- STATCOM

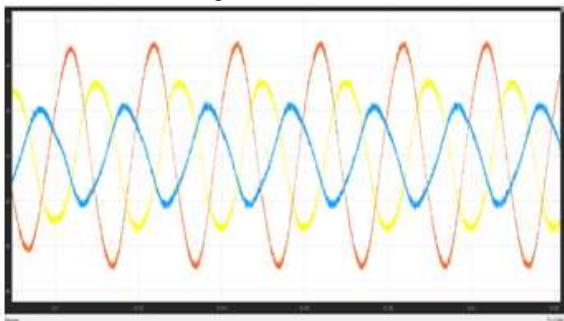


Fig 6.4: Field current with capacitor using D- STATCOM

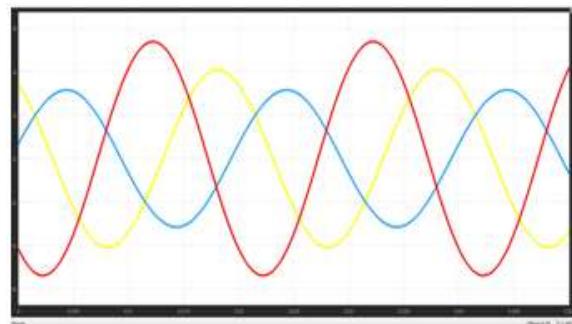


Fig 6.5: Load current with capacitor using D- STATCOM

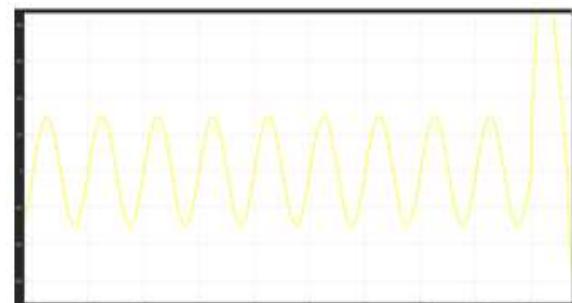


Fig 6.6: V-I Characteristics with capacitor using DVR

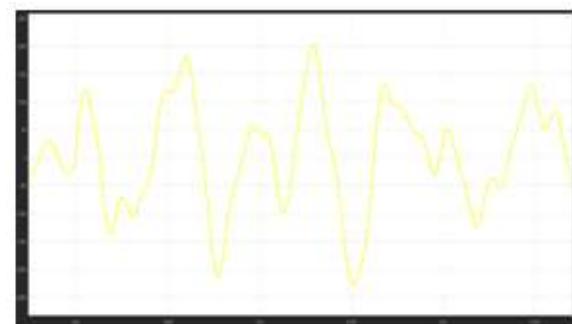


Fig 6.7: V-I Characteristics with capacitor using DVR

Load Current with DVR

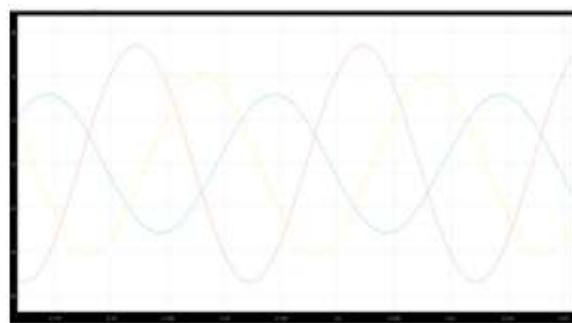


Fig 6.8: Load current with capacitor using DVR

VIII. Conclusion

In this PQ issues in smart grid in reviewed by studying literature of recent years and distributed generation system like solar, wind based PQ issues discussed. In this research outcome, PQ issues are due to voltage sag, swell and interruptions. It has been determined that DSTATCOM and DVR has possible choice due to the rewards it offers.

IX. Future Scope

Power Electronics system is a significant expertise for distribution networks which can transfer electrical power from renewable energy sources to grids or generate regulated frequency and voltage for dissimilar loads such as variable speed drives and battery chargers. Due to of smart distribution grid New demands for i) price and size reduction, ii) performance and quality improvement and iii) flexibility on power management have helped power electronics applications widely in industrial, commercial and residential sectors such as in transportation, utility and home appliances in the recent years.

References

- [1] A. E. Hammad, "Comparing the voltage source capability of present and future var compensation techniques in transmis, July/August, PP. 682-688, 1999.ery. Volume1. No.1 Jan 1995.
- [2] G. Yalisenkaya, M.H.J Bollen, P.A. Crossley, "Characterization of voltage sags in industrial distribution system", IEEE Trans on industry applications, volume 34, No, July/August, PP.682-688, 1999.
- [3] Anaya-Lara O, Acha E., "Modelling and analysis of Custom Power Systems by PSCAD/EMTDC ", IEEE Trans on power Delivery , Volume 17, Isuue:2002, Pages: 266-272.
- [4] Haque , M.H., " Compensation of Distribution Systems Voltage sags by DVR and D-STATCOM", Power Tech Proceedings,2001 IEEE Porto, Volume 1, PP. 10-13, September 2001.
- [5] Wind Turbine Generating System—Part 21, International standard-IEC61400-21, 2001.
- [6] Yuvaraj and Dr. S.N.Deepa, " Improving grid power quality with FACTS Devices on Integration of Wind Energy System" Student Pulse April 2011 Vol. 3, Issue 4.
- [7] S. Heier, Grid Integration of Wind Energy Conversions. Hoboken, NJ: Wiley, 2007, pp. 256–259.
- [8] J. J. Gutierrez, J. Ruiz, L. Leturiondo, and A. Lazcano, "Flicker measurement system for wind turbine certification," IEEE Trans.Instrum. Meas., vol. 58, no. 2, pp. 375–382, Feb. 2009.
- [9] Indian Wind Grid Code Draft report on, Jul. 2009, pp. 15–18, C-NET.
- [10] Sharad W. Mohod and Mohan V. Aware, " A-STATCOM control scheme for grid connected wind energy system for power quality improvement", IEEE System Journal, Vol. 4,No. 3, Septe
- [11] C. Han, A. Q. Huang, M. Baran, S. Bhattacharya, and W. Litzenberger, "STATCOM impact study on the integration of a large wind farm into a weak loop power system," IEEE Trans. Energy Conv., vol. 23, no. 1, pp. 226–232, Mar. 2008.
- [12] D. L. Yao, S. S. Choi, K. J. Tseng, and T. T. Lie, "A statistical approach to the design of a dispatchable wind power—Battery energy storage system," IEEE Trans. Energy Conv., vol. 24, no. 4, Dec. 2009.
- [13] F. Zhou, G. Joos, and C. Abhey, "Voltage stability in weak connection wind farm," in IEEE PES Gen Meeting,2005, vol. 2, pp 1483–1488.
- [14] T. Kinjo and T. Senju, " Output leveling of renewable energy by electric double layer capacitor applied for energy storage system", IEEE Trans. Energy Conv., Vol 21, No 1, March 2006.
- [15] R. S. Bhatia, S.P. Jain, D.K. Jain and B. Singh, " Battery Energy Storage System for power conditioning of renewable energy sources", in Proc. Int. Conf. Power Electron Drives System, Jan. 2006, Vol. 1, PP. 501-506.
- [16] K. Somsai and T. Kulworawanichpong , " Instantaneous Power control of D-STATCOM with consideration of power factor correction", IEEE International conf. on May 2010, PP. 1186-1190.
- [17] H. Akagi, E. H. Watanabe and M. Arede, "Instantaneous Power theory and Application to power conditioning", Hobo.

Power Quality Conditioning By UPQC Using DQ Theory

M Balasubbaredy

Department of EEE,

Chaitanya Bharathi Institute of Technology,
Hyderabad-500075, India.
balasubbaredy79@gmail.com

Saini Varshini

Department of EEE,

Chaitanya Bharathi Institute of Technology,
Hyderabad-500075, India.
varshiniraosaini@gmail.com

Abstract: the people are utilizing power for many works to be finished in a day and the electricity has become a major part in our daily life due to this there is a rapid increase in power demand. This lead to the problem of supplying quality power to the purchasers. As a solution to this problem here we proposed a unified power quality conditioner (UPQC) to satisfy consumers by providing them harmonic free and quality in the power supply. The UPQC is combining series and shunt active filter. This is generally placed near to the source and before the load. It solves all the power quality problems that are related to current and voltage, and provides the consumers a harmonics-free power supply. Here we need sensed source voltage and current, load voltage and current which can be obtained by sensing them through sensors. To obtain the reference signals synchronous reference frame dq theory (DQ theory) is used. Compensating voltage to be injected in line is obtained from the reference signals and the sensed signals. The nonlinear loads that are connected at the consumer side injects voltage swell, voltage sag, flicker, voltage imbalances into the line which does not allow for providing quality power supply. Here we proposed solution for the problem of voltage swell and sag by using UPQC with DQ theory.

Keywords: unified power quality conditioner, voltage sag and harmonics, active filters, power quality.

I. Introduction

Unified power quality conditioner (UPQC) was proposed to increase the power system working and had went through various modifications to increase the performance[1]. generally, UPQC had been implemented successfully for mitigating or to compress the many power quality (PQ) problems like voltage sag/swell, flicker, harmonics, fluctuations, unbalanced voltages, poor power factor and currents, load current harmonics, neutral and reactive current[2-3]. The Research on the UPQC has improved tremendously over last decade in the areas like type of converter in UPQC (CSC or VSC), the supply system (single-phase and three-phase), and the configuration of the UPQC topologies [4-5]. All the above power quality issues cannot be solved in one topology configuration, but based each issue priority, they can be dealt accordingly.

The APFs (active power filters), like series APF, shunt APF and hybrid APFs are widely used to mitigate the power quality related problems .The decreasing quality of the power is mainly due to voltage and current harmonics mainly because of wide spread of application the power electronics converters static negative and zero sequence components obtained by utilizing the single phase and unbalanced loads. Therefore, it's very important to maintain high standard of power quality [6].

The unified power quality conditioner (UPQC), also known as hybrid filter, is the most precise hybrid filter design. UPQC is a multi-role power conditioner which is shunt and series active filter combination that is connected in cascade through DC link capacitor that is utilized to eliminate many disturbances in power supply, to clear fluctuations in voltage, and to check load current harmonics entering into the power system[7],[8].

This is the traditional and widely acceptable power device utilized to suppress the disturbances that affect the behavior of critical and sensitive loads. The UPQC has series and shunt compensation abilities for reactive power, harmonics, and power-flow control and voltage disturbances. The UPQC consists of the two voltage-source converters connected through DC link designed in three-phase three-wire, single phase or three-phase four-wire topologies.

One of the converters is combined through a transformer in series between nonlinear load and source at PCC and functions as voltage-source inverter. One more inverter is connected through a transformer in shunt at PCC and operates as current-source inverter. Series active inverter performs harmonic isolation, compensates the voltage supply disturbances and eliminates harmonic oscillations. Shunt active inverter eliminates the reactive power,load current distortions and performs the DC link voltage regulation.

The series converter of UPQC acts as the voltage source controller that it performs as the series APF, whereas the PWM shunt converter acts like the current source controller that it performs as the shunt APF. The Power supply is been not connected at the common DC link. It just contains only the small DC capacitor the Energy storage element.

The PQ theory was implemented in UPQC [9]-[11], [13], but it is not very advantageous during grid conditions are non-ideal. So DQ control scheme with the phase locked loop (PLL) implemented is used in with UPQC for more effective use.

II. Construction of Proposed UPQC

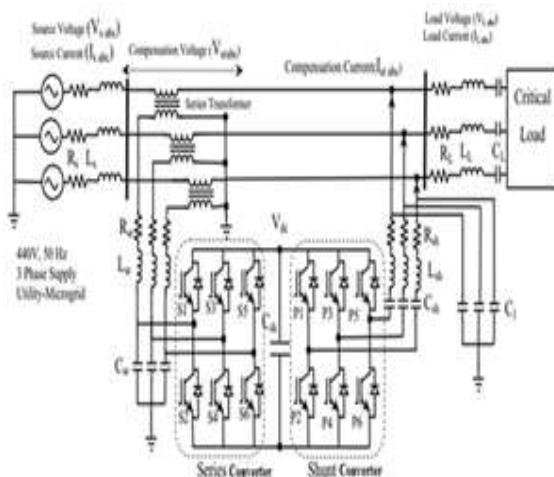


Fig 1: proposed UPQC model construction.

The construction of proposed network of UPQC given in fig.1. Here UPQC is connected between load and source. There is common DC link placed between the converters. The series inverter is series connected with load and it injects compensating voltage into the line through transformers. The shunt converter attached across the load and it adds UPQC current into line. The power supply is not supplied at the dc link [12].

III. Reference Signal Generation Technique

Most of the control schemes published for shunt and series active filters are applied for Upqc. Various reference generation techniques can be applied while using UPQC for improvement of power quality. Each technique has both advantages and disadvantages. The algorithm can be chosen based on the power quality problem to be eliminated.

A. Reference Signal for the Series APF and shunt APF

The purpose of series voltage controller is to compensate all the source side voltage disturbances, which has happened due to the fault occurred in distribution line[14]. The series APF control technique computes reference value of the voltage that is to be injected by series APF comparing load side line voltages with the positive sequence components. The proposed voltage reference signal

for the series APF is computed by using the d-q theory.

ABC to dq0 conversion:

$$\begin{bmatrix} v_{s0} \\ v_{sd} \\ v_{sq} \end{bmatrix} = \frac{2}{3} \begin{bmatrix} 1 & 1 & 1 \\ \frac{1}{2} \sin \omega t & \sin \left(\omega t - \frac{2\pi}{3} \right) & \sin \left(\omega t + \frac{2\pi}{3} \right) \\ \cos \omega t & \cos \left(\omega t - \frac{2\pi}{3} \right) & \cos \left(\omega t + \frac{2\pi}{3} \right) \end{bmatrix} \begin{bmatrix} v_{sa} \\ v_{sb} \\ v_{sc} \end{bmatrix} \quad (1)$$

dq0 to ABC conversion:

$$\begin{bmatrix} v_{s0}^* \\ v_{sd}^* \\ v_{sq}^* \end{bmatrix} = \frac{2}{3} \begin{bmatrix} 1 & \sin \omega t & \cos \omega t \\ 1 & \sin \left(\omega t - \frac{2\pi}{3} \right) & \cos \left(\omega t - \frac{2\pi}{3} \right) \\ 1 & \sin \left(\omega t + \frac{2\pi}{3} \right) & \cos \left(\omega t + \frac{2\pi}{3} \right) \end{bmatrix} \begin{bmatrix} v_{sa} \\ v_{sb} \\ v_{sc} \end{bmatrix} \quad (2)$$

The three phase reference voltages can be computed using equation (2). These calculated voltage references are then compared to the load line voltages and obtained errors are sent through the PWM sinusoidal controller. This generates required switching signals that are then given to IGBT switches of series APF.

The demonstrated shunt APF is generally utilized to compensate the reactive power and current harmonics generated by nonlinear load. Voltage control and power extraction

1) Load power:

$$\begin{aligned} v_{ld} i_{ld} + v_{lq} i_{lq} &= P_L \\ v_{ld} i_{lq} + v_{lq} i_{ld} &= Q_L \\ v_{l0} i_{l0} &= P_{0L} \end{aligned}$$

2) Reference power:

$$\begin{aligned} v_{sd} i_{ld} + v_{sq} i_{lq} &= P_{L1} \\ v_{sq} i_{lq} + v_{sd} i_{ld} &= Q_{L1} \\ v_{s0} i_{l0} &= P_{0L1} \end{aligned}$$

3) DC power:

$$(v_{dc} * i_{PI}) \frac{1}{\sqrt{2}} = P_{dc}$$

Where is the current obtained by passing and through a PI controller.

$$P_L - P_{dc} = P$$

$$Q_L = Q$$

All these equations are utilized for generating reference signals that are required. After obtaining reference signals, the reference signal and the actual signal are passed through the PWM controller for generating gate pulses required for the triggering the IGBT switches and they generate the compensating voltage according to the gate pulse given. In this way the harmonics generated are being eliminated.

IV. Performance Analysis of the Proposed D-Q Synchronous Reference Frame Based Control of the UPQC by the Simulation Study.

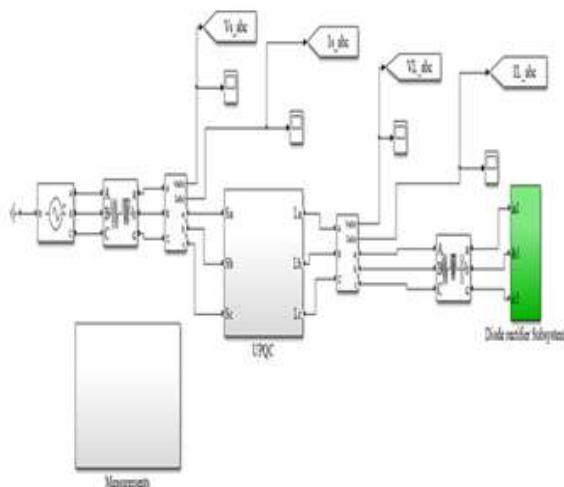


Fig 2: upqc connected between load and three phase source.

The upqc connected in between load and source for injecting the compensating signal into the line and eliminating the harmonics as required. The connection of upqc between source and load is shown in fig 2.

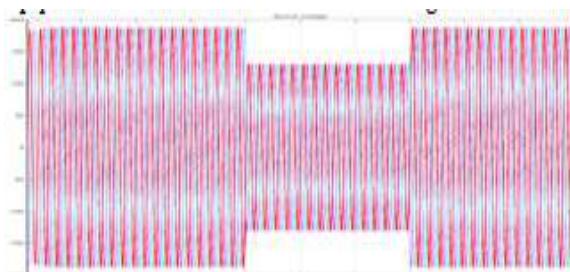


Fig 3: voltage supplied

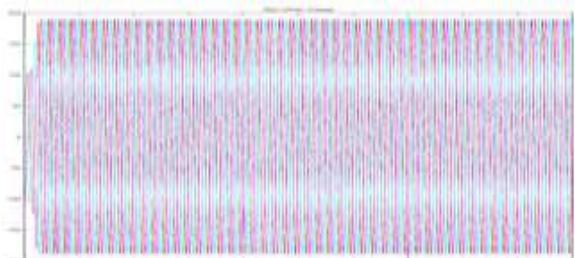


Fig 4: after voltage compensation

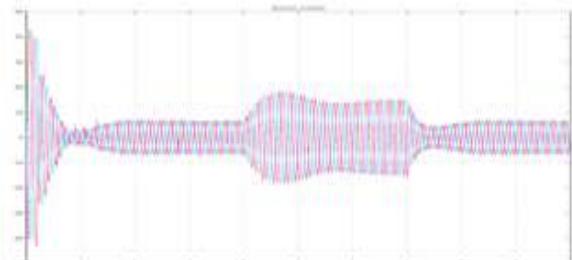


Fig 5: current at source

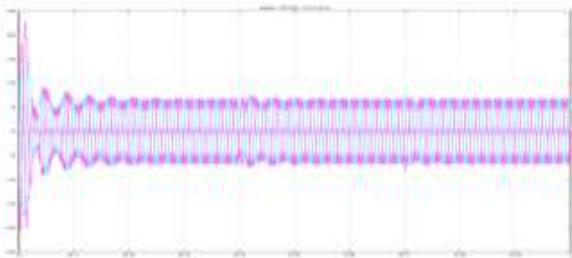


Fig 6: current after compensation

The performance evaluation of the proposed three-phase d-q reference synchronous frame control based on the controller for the UPQC is explained by obtained simulation study. The Simulink/MATLAB based simulation results is displayed. Where the fig 3. Represents the simulation output of source voltage sag condition from time 0.4sec to 0.7sec due to the harmonics injected by the nonlinear load. Then after injecting the compensating voltage the sag condition is controlled as shown in fig 4. That is load voltage after UPQC compensation as noticed series converter eliminates harmonics that are present in supply voltage. Similarly fig 5. Displays the swell condition from time 0.4 sec to 0.7 sec then after UPQC compensation the swell is controlled as the result shown in fig 6. Thus, the experimental study exhibits the concept of three-phase d-q synchronous reference frame can be used for three phase UPQC configuration for load current and supply voltage harmonics compensations at the same time.

V. Conclusion

UPQC is installed for the elimination of voltage sag and current distortions in a 3P3W distribution. The UPQC model presented here can also be enhanced for future emerging distribution systems. For mitigation of power quality problems

the proposed UPQC model. Here we successfully mitigated voltage sag and current distortions using UPQC by DQ theory. The power quality problems such as distorted currents and unbalanced voltages are successfully eliminated by the proposed technique which is proved by the simulation study. Therefore, with harmonics-free and with eliminated power quality problems the power is supplied to consumers. This is much better compared to the active filters that are being used and this is proved by the provided experimental results.

power quality control and continuous diagnostics," IEEE Trans. Power Del., vol. 13, no. 4, pp. 1494–1500, Oct. 1998.

- [14] M. Aredes and E. H. Watanabe, "Three-phase four-wire shunt active filter control strategies," IEEE Trans. Power Electron., vol. 12, no. 2, pp. 311–318, Mar. 1997.
- ## References
- [1] Akagi, H. 1996. New trends in active filters for power conditioning. IEEE Trans. Ind. Applicat., 32(6):1312–1322
 - [2] D. Graovac, A. Katic, and A. Rufer, "Power Quality Problems Compensation with Universal Power Quality Conditioning System," IEEE Transaction on Power Delivery, vol. 22, no. 2, 2007.
 - [3] Khadkikar, V. & Chandra, A. 2011. UPQC-S: A novel concept of simultaneous voltage sag/swell and load reactive power compensations utilizing series inverter of UPQC. IEEE Trans. Power Electronics, 26(9):2415-2425.
 - [4] Ketabi, A., Farshadnia, M., Malekpour, M. & Feuillet, R. 2012. A new control strategy for active power line conditioner (APLC) using adaptive notch filter. Elsevier, Int.J. Electrical Power and Energy Systems, 47:31-40.
 - [5] Khadkikar, V. 2012. Enhancing electric power quality using UPQC: A comprehensive overview. IEEE Trans. Power Electronics, 27(5):2484-2497.
 - [6] Vinod Khadkikar, "Enhancing Electric Power Quality Using UPQC: A Comprehensive Overview", IEEE TRANSACTIONS ON POWER ELECTRONICS, Vol. 27, No. 5, MAY 2012.
 - [7] S. N. Gohil,"Three phase unified power quality conditioner ffo power quality improvement using UVTG technique", ICRESE, 2013.
 - [8] Mehdi Forghani and Saeed Afsharnia," Online Wavelet Transform-Based Control Strategy for UPQC Control System", IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 22, NO. 1, JANUARY 2007.
 - [9] A. R. Reisi, M. H. Moradi, and H. Showkati, "Combined photovoltaic and unified power quality controller to improve power quality," Solar Energy, vol. 88, pp. 154–162, 2013.
 - [10] B. Rahmani, W. Li, and G. Liu, "An advanced universal power quality conditioning system and MPPT method for grid integration of photovoltaic systems," International Journal of Electrical Power & Energy Systems, vol. 69, pp. 76–84, 2015.
 - [11] A. Shrivastava and P. Nene, "Power quality enhancement using upqc connected with pv arrays," in Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on. IEEE, 2015, pp. 1232–1237.
 - [12] M. Aredes, K. Heumann, and E. H. Watanabe, "An universal active power line conditioner," IEEE Trans. Power Del., vol. 13, no. 2, pp. 545–551, Apr. 1998.
 - [13] J. S. Hsul, "Instantaneous phasor method for obtaining instantaneous balanced fundamental components for

Session-B2:
Big Data and Data Mining

Ransomware Attacks – Prevention and Mitigation

Mandru Suma Sri

Department of Computer networks and
Information Security
Chaitanya Bharathi Institute of Technology
, Hyderabad-500075, India
mandrusumasri98@gmail.com

Rayapati Goutham

Department of Cyber Forensic and Security
Illinois Institute of Technology
Illinois, US
grayapati@hawk.iit.edu

Abstract: Cyber-attacks are increasing day by day. Ransomware has become one of the major cyber-attacks in the past 15 years which causes heavy loss to the organizations and an individual. It is one of the fastest growing cybercrimes which has set its prime target as healthcare, where it can be on an individual or an organization. A successful ransomware attack on an organization causes loss of business and permanent loss of data. The ransomware encrypts the data on the victim computer and holds it until some ransom is paid. The main purpose of the ransomware attack is to gain money from the victim and the payment option used by the ransomware attackers is cryptocurrency as the transaction cannot be tracked. Sometimes even after paying the ransom, the data may not be released by the attacker. There are some preventive measures to be taken for various ransomware attacks. This paper discusses the operation of ransomware and its targets and also investigates on protecting against the ransomware attacks and mitigating the risk of ransomware attack along with the future of ransomware attacks. Different types of ransomware attacks and the way they perform the attack is also discussed in this paper.

Keywords: Ransomware, Cyber-attacks, malware, Vulnerability, WannaCry

I. Introduction

Ransomware is nothing but a type of malware and its concept is as old as crime. The word Ransomware is made out of two words, ransom and malware. This malware encrypts the data on victim's device and hold until ransom is paid for the attacker. It has become one of the fastest growing cyber-attacks affecting businesses of all sizes. Since the mid-2000s, this has been a major threat to SMB's and individuals (Groot, 2019). Earlier when it was developed in late 1980's, the ransom was to be sent via snail mail. In current days, Ransomware authors are using cryptocurrencies as the payment method because of the anonymity of transactions. Once the attackers verify payment, then they provide decryption key or software. Previously attackers try to infect ransomware by sending phishing links or by downloads from compromised sites but WannaCry was made to install by using known vulnerability on computers. The fact was that the vulnerability

WannaCry had exploited and actually been identified by National Security Agency and was built on a system developed by a static security agency. An average computer takes 6.4 quadrillion years for cracking the key that is encrypted by a typical ransomware which uses RSA 2048 encryption algorithm to encrypt files. There are some best practices to protect organization from ransomware attacks. The advice given by the FBI is to never pay the ransom if you are infected with ransomware. Even if you pay the ransom there is no guarantee that you will get the data back. 467,361 complaints were received by FBI in the year 2019 and more incidents were reported to FBI than any previous year. The Internet Crime Complaint Center which is known as IC3 has received more than 1,200 complaints each day in the last five years, since from its foundation. According to FBI, \$3.5 billion was lost to cyber criminals in 2019. The most damage was caused by business email compromise.

A. Ransomware

Ransomware is a malicious software that encrypt files and locks the computer and prevents user from accessing it until a ransom is paid by the user (Manning, 2017). The basic idea behind ransomware is simple, a malicious software will lock and encrypt the data present in the victim's computer and then the attackers will ask for ransom to decrypt the data. In certain situations, the victims are extorted to pay the ransom within the given time or else they lose the data forever ("What is Ransomware and how", n.d.). As these attacks are being carried out by the cyber criminals, there is no assurance that victim will get the data back on paying ransom. Ransomware does not delete files in the device but makes inaccessible to the user. Ransomware can be of different forms but in its pith, it denies access to files until some ransom has been paid. The attackers usually use the following vectors to infect a machine. They are phishing emails, compromised websites, unpatched programs and free software downloads.

B. How Ransomware attacks work?

Now let's go more detailed about how these malware gain access to device data. The term "ransomware" itself explains the function of the malware which extorts users for financial gain (Groot, 2019). Ransomware usually spreads through

phishing mails or spam or through websites. There are five steps in a typical ransomware attack which are given below

- a. Infection: In the first step, the ransomware is delivered to the system through phishing mail or infected application, and then it installs itself on an end point and other network devices to which it has access (Bauer, 2019).
- b. Secure Key Exchange: Here, the malware connects with command-and-control server which is operated by the attackers and then generates and exchanges the cryptographic key.
- c. Encryption: After the key exchange, ransomware starts encrypting files on the computer and also on any connected storage devices.
- d. Extortion: After encrypting the files, Ransomware displays instructions on how to make ransom payment or else threatens of deleting the decryption key.
- e. Unlocking: Companies pay the ransom and hope for the attackers to decrypt the data, though there is no guarantee that they will decrypt the files. Another method is removing infected files and restore files from backups (Bauer, 2019.).

C. How malware enters into computer?

There are many ways for viruses to enter into computer. The malware gets hold of device data through infection vectors. These attack vectors are of two types.

- a. Human Attack Vectors: If the malware enters your computer by the action of human, then it is infected through human attack vector. The activities of humans include opening the E-Mail attachments that appear to be from legitimate users and through messages on social media which has some file attachments and Pop-ups which imitate commonly used software (Groot, 2019).
- b. Machine Attack Vectors: If the malware enters into your computer by the action of machine, then it is infected through machine attack vector which includes Drive-By, which infects the system just by opening the page with malicious code image. The systems with vulnerabilities are exploited and also propagates through the network from one infected system. (Bauer, 2019).

D. Operation of Ransomware

Ransomware encrypts both the local and network shared files with high encryption capabilities. The targeted file types of ransomware include images, videos, documents, database files, digital certificates, gaming profiles, etc. After

encrypting the malware sends back the encryption key to the control and command server (C2 server) and leaves extortion message as if it were pop-up on desktop of infected computer (Groot, 2019). In order to get the decryption key, it asks for ransom in the form of bitcoins otherwise the unique decryption key will be deleted. Due to strong encryption algorithm used by ransomware it is very difficult to decrypt the data without decryption key (Groot, 2019).

E. The future of Ransomware

The ransomware attacks till now are catapulting ransomware into a new era, for an instance attacker can easily duplicate smaller attacks and carry them out against much larger organization in order to demand greater ransom (Groot, 2019). The recent ransomware Crypto locker extorted around \$3 million from users but not all those who got their files decrypted (Groot, 2019). Datto's study showed that cyber criminals neglected to decrypt users' files in one out of each four cases even when ransom was paid. The creators of Cerber ransomware were particularly greedy, offering their ransomware operations as service in return for a 40% cut of the profits earned through ransom. As indicated by Check Point Researchers, Cerber ransomware infected about 150,000 victims on its own July 2016, earning an estimated \$195,000 of which \$78,000 went to the creators of ransomware (Groot, 2019).

A recent study from the United Kingdom's National Cyber Security Centre (NCSC) and National Crime Agency (NCA), warns against threats like mobile ransomware and ransomware-as-a-service (Groot, 2019).

II. Overview

A. Types of ransomware

Ransomware attacks can take various forms. Some ransomware could be of more damaging than others, but the common thing between them is ransom. Below are the ransomware types.

- a. Encrypting Ransomware: This type of malware once executed, searches for valuable files on victim's device and encrypts them. After encrypting, a message asking ransom and detailed instructions regarding the payment are displayed on the screen for file decryption. After the ransom is paid, they will provide a key or code for the decryption of data or an executable file specially for the decryption of data on that particular machine. Encryption ransomware took prominence in 2013 with CryptoLocker ransomware which used bitcoin digital currency platform to collect ransom. The examples of

encrypting ransomware are CryptoLocker, WannaCry and CryptoWall.

- b. Non-Encrypting Ransomware: This class of malware does not use encryption. Once executed, it locks the device and restrict access to the files. After locking the device, it asks for a user action or ransom which ends up costing money to unlock the device. Most of these ransomware attackers ask the user to send a premium-rate SMS or call high-rate phone number to get a code that could be used to unlock the device. In the year 2011, a non-encrypted ransomware emerged that imitated the windows product activation notice, making it difficult for users in finding out the genuine notifications and threats (Sjouwerman, n.d.). Winlocker is the typical example of non-encrypting ransomware.
- c. Leakware or Doxware: This is a type of ransomware which does not encrypt the files or restrict the user from accessing the device (Sjouwerman, n.d.), rather it silently collects sensitive information from the device and uses it to threaten or blackmail the victim. As people store sensitive files and personal photos on computer, it is understandable that some people get panic and pay the ransom if their data is hijacked. The collected sensitive data is stored by attacker and threatens to publish the stolen information if the payment is not made. Thus, the attacker blackmails the user to publish sensitive information if ransom is not paid.
- d. Mobile Ransomware: The ransomwares targeting mobile operating systems has increased rapidly in the recent times. It is very easy to back-up and restore the data from cloud in mobile phones. Usually, these malwares act as blockers, with little incentive to encrypt data. Typically, the payload is distributed as an APK file, installed by an unwitting user and attempts to display a blocking message through all other applications. While others use a form of click-jacking to cause the user to allow its higher privileges in order gain deeper access (Anghel, 2019).

B. Notable Ransomware Attacks

Now let's explore some notable ransomware attacks and understand how dangerous and different each type can be.

- a. CryptoLocker: This ransomware was first seen in 2007. This malware spreads via infected email attachments. After execution, it searches for important and sensitive files to be encrypted and stored for ransom. It was believed to have compromised about 500,000 computers, law

enforcement and security companies finally succeeded in catching a global network of home computers that were being used to spread this ransomware. CryptoLocker reappeared in 2013 as an encrypting ransomware. This CryptoLocker used 2048-bit RSA encryption algorithm to encrypt the data and used bitcoin as payment method. This malware threatened to remove the decryption key if payment had not been made within 3 days of the infection. Even after 3 days we can use an online tool to get the decryption key, but the price could increase to 10 bitcoins which is about \$2300 in the year 2013. These attacks infected more than 250,000 computers and \$3 million was extorted before taking it offline.

- b. CryptoWall: CryptoWall was first appeared in 2014 and targeted windows operating system. CryptoWall uses java vulnerability. Malicious ads on domains belonging to Disney, Facebook and several other websites redirected to websites that exploited browser plugin to download payload in the system. The FBI reported that almost 1,000 victims had approached the IC3 for reporting CryptoWall infections in June 2015. It is estimated that the malware will reap at least \$18 million.
- c. Petya: Petya ransomware attack first hit in the year 2016. Instead of encrypting specific files, this ransomware was designed to infect the entire master boot record and shutting the computer from running into windows until ransom is paid. It encrypts the entire hard disk making it impossible to access the files. Petya ransomware spread through a fake job email with a drop box link which is infected.

Petya's updated version was used for global cyber-attack which targeted Ukraine in 2017. This version also used the EternalBlue exploit which was previously used in WannaCry ransomware. Whereas, modified version cannot unlock the system even after the ransom is paid. So, this attack was done just to cause disruption and not for ransom.

- d. WannaCry: WannaCry is an encrypting ransomware which was spread over 150 countries in 2017. This ransomware used vulnerabilities in windows to exploit the systems and the exploit was reportedly developed by National Security Agency and leaked by The Shadow Brokers team. This attack caused an estimated financial loss of \$4 billion and infected over 230,000 computers globally.
- e. It demanded ransom in the form of bitcoin around \$300 per computer. This ransomware

spread anonymously and disrupted businesses globally. The National Health Service of British was highly affected by this ransomware

- f. Syskey: This is not a ransomware but a scam. Syskey is a windows-NT operating system tool that encrypts the user account database with a password. A caller with remote access as technical support locks the computer with a password using this tool. This tool was removed in later version of windows.
- g. Bad Rabbit: Bad Rabbit is ransomware and it followed similar patterns of WannaCry and Petya by encrypting users' hard disk and then demanding bitcoin as ransom. But this ransomware did not used EternalBlue exploit. During this attack, user visits a legitimate website which have been compromised by the attacker which requires no action from the user. The user has to do nothing beyond browsing the compromised web page. This ransomware is a false request for you to install abode flash player as malware dropper to spread the infection. The sites which are spreading this malware have gone offline after few days of its discovery.
- h. TeslaCrypt: It is a ransomware that targets game-play data for computer games such as Call of Duty, Minecraft and World of Tanks. It encrypts some files of the games like save data, player profile, custom maps. The recent version of this ransomware targets word file, jpeg file including game files. It demanded \$500 worth BTC as ransom per computer. This malware was infected through angler adobe flash exploit. Ransomware claimed that TeslaCrypt used asymmetric encryption, but Cisco researchers found that symmetric encryption was used in this ransomware and developed a decryption tool. At last, in May 2016, TeslaCrypt developers has shut down this ransomware and released master key. Later, ESET Developed and released a tool to decrypt the infected computers at free of cost.

C. Impacts of Ransomware Attacks

The impacts of ransomware attack on a business organization could include the following:

- a. Temporary or permanent loss of organization's data.
- b. Potential harm to organization's reputation.
- c. Financial loss to the business
- d. Possibly a complete shutdown of company.

D. How to Defeat Ransomware?

If you are infected with ransomware, do not pay for ransom immediately. The advice endorsed by

FBI is never pay the ransom if you are infected with ransomware. Do the following steps to mitigate the risk of ransomware.

- a. Isolate the infection: The first thing to do is isolate the infected computer from other devices and storage. Prevent the ransomware from spreading all the computers in the network by isolating it. Disconnect it from the network and any other storage devices. Isolating from network prevents ransomware communicating with command-and-control center.
- b. Identify the infection: There are many sites to help in identifying ransomware. Identifying the type of ransomware helps you in understanding what type of files it encrypts? Whether it is an encrypting ransomware or not? And what are the options to recover? So always identity what type of ransomware you are infected with and it is also recommended to report the attack to authorities.
- c. Report to the Authorities: Always report the attack to authorities regardless of the outcome. Reports can be filed with the FBI at the Internet Crime Complaint Center (IC3). Knowing more about the victims experiences will help FBI in finding the attackers (Bauer, 2019).
- d. Determine Your Options: There are three options for an individual if he is infected with the ransomware. They are: Pay ransom to the attacker, try to remove malware, Format the system and reinstall it and it is not advised to pay the ransom, though you pay ransom there will be no guarantee that you will get the data back. So that remains only two options which is either try to remove malware and restore data or format system and reinstall it.
- e. Restore or Start from Scratch: There are some software packages that claim to be able to remove ransomware from computer and No More Ransom! Project is one of them. It is very difficult to get rid of the newer ransomware because there will be less time for developers to develop decryptions. If you have a backup of storage, the best way is to wipe the system and install from scratch.

E. Protecting against Ransomware Attacks

There are steps to be taken to protect your organization from ransomware attacks. Basic cyber security practices reduce the risk of becoming a ransomware victim. Here are some security practices must be followed in any organization:

- a. Frequent backups: Backup is very important for a ransomware recovery strategy. Make sure the backups are isolated from live data sources because ransomware infects local drives and network shares. Backup files must be checked to ensure the data consistency (Groot, 2019).
- b. Consistently update operating system and anti-virus software: Patch the vulnerabilities in operating system by updating it consistently. The software used by organizations are usually updated by developer of that software. These updates include patches which makes software more secure against attacks (Groot, 2019).
- c. Educate employees on security best practices: Make your employees aware of the best security practices like do not click on attachments from unfamiliar email addresses, do not download softwares from torrents, do not disable anti-virus or anti-malware software, do not click on phishing links.
- d. Proper credential tracking: Any employee who is given access to systems create a potential vulnerability point for ransomware. Change the passwords frequently.
- e. Settings and access control: Always disable apps running from AppData/LocalAppData folders like %TEMP%, %APPDATA%. Limit end user access to mapped drives and disable RDP.

III. Conclusion

Ransomware authors are developing malwares more sophisticatedly day by day. In most of the cases it is via human attack vectors like phishing mails. So, it is advised not to click on phishing mails and download software's from unknown resources and this can reduce the chance of getting infected by the ransomware. The only best way is to keep the offsite backup of data because even if you are infected with ransomware you can wipe off the data and reinstall the software and you still have backup data. It is impossible to stop the ransomware attacks however, following preventive strategies can help to mitigate the risk of ransomware. No organization is immune to ransomware attacks, but you can defend it by following best security practices. Never pay ransom, advice endorsed by FBI. Following the guidelines helps in not undergoing the attack and preventive measures are quite helpful. The future work of this paper might include the new strategies to overcome from this attack without undergoing huge losses and also we try to explore different ways in which the attackers try to breach the security.

References

- [1] Bauer, R. (2018, April 18). Complete Guide to Ransomware: How to Recover and Prevent an Attack. <https://www.backblaze.com/blog/complete-guide-ransomware/>
- [2] Brunau, C. (2019, August 22). Common Types of Ransomware. <https://www.datto.com/blog/common-types-of-ransomware>
- [3] Davis, J. (2020, February 12). FBI: \$3.5B Lost to Cybercrime in 2019, Led by Business Email Compromise. HealthITSecurity. <https://healthitsecurity.com/news/fbi-3.5b-lost-to-cybercrime-in-2019-led-by-business-email-compromise>
- [4] Eric, C. (2019, December 23). Ransomware Facts, Trends and Statistics for 2020. SafetyDetectives. <https://www.safetydetectives.com/blog/ransomware-statistics/>
- [5] Fruhlinger, J. (2018, December 19). Ransomware explained: How it works and how to remove it | CSO Online. <https://www.csionline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html>
- [6] Gallagher, S. (2015, June 25). FBI says crypto ransomware has raked in >\$18 million for cybercriminals | Ars Technica. <https://arstechnica.com/information-technology/2015/06/fbi-says-crypto-ransomware-has-raked-in-18-million-for-cybercriminals/>
- [7] Groot, J. (2018, November 19). A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time [Text]. Digital Guardian. <https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time>
- [8] Johansen, A. (n.d.). What is ransomware and how to help prevent ransomware attacks. Retrieved April 4, 2020, from <https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html>
- [9] Ng, A. (n.d.). The real victim of ransomware: Your local corner store. CNET. Retrieved April 4, 2020, from <https://www.cnet.com/news/wannacry-ransomware-real-victim-small-business-local-corner-store/>
- [10] Ransomware—What Is It & How To Remove It. (n.d.). Malwarebytes. Retrieved April 4, 2020, from <https://www.malwarebytes.com/ransomware/>
- [11] Rubens, P. (2017, March 2). Types of Ransomware. <https://www.esecurityplanet.com/malware/types-of-ransomware.html>
- [12] Sjouwerman, S. (n.d.). Ransomware on the rise: The evolution of a cyberattack. TechBeacon. Retrieved April 8, 2020, from <https://techbeacon.com/security/ransomware-rise-evolution-cyberattack>
- [13] Smith, M. (2013, November 4). CryptoLocker crooks charge 10 Bitcoins for second-chance decryption service. CSO Online. <https://www.csionline.com/article/2225714/cryptolocker-crooks-charge-10-bitcoins-for-second-chance-decryption-service.html>
- [14] Sterling, B. (2017, May 13). Ransomware: The basics | WIRED. <https://www.wired.com/beyond-the-beyond/2017/05/ransomware-the-basics/>
- [15] Ward, M. (2014, August 6). Ransomware victims given free fix. BBC News. <https://www.bbc.com/news/technology-28661463>
- [16] Zetter, K. (2019, May 14). What Is Ransomware? A Guide to the Latest Global Cyberattack | WIRED. <https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/>

Towards Privacy-Preserving of Time Series IoT Data Publishing

J.Aruna Santhi,

Assistant Professor

Department of Information Technology

Mahatma Gandhi Institute of technology,, Hyderabad-500075, India.

jarunashanthi_it@mgit.ac.in

Abstract: The wealth and accessibility of individual data on-line and from encompassing sensors has lead to an expanding rate in events of protection penetrates and potential security damages to people. However, admittance to these data is critical for the accomplishment of numerous valuable applications, for example, populace wellbeing considers or metropolitan arranging. During this re-search paper we plan a coordinated detecting structure to more readily deal with the approaching nonstop information stream (time-arrangement) from sensors implanted in various sort of information sources. We give a confided in zone to overseeing access to individual time-arrangement information to give utilities and gains while securing the people's protection.

I. Introduction

Keen gadgets around us are turning out to be an ever increasing number of between associated and a great many estimations caught by sensors consistently, bringing about a wide assortment of recently generated information. From savvy meters in homes to keen shirts for competitors, to keen beds for elder lies, pretty much every gadget in our regular daily existence can create information. Among every one of the sorts of information, information from sensors is the most boundless and is alluded to as time-arrangement information. Numerous elements need to get to this purported Internet of Things information after some time for leading information mining, and clients additionally advantage from offering their information to them.

A portion of these applications center around information gathered for individual reason (e.g., wellbeing observing), and others are produced for the assortment of detecting information at a local area wide level to add to populace studies(e.g. metropolitan arranging). This indistinct information assortment can likewise prompt significant individual protection concerns. Since itemized individual explicit information in its unique structure regularly contains sensitive data about people, namelessly distributing such information with no disclosure of delicate data to outsiders is a difficult errand. Besides, security concerns and issues emerge while re-appropriating this information to the cloud, since information subject misfortunes the power over information.

There have been various efforts to address this need, yet these are by and large loaded with the inadequacies of centralization as well as certainly overexpose individual information to outsiders. As of late, Data box [1] has expected to settle this test by upholding responsibility and control by plan at the clients' end. The Databox fills in as a stage whereupon the handling of individual information should be possible locally, with regards to containerized. Databox applications, and just emanate the important outcomes to an outsider. In this examination paper, we depict a system (as a piece of Databox) for distributing IoT time-arrangement information in a forceful climate, so the distributed information remains for all intents and purposes valuable while singular protection is saved.

II. Challenges and Research Questions

Soon, IoT takes into consideration inescapable information get-together and client following, however when these worthwhile highlights planned inappropriately, can prompt security breaks that are restricted the achievement of IoT vision [3]. The wide assortment of associated gadgets that structure the IoT, various sorts of information recorded by their sensors, and variety of correspondence conventions, prompting inborn information security and protection chances[5]. The principle questions is the manner by which wanted insights of individual time-arrangement information can be delivered to an un trusted outsider without trading off the person's security. All the more absolutely, how to change time-arrangement so that subsequent to delivering, person's delicate data can't be surmised from changed time-arrangement.

Examination of time-arrangement represents the way that information focuses assumed control over the long haul may have an inner design (like autocorrelation, pattern, occasional variety, repeating or Irregular part). Earlier ways to deal with security were formulated for the static cases, and when they are stretched out to the dynamic and intelligent instances of time-arrangement information, versatility challenges emerge. Then again, time-arrangement are profoundly wealthy in data about clients' conduct, especially when constantly gathered. This test makes it hard to secure the protection of one delicate conduct in separation of the others and it restricts the components that can be utilized. At last, a chief errand in security saving information distributing is

the meaning of legitimate measures that can genuinely survey the protection utility compromise. A large portion of proposed measures center around ensuring the character of a member without considering the data substance of the comparing information. An adequate answer for time-arrangement distributing requirements to precisely gauge the measure of unique data that is contained in the changed information.

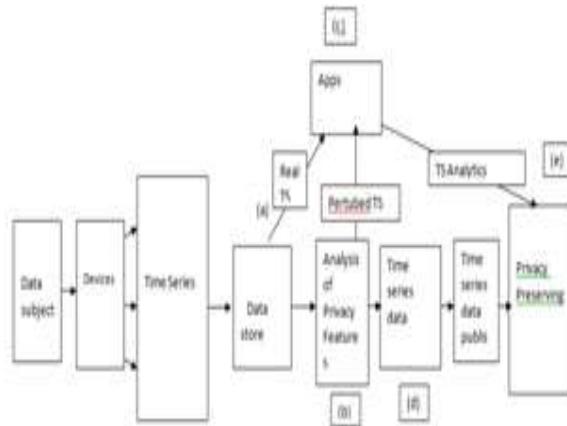


Fig 1: Design Approach for privacy-preserving time-series data

III. Sensing Framework

The inescapability of cell phones just as the assortment of their locally available sensors have empowered the robotized procurement of huge scope information. Working frameworks, for example, Android and iOS give application programming interfaces (APIs) to get to these sensors. SensingKit1 is another portable detecting system, viable with iOS and Android de-indecencies, which empowers catching movement, area, and vicinity information and sending them to a worker. Sensors can be progressively arranged and information can be extricated in both CSV and JSON design [2].

We will exploit SensingKit design for making some application for shrewd gadgets and arrange them such that every one reports its detecting information in a constant way and appropriate organization to the Data box. At that point, we will engage it with a vigorous part that incorporates and stores these time-arrangement information in a containerized confided coming up for future handling (Figure 1 (a)). Put away time-arrangement will be overseen by a Time-Series Data Base (TSDB) in a brought together capacity lives in Data box.

IV. Initial Approach and Future Work

Right now, there are two significant ways to deal with time-arrangement information distributing for breaking down reason. One arrangement is imparting the information to believed outsiders with

no change dependent on non-revelation arrangements. Another is change (for example adding clamor) of information prior to distributing them to the untrusted outsiders. Notwithstanding, there are downsides to the two of them: troubles in confiding in others and the compromise between data misfortune and client protection[4]. Furthermore, since in the both methodology information regularly dwells in a common climate, for example, cloud workers, clients will know neither the specific area of their information nor different wellsprings of the information by and large put away with theirs.

Thinking about these issues, we propose a protection by plan answer for security saving IoT information distributing through the Databox [1]. Attention to dangers on gathered time-arrangement that can risk client security, will assist clients with picking whether to give applications their crude information or applying some change prior to giving admittance to them (Figure 1 (b)). A Databox app (Figure 1 (c)) is an app specially designed to run on a Databox. Data subject can download a Databox.1 <http://sensingkit.org/>

Application proposed by an outsider and run it on their own gadget. Outsiders' applications introduced on Databox can demand for a few information from various sources and perform wanted examination on the enormous amount of information. For instance, report the connection between home temperature and client pulse (for example one information is gathered from a temperature sensor and another from a wearable watch). Note that, such investigation are just accessible through a unified TSDB per every client. Aftereffects of these investigation are summed up and simply answered to the client of Databox and never leave it in their unique structures.

To profit by information mining strategies, Databox apply a change which diminishes the danger of security infringement of the fundamental information (Figure 1 (d)). Clients have distinctive inclination in different situations: they are moderate in certain circumstances, and less worry in different cases. For this reason, we will fabricate a dashboard for clients to control their security and convey it on Databox. There are a few inspirations for distributing individual information assembled by IoT gadgets (for example how much client's TV watching hours is unique in relation to the normal populace). At the point when the preparing of clients' information is finished, clients can permit their applications to send the outcomes back to their suppliers through a security protecting information distributing technique (Figure 1 (e)). The primary objective of this strategy is to forestall the remaking of unique time-arrangement from changed ones, yet permit to

precisely appraise a few insights regardless of the irritation.

V. Conclusion

The amount of individual information individuals produce is being in-wrinkled consistently. Breaking down such information with no disclosure of delicate data to an unapproved party is the fundamental worry of the up and coming age of IoT organizations. In this paper we portrayed a security by plan answer for protection saving IoT information distributing through the Databox. Approved outsiders keen on the individual data are allowed admittance by this imagined part. Our proposed structure permits client to profit by information examination apparatuses while as yet being protected from intrusion of security.

References

- [1] Hamed Haddadi, Heidi Howard, Amir Chaudhry, Jon Crowcroft, Anil Madhavapeddy, Derek McAuley, and Richard Mortier. Personal data: thinking inside the box. In Proceedings of The Fifth Decennial Aarhus Conference on Critical Alternatives, pages 29–32. Aarhus University Press, 2015.
- [2] Kleomenis Katevas, Hamed Haddadi, and Laurissa Tokarchuk. Sensingkit: Evaluating the sensor power consumption in ios devices. In 12th International Conference on Intelligent Environments (IE'16), 2016.
- [3] Jan Henrik Ziegeldorf, Oscar Garc'ia Morchon, and Klaus Wehrle. Privacy in the internet of things: threats and challenges. Security and Communication Networks, 7(12):2728– 2742, 2014.
- [4] Chang, C.-C.; Nagel, D.; Mufic, S. Assessment of Energy Consumption in Wireless Sensor Networks: A Case Study for Security Algorithms. In Proceedings of IEEE International Conference on Mobile Ad hoc and Sensor Systems.
- [5] Evans D. The Internet of Things - How the Next Evolution of the Internet Is Changing Everything. CISCO white paper 2011.
- [6] Presser M, Krco Sa. IOT-I: Internet of Things Initiative: Public Deliverables – D2.1: Initial report on IoT applications of strategic interest 2010.

Intelligent System to Manage and Monitor Machine Health

J. Hima Bindu

Dept of IT

Mahatma Gandhi Institute of Technology,
Hyderabad-500075, India.
jhimabindu_it@mgit.ac.in

V.AmruthaValli

Dept of IT, M.Tech in CNIS

Mahatma Gandhi Institute of Technology,
Hyderabad-500075, India.
amrutha007valli@gmail.com

Abstract: The concept of intelligent systems was introduced to increase the safety of industry, manage work traffic efficiently and protect the light environment. Today, IMS applications are becoming more focused and their data is written using parallel distributed systems such as clouds, clusters, and grids to store big data. The Industrial Internet of Things (IIoT) connects IMS devices to cloud computing centers where data processing is performed. IIoT applications can perform multiple operations at once, such as receiving, cleaning, adjusting, transforming, and shaping data. This process begins with a continuous stream of data from multiple sources. Data cleansing focuses on noise removal, outlier detection, and missing value handling. Data preparation includes refinement, orchestration, virtualization, and mixing operations. When you're ready, run the data analytics process on your IIoT to enhance your application's intelligence. This process is iterative and consists of four steps. During the model building phase, the training model is trained for hidden data. These models are designed primarily for classification, regression, clustering, and frequent pattern analysis purposes. Control and Automation Pipeline provides secure access control for monitoring and manipulating sensor data. It also predicts data from offline industrial sensors, such as sensors used to monitor temperature and humidity levels. Managing and automating Pipeline have administration with security access for monitoring and handling sensor data. And also forecast the industrial standalone sensor data, for example those used for temperature and humidity level monitoring. This document suggests managers for each archiving department, including meaningful data transfer, edge analysis, real-time streaming data and a combination of security and privacy. This automatically shows the status of the machine so you can take care of it without doing anything. Production interruption. In the industry.

Keywords: IIoT, SVM, QOS, DCC, IMS

I. Introduction

The current pattern of the last item, quality expanding is influenced by time examination of the whole assembling process. The essential necessity of assembling is to deliver however many items when

could be expected under the circumstances, at the most reduced conceivable expense, obviously with the highest caliber. Insightful assembling framework itself ought to be a framework that can deftly react to utilize the information being created by the Industrial Internet of Things to achieve the most extreme creation proficiency and benefits by performing appropriate investigation. Perhaps the best advantage of shrewd assembling framework must be found in the decrease of human blunders and physical work, the expansion in by and large proficiency and the decrease of costs, both regarding time and cash. We additionally can't overlook the conceivable underpinnings of IIoT in quality control and support. The insightful assembling framework is a piece of the Industrial Internet of Things.

Traditionally, Big data analytics alludes to the procedure of information assortment, move in concentrated cloud server farms, preprocessing, investigation, and perception [4]. Implementing BDA in the cloud is a daunting task given the multifaceted nature and heterogeneity of information flow and sources [5]. Being able to identify assets that are close to the source reduces the diversity and heterogeneity of huge information structures [6]. Previously, cloud-driven information handling frameworks have enabled the IIoT for versatile constant information preparing. Be that as it may, new geographies for information handling are rising because of scaling down of figuring innovations and accessibility of decentralized cloud administrations at one bounce remote good ways from detecting hubs in IIoT.

II. Existing System

The new Concentric Enrollment Model (CCM) needs to monitor, measure, and learn a wealth of information across multiple IIoT levels. In addition, companies need purely financially savvy solutions to limit operating costs and the costs of generating and maximizing profits. In order to get a wealth of information on the IIoT, you need to focus on your business activities rather than overseeing filing and communications funding.

A. Drawbacks

1. There is no module for Transmission of only Meaningful Data so, its causes to extra storage and processing costs.

2. There is no Edge Analytics for respected application.
3. No concept to monitor machine health

III. Proposed System

In spite of the fact that IIoT has made an extreme move in cutting edge energy creation and conveyance advances, incorporation of the information gathered through sensors and other keen advances has gotten exceptionally testing because of absence of bound together information design arrangements. The sensors conveyed in enterprises communicate a tremendous measure of crude information. Nonetheless, all the sent information isn't advantageous. Consequently, arrangements should be planned that empower IIoT gadgets to only communicate significant information, which can prompt performing clean investigation by disposing of garbage information. While the IIoT has revolutionized advanced power generation and distribution technologies, integrating data collected by sensors and other smart technologies can be a daunting task due to the lack of a unified data format solution. It has become. Sensors deployed in the industry send large amounts of raw data. However, all the data sent is meaningless. Therefore, we need to develop a solution that allows IIoT devices to send only meaningful data. This allows you to remove unwanted data and perform pure analysis. Edge analytics can empower enterprises by bringing storage and detailed analytics capabilities closer to the user's network, but it also poses new infrastructure challenges (such as legal compliance). In this way, we will inform you of the condition of the machine according to the situation of the industry.

A. Advantages

1. Helps the industry make better decisions and increase productivity.
2. Need to develop a reliable and cost-effective data integration method. And this leads to additional storage and processing cost savings.
3. Designing and implement ways to maintain and repair the machine .

IV. Literature Survey

8Habib ur Rehman, Ejaz Ahmed, Ibrar Yakub, Ibrahim Abaker Targio Hashem, Muhammad Imran, Shafiq Ahmad "Analysis of Internet of Things Big Data Using Concentric Computing Models" IEEE Communications Magazine • February 2018
The IIoT consolidates AI and hugely equal dispersed frameworks, for example, mists, bunches, and lattices for huge information stockpiling, handling, and examination. In IIoT, end gadgets consistently create and send information streams, bringing about expanded organization traffic between gadget cloud

interchanges. Additionally, it increments in-network information transmissions.

They give a few future examination headings (e.g., continuous information investigation, information reconciliation, transmission of significant information, edge examination, ongoing combination of streaming information, and security and protection).

Industrial analysis and internet of things for industrial use, the author P.Lade , R.Ghosh , S.Srinivasan in the year 2017 previous approaches to production analysis were limited to a short time frame of data. Recent advances in big data analytic have allowed researchers to dig deeper into their data over the years. This is useful ,For example ,to find the root cause of internal defects. This article provides practical examples and details the challenges and approaches of data extraction, modelling and visualization.

V. Module Details

A. Sensor data

The insightful ones are considered the structural squares of the IMS. The special type of article in which the sensor is presented contains a large amount of data and is provided. This is a consistent streaming of the data collected by the sensor. This data is used for persistent, powerful and informative data. A usage class that generates data that takes into account whether the plan is logical. This general raw data required a signature to prepare a score that would link the AI or data to all sorts of good things.

B. Prepossessing

The sensor board needs more handling power, memory to manage information locally. In this way, for additional handling, it sends the information to data prepossessing. Preparing information at the edge and decrease the measure of information that need to trade in the cloud. Sending information back to the cloud or distant server farm is slower than preparing at the edge. It additionally lessens the information preparing and the board cost.

C. Intelligent system

The intelligent system concept was introduced to increase Industrial safety, manage work traffic efficiently, and preserve our easy environment. These days, applications are turning out to be more information serious and their information are depicted utilizing equal circulated frameworks, for example, mists, bunches, and networks for large information stockpiling. Modern Internet of Things

(IIoT) interfaces the IMS gadgets to distributed computing habitats, where information preparing is performed.

D. Cloud computing Center

In the current time frame, appropriated processing is getting stacks of eagerness for a couple of spaces by planning huge data. When data is collected from multiple sources, such as sensor associations, random associations, and vehicles. There are still add-ons to address security issues with the data collected from the above sources at Cloud Worker Ranch. A common device is needed to help collect information from the sensor to the cloud. A system show is the backbone of a communication structure that matches a particular quality of service (QoS) for each communication application.

E. Data Collection Controller

Here oversees is only the information assortment regulator (DCC) deals with the information assortment activity. The setup is finished by the information assortment regulator, which includes: The actuation and deactivation time observing of the framework. The determination of the security system for gathered information insurance. The determination of the correspondence interfaces that will be suitable for achieving and maintain the health of the machinery

VI. Algorithms Used

A. Support Vector Machine (SVM):

Support Vector Machine (SVM) is a tuned artificial intelligence algorithm that can be used for both queries and rollback tasks. However, it is usually used together for all questions. In this aggregation, each data is plotted as points in n-dimensional space (n is the number of features), and the score for each component is as follows:

Evaluation of a specific grade. By then, we've found and collected hyperplanes that generally make a good distinction between the two classes (see preview below).

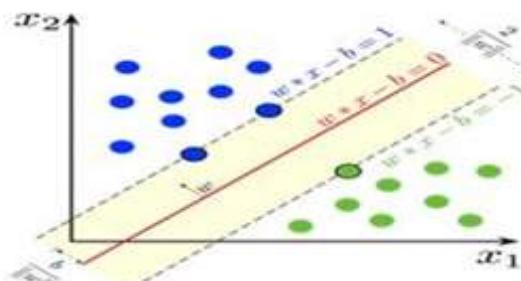


Fig 1: SVM Hyperplane Graphs

Figure above shows the Maximum-edge hyperplane and edges for a SVM prepared with tests from two classes. Tests on the edge are known as the help vectors.

A. Advanced Encryption Standard

It is s based on the "substitution-permutation". It consists of a series of related operations, some of which involve swapping (swapping) inputs to specific outputs, and others involving shuffling (swapping) bits. Each of these rounds uses a different 128-bit round key, calculated based on the original AES key.

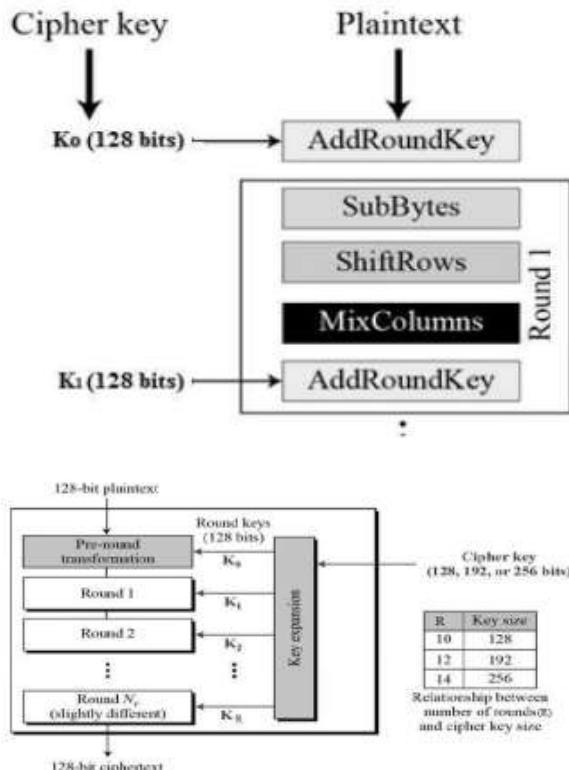


Fig 2: AES Encryption standards

VII. Results

A. Sensor Data

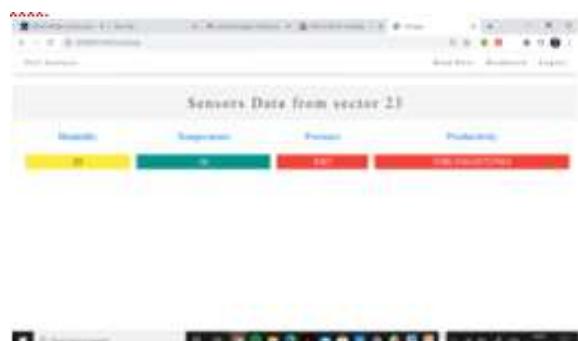


Fig 3: Simulation Sensor data

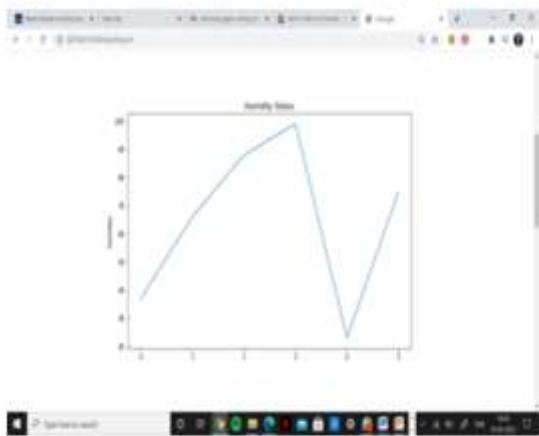
B. Humidity Graph

Fig 4: Simulation of Humidity Parameter

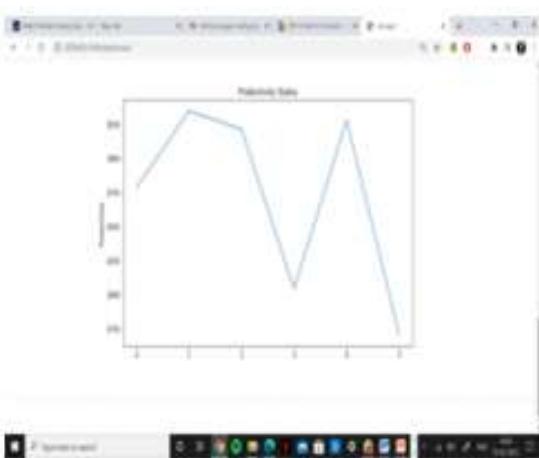
C. Productivity Graph

Fig 5: Simulation of Productivity Parameter

D. Pressure Graph

Fig 6: Simulation of Pressure Parameter

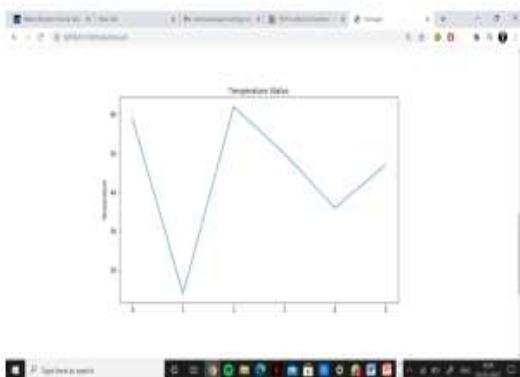
E. Temperature Graph

Fig 7: Simulation of Temperature Parameter

VIII. Conclusion & Future Enhancement

To address IIoT data availability issues, manufacturing plants make extensive use of IMS and smart sensor technologies to monitor and track products in real time. This approach of automatically generating and collecting data includes ways to predict the performance of big data as it recognizes and reads data, and how to detect and share big data from multiple life cycle sources in real time. , Brings new challenges. Hidden knowledge to improve productivity at all stages. To address these issues, this study uses a machine learning technology called (support vector machine) SVM. This technology allows you to use this application to measure performance based on real-time sensor data.

Stem not only predict the productivity based on the data but also to check and have a record of the machine health. The environmental factors of the industry would have an impact on the machinery. Therefore, machine health prediction, maintenance, scheduling timely servicing and knowing the problem in the machine will not hinder the production thereby saving time and increasing productivity, in turn increasing the profit margin for the industry.

References

- [1] J. Hima Bindu, V. Amrutha Valli Intelligent Manufacturing System To Manage Industrial Internet Of Things (IIOT) Science , Technology and Development Multidisciplinary Journal vol IX , issue XI , November 2020.
- [2] P. Lade, R. Ghosh, nd S. Srinivasan, "Manufacturing Analytics and Industrial Internet of Things," IEEE Intelligent Systems, vol. 32, no. 3, 2017, pp.74–79.
- [3] J. Wan et al., "Software-Defined Industrial Internet of Things in the Context of Industry 4.0," IEEE Sensors J., vol. 16, no. 20, 2016, pp.7373–80.
- [4] E. Ahmed et al., "The Role of Big Data Analytics in Internet of Things," Computer Networks, 2017;

- http://www.sciencedirect.com/science/article/pii/S1389128617302591, accessed 8 Oct.2017.
- [5] M. S. Hossain and G. Muhammad, "Cloud-Assisted Industrial Internet of Things (IIoT)- Enabled Framework for Health Monitoring," Computer Networks, vol. 101, 2016, pp. 192– 202.
 - [6] Q. Zhang et al., "An Incremental CFS Algorithm for Clustering Large Data in Industrial Internet of Things," IEEE Trans. Industrial Informatics, vol. 13, no. 3, 2017,pp.1193–201.
 - [7] L. Da Xu, W. He, and S. Li, "Internet of Things in Industries: A Survey," IEEE Trans. industrial informatics, vol. 10, no. 4, 2014, pp.2233–43.
 - [8] X. Li et al., "A Review of Industrial Wireless Networks in the Context of Industry 4.0," Wireless Networks, vol. 23, no. 1, 2017, pp.23–41.
 - [9] E. Ahmed et al., "Green Industrial Networking: Recent Advances, Taxonomy, and Open Research Challenges," IEEE Commun. Mag., vol. 54, no. 10, 2016, pp.38–45.
 - [10] M. Chen et al., "EMC: Emotion-Aware Mobile Cloud Computing in 5G," IEEE Network, vol. 29, no. 2, Mar./Apr. 2015, pp.32–38.
 - [11] P. O'Donovan et al., "An Industrial Big Data Pipelinefor Data-Driven Analytics Maintenance Applications in Large- Scale Smart Manufacturing Facilities," J. Big Data, vol. 2, no. 1, 2015, p.25.
 - [12] Y.-C. Lin et al., "Development of Advanced Manufacturing Cloud of Things (AMCOT) - A Smart Manufacturing Platform," IEEE Robotics and Automation Letters, 2017.
 - [13] J.Wan et al., "A Manufacturing Big Data Solution for Active Preventive Maintenance," IEEE Trans. Industrial Informatics,2017.
 - [14] K. Wang et al., "Wireless Big Data Computing in Smart Grid," IEEE Wireless Commun., vol. 24, no. 2, Apr. 2017, pp.58–64.
 - [15] Y. Zhang et al., "A Big Data Analytics Architecture for Cleaner Manufacturing and Maintenance Processes of Complex Products," J. Cleaner Production, vol. 142, 2017, pp. 626–41
 - [16] <https://www.analyticsvidhya.com/blog/2017/09/understanding-support-vector-machine-example-code/>

The Verge of Extinction

K. Suganya

Department of IT,

Chaitanya Bharathi Institute of Technology,
Hyderabad-500075, India.

B.Surya Samantha

Department of IT,

Chaitanya Bharathi Institute of Technology,
Hyderabad-500075, India

S. Vamsi Krishna

Department of IT,

Chaitanya Bharathi Institute of Technology,
Hyderabad-500075, India

Abstract: India diversity, cultural beauty and reverent tradition makes India very unique from all other countries. The way India is, with all different ideas, concepts, beliefs holding on to the same ground as an amalgam makes India more beautiful. The profound beauty of India lies in the traditional and cultural works of India, the songs, the dance, the arts and crafts and the spiritual way of dealing with arts shows the world that India is a paradise of everything mixed together. But sadly due to change in the way of life and lack of support, the number of professionals, consummates of the Art works is decreasing over time. It is because of these professionals that our country is hailed high and venerated heartfully. So its our responsibility to know the Art works, to preserve them and to spread it across the globe and give the coming generations as it was given to us.

I. Introduction

The different traditional and cultural Art forms make India a special country form the rest of the world. All the professional who are adroit in these art forms, hold the prestige, honour and extols of India, they keep India in such a beautiful form that no one can withstand the temptation to laud Indian beauty. But their essence is decreasing day by day, India is more moving towards heated political economy but not checking whether the cultural industries are working and are stable economically or not. All around the globe, our tradition and culture reverberates but we are not giving enough support to it. We have limited, dearth of the upholders of the traditional and cultural professionals. We can't let the profession dry up. The traditional and cultural professionals are losing their patriotism and the support from the public. As a result of losing their patriotism they are quitting their self-learned, interested professions and changing their profession due to worst financial status. This results in two major losses first, the person is losing his means of living, the thing what he is interested to do and second, it's the end of tradition and process of work, the persons unique talent is being ended. This is the real extinction that should be stopped. So, my application can provide a platform for these

professionals and our traditional arts sector to spread, evolve and infuse the value, importance of these traditions. All the artisans can showcase their works, conduct their own courses and can have trading feature also though my application. This allows the artisans all the flexibility needed. By this application all artisans can continue their work without hesitation about their future and the feeling that their kind of traditional work is in the verge of extinction.

II. Existing System



Fig 1: Dharavi website

This is a website created for craftsman in Dharavi for developing people and their families, by providing a feature for buying the crafts made by the people in bulk.



Fig 2: Other website

This is another website, where the history and biography of the cultural and traditional protectors. It stores the information about the

traditional expert, his skill, his history with the tradition.

III. Proposed System

The project aims to provide a stratagem to outwit the extinction of Indian Tradition and incites to spread the tradition pervade the country. The motivational factors and key points of the application are:

1. To provide a platform for the craftsmen to showcase their work.
2. To revive or at least archive the workmanship.
3. To provide a platform to report any identified local crafts work/art crafts which are on the verge of extinction.
4. To archive the stories, techniques, skills about these activities.
5. To save our traditional and cultural values from the verge of extinction and ultimately preserve the uniqueness of our country.
6. To make a platform for the public to request for any small trade, shows and events.

IV. System Design

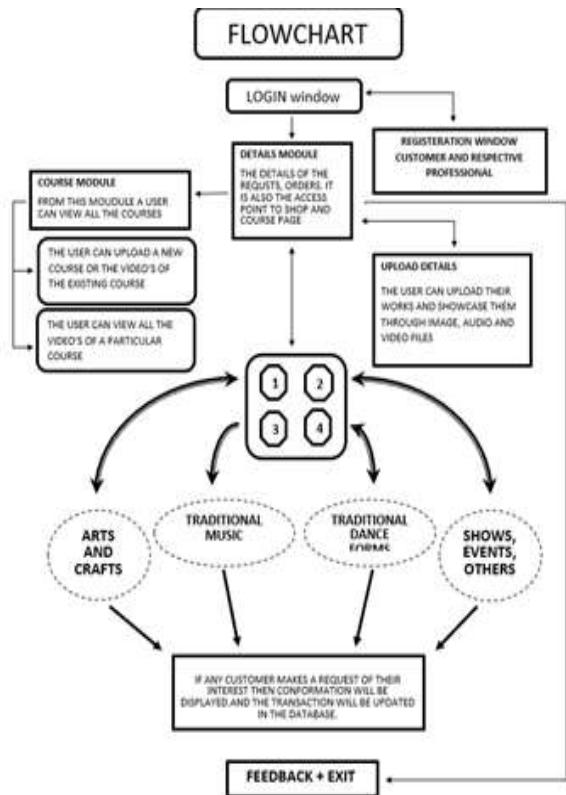


Fig 3: flowchart

V. Implementation of Project

The application can be used to upload the arts, crafts, musical and dance material by different

sellers through an image file with all the details of the material. The uploaded materials can be ordered by any customer. The traditional musical and dance experts can showcase their works musical, dance forms by uploading audio and video files with all the details. A music listener can listen the a audio file, a viewer can view the video file and the user can have their own choice based on the details of the music file and the video file. Through our application events such as puppet show, drama shows and so on, can be uploaded as a video file and these events can be booked by any customer(user) on their required date. A sms will be sent to the phone after registration, and after every image, audio and video file upload. A sms will be send to the buyer and the seller of a particular material that is ordered and if it is a event that is booked, then the event head(user) and the customer will receive the sms. Apart from all the above features any traditional expert can upload courses to extend their technique, works, skills so that, that traditional act can be continued without being tagged as an endangered tradition.

The Application will serve as the best platform to view all the arts of India. This application was built using Java Swings and Java FX as the front end and as the back end we used Mysql (Database Management System) to store all kinds of data(image, audio, video and transactions). Each profile that had registered will be stored in the database. A user can be a customer or seller or both. The profile of any user contains both request(order as customer) and orders(sell as seller) parts. The users can sell their items and buy other items. Lets talk as a customer and seller separately to understand how transactions work through our application. A customer can see all the works of arts and crafts or musical performance, dance performances and shows and get interested in anytime and place an order (in case of arts and crafts) or book a musical/dance/any other show as per their choice of date. Coming back to the sellers end, seller showcases all their hard work in these arts and once received the order or booking will act accordingly.

In our application, we have developed the upload page so that the artisans and traditional professionals can put their works as image, audio and video files. In the upload module, we have asked the professionals to upload their work, details of the work and in which art forms the work belongs to and cost of it(if required). If the professional has uploaded audio or video file, then the file will be played for 15sec so as to confirm that the file is correct file.

In our application, we have developed a VISION page which hold the key idea of the application. This page is the root page to direct the users to any other page. This page directs to arts and

crafts, music, dance and small shows pages. Now, coming to all these fine arts pages, they data in those pages justify their arts. Each page has its own content and all the details of the professional who did the work will be provided.

Apart from showcasing, selling and booking shows. This application provides users to learn these fine arts like music, dance, painting and all traditional works through free courses. We have provided a module where all the traditional workers can showcase how things are being done, how everything is happening in the background, what are the techniques, methods to do these fine arts. By keeping these things as course, we are letting the tradition which is esoteric pervade through many people and make them feel that these are special to them. This is a huge opportunity to spread the working of the arts. Even the users who learn can do it as a hobby, which make them feel good. By this, we can save any traditional work from extinction

VI. Results



Fig 4: The login page



Fig 5: The details module

This is the login page of our application. After the credentials are satisfied, it will be redirected to the details module which tell all the details of the particular user. The details module contains the links to VISION page, courses page, upload page of the application.



Fig 6: Vision Module

This is the VISION page which contains all the links to any art form. We consider this page to be central because it roots all the art forms pages



Fig 7: Uploading item through image



Fig 8: Uploading dance show through video

This is the uploading module where an arts and craft item on fig7 and a dance video is being playing in f8 will all the respective details of their work



Fig 9: Playing song



Fig 10: Placing the order

Here, fig9 we can see the music showcase page where music is being played and fig10 shows

the arts and crafts showcase page with a transaction going on



Fig 11: Playing dance video



Fig 12: Small Events Page



Fig 13: Playing event video

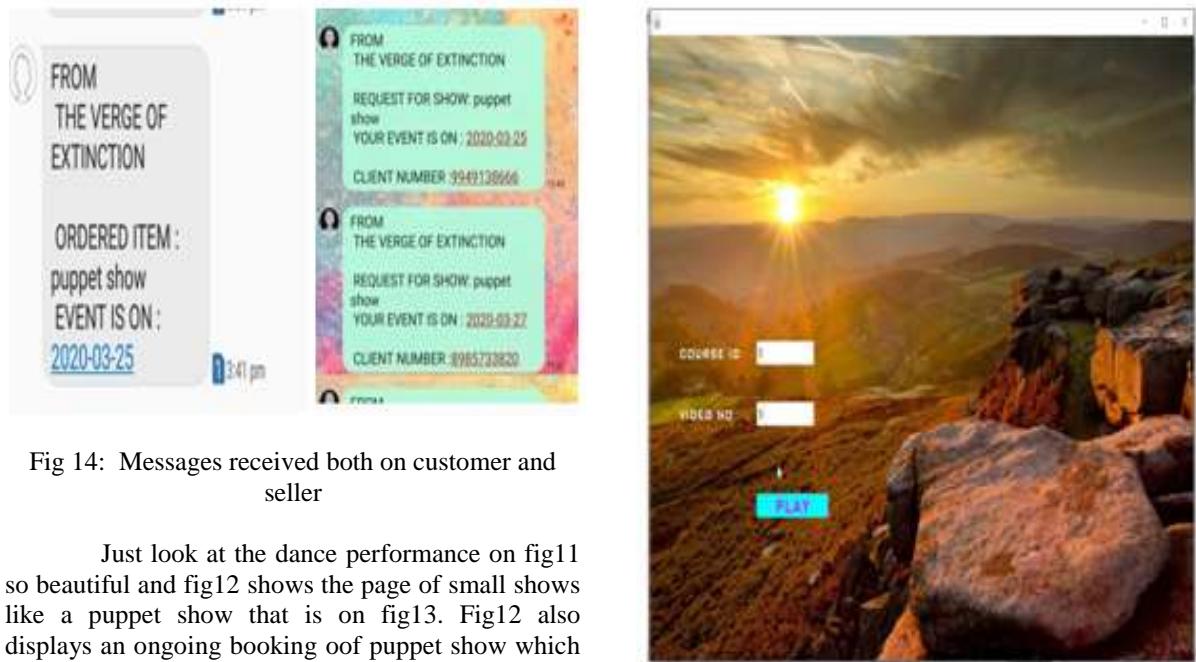


Fig 14: Messages received both on customer and seller

Just look at the dance performance on fig11 so beautiful and fig12 shows the page of small shows like a puppet show that is on fig13. Fig12 also displays an ongoing booking oof puppet show which u can see in the sms send to customer and the event seller phone numbers in fig14



Fig 15: Viewing the course details

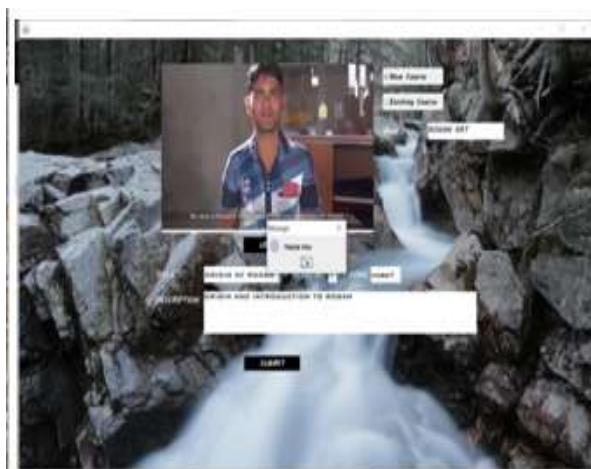


Fig 16: Uploading course video

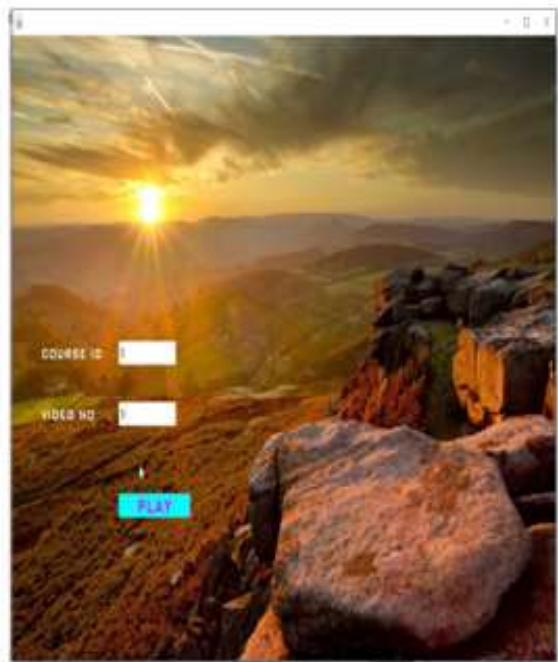


Fig 17: and Fig 18 Learn module with course id - 1 and video number - 1

Coming to the courses phases, this is learning phase of any user and in fig15 we can see the details of the courses available and in those available courses how many lectures and videos are currently available. In fig 16, we have the course uploading module in which all the details will be uploaded by the course instructor. While starting a new course, a unique code will be sent to the mentor and using this code only the mentor can upload and edit the course. In fig17 & 18, we can see that a user is trying to play course 1 and video 1 to learn Rogan painting manufacturing process.

VII. Conclusion

1. Finally, this application has thought so many things about our Indian tradition and culture that needs so much support for us.
2. Knowingly or unknowingly there are so many traditional arts, musical and dance forms that are passed to us by your ancestors so it is our responsibility to keep them alive.
3. This application can identify and extend the scope of that traditions that are in the verge of extinction
4. In this contemporary world of change, the tradition has to may flow and evolve through us, through this application. We grow to help others.

Bibliography

- [1] G. Nageswara Rao “Core Java, An Integrated Approach” textbook
- [2] www.javatpoint.com
- [3] www.tutorialspoint.com

Stock Price Prediction on News Data and Market Data Using ML Techniques

Veena Madhuri. S

Information Technology

Chaitanya Bharathi Institute of Technology
Hyderabad-500075, India
vinasnazzy@gmail.com

Sirisha. A

Information Technology

Chaitanya Bharathi Institute of Technology
Hyderabad-500075, India
asirisha_it@cbit.ac.in

Abstract: Stock Price Prediction is a progressive research area, where the returns in stocks depend on the prediction. Stock prices vary based on the market sentiment [1]. The news also plays a major role in the prediction of stock prices. So, using news for prediction may have immense consequences on the financial world. The aim of this article is to develop a model which can anticipate the stock price movements using the market data and the sentiments of news data. The proposed framework is beneficial to investors and can be used by firms to preserve shares of their shareholders. The authors have preprocessed data, feature engineered and trained data on various classification models, the model showing the highest accuracy is chosen for predicting stock prices. The authors have observed the accuracy of around 77% for the next day prediction. The accuracies decreased gradually, when the stock price movements are calculated 10 days in advance.

Keywords: Stock Price; Market Data; News Data; Classification Models; Data Preprocessing; Feature Engineering

I. Introduction

Stock price prediction is the act of predicting the subsequent value of a particular company's stock, share or any other financial share traded on an exchange. Investors would gain more profits if the prediction produces a better result. So, the stock price prediction is the active research area in this era. Market data has the information of open and close prices, volume and returns of the stock market. News data includes many features, such as word count, sentence count, relevance and sentiment score. The daily news about the companies effects the stock prices in many ways, such as the stock price may increase or decrease. Since, the news has a lot of information about the company's happenings.

Investors, before investing in any company would first do research on that company by knowing the shares of previous years, share values and profits of the company. In this process, they even go through many news articles published regarding the company to know the latest happenings in the company which would help them decide whether to buy the share, sell or hold if they already own a share.

The time series is the series of data points listed in equally spaced points of time. Mostly a stock price relevant data such as market data or news data are time series because, they are collected on a daily basis. Time series analysis comprises of methods to analyse time series data which extracts the characteristics and the statistics of the data. Forecasting of time series is the process of using a model to anticipate the future values based on historical values.

Classification models can be used to anticipate the stock price movements when given new data as an input. There are many classification models among which authors have used 4 popular models for training and predicting the stock price. The authors have used the following models: Multi-layer Perceptron (MLP), Recurrent Neural Network (RNN), Light Gradient Boosting Machine (Light GBM or LGBM), Extreme Gradient Boosting Machine often called as XG-Boost. The RNN and MLP are from Neural Networks, Light GBM and XG-Boost are from gradient boosting machines. RNN and MLP use hidden layers and activation functions to train the model. Light GBM and XG-Boost uses the inbuilt parameters which are tuned and optimised for training the model.

The primary motivation of this article comes from the challenge hosted by the company Two – Sigma on Kaggle. The company hosted market data with the values of returns calculated and news data with the sentiment of the news articles already determined. The data provided by the company have a part of US listed companies. The included set of companies change every day based on the trading amount and information availability, which means that there may be few companies which enter or leave the data on a particular day. Both, the market data and news data are used for predicting the stock price movements. The methodology used for prediction is: data collection, data preprocessing, feature engineering, building classification models, model evaluation and results analysis.

II. Literature Survey

In recent years, remarkable efforts have been put into generating models to predict the market trend or the trend of a stock price in the future.

Research has shown that there is a powerful connection between a news article regarding a company and company's stock price movements.

Reference [14] introduced an automated text mining-based approach to combine news articles from different sources and created a News corpus. The news corpus is filtered for relevant sentences and analysed using NLP methods. Then, a sentiment score for positive and negative news is assigned as a measure of sentiment which is called as News Sentiment. Their work collected news, to develop the sentiment analysis engine which analyses news articles and predict stock prices for companies.

Reference [17] have studied the effect of level of relevance to financial forecasting. The information extracted from various categories of news articles are aggregated based on the sectors and industries using the multiple kernel learning method for predicting stock price movements. The news articles were divided into five types of relevance to a targeted stock while different kernel is employed to analyse each category. The results showed that dividing news into more categories improved the performance in comparison to methods based on a low number of news categories.

Earlier studies have proved that previous stock prices aren't better predictors for determining future stock prices, but it can be helpful in predicting the slope of short-term stock price movements. Reference [8] have shown that positive news articles increase the returns quickly whereas negative articles have delayed reaction. The majority of delayed responses to articles occurs around the successive earnings announcement. Reference [9] aggregated crowd sourced data obtained from Google news and Wikipedia with stock market data to forecast daily stock price movements and also predicted a daily minimum and maximum of stock prices by technical indicators. Their research has used news sentiment to develop an ANN model for the prediction of stock prices of Google Inc. and tested their model profitability with out-of-sample prediction. Other researches have suggested that rather building concept models, then checking for the correlation among sentiments and stock prices, good predictive models [16] can be built such as dual sentiment classifiers and predictors [5], Artificial Neural Network models and time series-based regression models. Reference [15] have introduced a new feature which simultaneously captures topics and their sentiments in the prediction model. The new topic model was developed named TSLDA to fulfil the above feature. They have used market data to obtain the prediction results and proved that including sentiment information from the social media helps the stock price prediction.

Reference [13] have found the correlation among market sentiment and public sentiment by using the twitter data and DJIA data. Twitter data is considered as public sentiment and DJIA data is considered as market sentiment. They have developed a cross validation method for market data and used a Self-Organizing Fuzzy Neural Networks (SOFNN) to predict the stocks.

Traditional algorithms such as Naïve Bayes (NB) [3], Logistic Regression (LR) has got 74.6% accuracy for classifying companies as "good" or "poor" [6], Decision Tree (DT) [4], Support Vector Machines (SVM) [4], has achieved 0.55 hit rate or the prediction accuracy[11], Artificial Neural Network (ANN) [12] have been proven to be effective for financial forecasting.

Reference [7] have proposed a feature selection method which is able to handle the class imbalance problem occurring from over the sampling of the minority classes. It considers the ensemble of selected features, which is called as Balanced Mutual Information (BMI). The authors have compared the results of this BMI with Mutual Information and Chi-square based feature selection methods which produced the better performance.

Reference [10] developed three models to predict the directional change in the Tehran Stock Exchange and compared their performance. The models used were Naïve Bayes, Decision tree and Random forest. Three macro-economic variables and ten micro-economic variables are used as inputs to these models. The accuracies for the models used were found to be 73.84% using NB, 78.8% using Random forest and 80.08% using DT.

The main aim of this work is to use some machine learning techniques to observe the effect of news sentiments along with market data on stock price movement.

III. Methodology

A. Tools used

The authors have used python for building classification models and java script, HTML, CSS and json for developing the user interface. The user interface was developed in flask which is used to build web applications in python. D3 (Data Driven Docs) is a JS library also used to develop the web application.

B. Data Collection

The data is collected from the challenge hosted on Kaggle by Two-Sigma, an investment management company (Two Sigma 2018). And the

data set has daily stock information of 3,510 stocks which is divided into news data contributed by Thomson Reuters and, market data contributed by Intrinio.

The market data initially comprised of 4,072,955 rows and 16 columns, including attributes such as closing and opening stock prices, stock volume and returns. The news data comprised of 9,328,749 rows and 35 columns. It contains the results of sentiment analysis done on features of news items such as word and sentence counts, as well as on news articles. The market dataset is comparatively smaller when compared to news dataset because there were multiple news articles per stock on any given day. The flowchart of the process is shown in the figure 1. The market data comprises the following features:

Table 1: Features of Market Data

Feature name	Description of feature
time	indicates the current time (in market data, all values are taken at 22:00 UTC)
assetCode	asset's unique id
assetName	name of the asset, which may be for a group of assetCodes
universe	boolean value denoting whether or not the asset on a day will be put in scoring
volume	trading volume in shares for a day
close	close price which is not adjusted for splits or dividends for the day
open	open price which is not adjusted for splits or dividends for the day
returnsClosePrevRaw1	description given below
returnsOpenPrevRaw1	description given below
returnsClosePrevMktres1	description given below
returnsOpenPrevMktres1	description given below
returnsClosePrevRaw10	description given below
returnsOpenPrevRaw10	description given below
returnsClosePrevMktres10	description given below
returnsOpenPrevMktres10	description given below
returnsOpenNextMktres10	description given below

The returns in the market data can be interpreted by the following properties:

1. Returns are always calculated either close-to-close or open-to-open, that is, from closing time of a trading day to open time on another day or from opening time of a trading day to open of another day.
2. Returns are either market-residualized (Mktres) meaning that the fluctuation of the market as a whole has been taken for, leaving the only fluctuations inherent of the asset or raw, meaning that the data is not adjusted against any benchmark.
3. Returns can be calculated over any random interval, but here 1 day and 10-day horizons are used.

Returns are tagged with 'Next' if they are forward looking, 'Prev' if they are backward looking.

The news data comprises the following features:

Table 2: Features of News Data

Feature name	Description of feature
time	UTC timestamp showing the availability of data on the feed
sourceTimestamp	UTC timestamp of creation of the news item
firstCreated	UTC timestamp of the item's first version
sourceId	each news item has a source id
headline	the news headline
urgency	comprehend types of stories as alerts (1), articles (3)
takeSequence	it is the sequence number of the news item when taken which starts at 1, for a story the articles and alerts has different sequences
provider	organisation which provided the news item
subjects	company identifiers and topic codes that relate to this news item
audiences	identifies which news item belong to the desktop news product
bodySize	size of the present version of the story body in characters
companyCount	this list has number of companies in the news item
headlineTag	headline tag of the news item given by Thomson Reuters
marketCommentary	general market conditions are indicated as a Boolean value

sentenceCount	number of sentences in the news item
wordcount	number of lexical tokens in the news item
assetCodes	code for the assets listed in the item
assetName	name of the asset
firstMentionSentence	score is assigned based on the news item placement, headline (1), the first sentence of story body (2), second sentence of the body (3) and so on. If the news item asset is not mentioned then 0 is assigned
relevance	relevance of the news article denoted by a decimal number
sentimentClass	sentiment score with respect to the asset
sentimentNegative	-1
senimentNeutral	0
sentimentPositive	1
sentimentWordCount	the sentiment of the word count relevant to the asset
noveltyCount	novelty of the content on a particular asset within a news item
volumeCounts	volume of news for each asset

The news data has additional features of noveltyCount and volumeCounts calculated per 12 hours, 1 day, 3 days, 5 days and 7 days respectively.

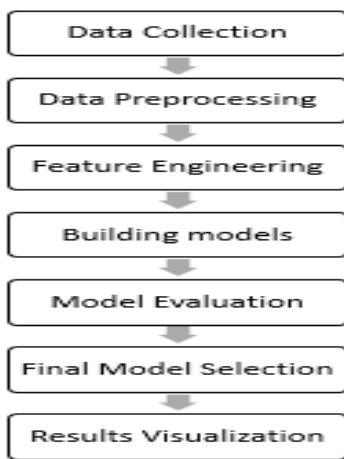


Fig 1: Flow chart of the process

C. Data Preprocessing

The authors have downloaded the dataset from Kaggle which primarily spanned from 2007-2016 and have limited it to 2010-2016, to avoid

impact from the financial crisis occurred in 2008. The authors have used the data from 2010-2015 for training and the data from 2016 for testing. The data cleaning and feature engineering was done on market data and news data but the majority of the processing was done on news data.

- Data Preprocessing on News Data: Delay is variable which is calculated between when a news item was created and when it became available. Firstly, the delay is determined and then rows of news data are removed where the delay is one day or more. Secondly, the authors have removed rows of blank headlines, since they have negligible impact on the prediction of stock price movements. Finally, the authors have removed rows with an urgency of 2, as these constituted less than 0.001% of the data and they are ignorable.
- Data Preprocessing on Market Data: Firstly, outliers with respect to open and close prices are removed, by clipping rows where difference between the close price of one day and the open price of the next day is more than 50%. Secondly, the imputation method is used on the market data by filling nulls in the market adjusted columns with the raw values in the same row. Finally, outliers based on the returns are also removed, that is, stocks with returns exceeding 50% or falling below 50% are removed.

D. Feature Engineering

The news data has an urgency feature, which indicates whether news items are articles (3) or alerts (1) based on urgency feature measured on a scale of 1 to 3 and a sentiment class feature which indicates overall sentiment toward a stock (1 for positive, -1 for negative, or 0 for neutral). To aggregate with stock price data the numerical and categorical attributes need to be merged. The authors have combined certain features of the news data on urgency and sentiment class, to create features which can be merged with the market data and hence can minimize the information loss. For example, wordcount_3_1 which indicates the word count of the news item and urgency of the news article being 3 and sentiment class being positive which is 1. The above transformation is performed on the original features and the derived feature set is as following:

- wordCount: the count of words in the news item
- sentenceCount: the number of sentences in the news item
- sentimentWordCount: the number of lexicons in a news item which are relevant to an asset.
- firstMentionSentence: the sentence where the asset is mentioned initially.

5. relevance: this value denotes the relevance of the news item to the asset between 0 and 1
6. rel_FirstMention: indicates where in a news item, the asset or stock was first found.
7. rel_SentCount: indicates the proportion of words in the news item which had sentiments affecting a stock.
8. To keep the effect of market data to minimal, only two features from market data are used to train the model:
9. returnsOpenPrevMktres1_dir: the directional change of the market adjusted stock price during the previous day.
10. returnsOpenPrevMktres10_dir: the directional change of the market adjusted stock price during previous 10th day.

Based on the asset code and date the news data is grouped to get the main features of all news items at the daily level. The authors have created a merged dataset by aggregating the transformed news data with the daily market data.

1. Feature Importance: Like random forests, Gradient Boosting Machines are relatively straightforward to retrieve feature importance scores for each feature after constructing the decision trees. Fig. 2 shows the importance of features produced by XG-Boost. The importance is a score which denotes how important or helpful the feature was in the construction of the boosted decision trees with in the model. The importance of an attribute or feature is higher if it is used to make important decisions with decision trees. The feature importance graph given by the XG-Boost is shown in figure This feature importance is calculated for each and every attribute used for prediction in the dataset, and ranks them in order. It is also useful for comparing the attributes. Feature importance is determined for a decision tree by considering the amount of each feature split point enhancing the performance measure, weighted by the number of observations the node is responsible for. The performance measure may be the purity such as Gini index is used to choose the split points or the other more definite error function such as Mean Absolute Error (MAE) or Mean Square Error (MSE). These values are calculated for all constructed boosted trees and then averaged across all within the model.

Authors have made few conclusions by seeing the plot above, they are:

1. People respond less to alerts and more to articles
2. Positive sentiment shows a powerful impact on the stock market than the negative sentiment

3. The news articles alone have an effect on stock price movement for few days, but the effect fades with time.
4. The fraction of sentences or words in a news article related to an asset has more importance than the actual sentence or word counts.

The relative position of where an asset first appears in a news article is more important than the actual sentence number of that first appearance.

E. Building Classification models

Initially, authors have used all the features from both market data and news data to build a model, but then it comes to notice that all the top features used to build the model are from market data. However, the purpose of this article is to anticipate the stock price movements using news sentiments. In order, to build the model the authors have removed market data's features and used the engineered two features for the prediction. Hence, two features of market data and all the features of news data are used to train the model. Neural networks and gradient boosting machines were found to be effective for predicting the stock price movement. Therefore, the main focus of this article was put on neural networks and gradient boosting machines to develop the model.

The authors chose to work with the multi-layer perceptron and recurrent neural network from neural networks. The earlier researches prove that MLPs are better to work with tabular data, time series prediction and classification. Since, the stock price data is a time series data, MLP is chosen as a primary neural network model for prediction in this article.

The authors chose to work with the two latest algorithms of this time they are LGBM and XG-Boost from gradient boosting machines. LGBM has a fast-training speed and is suitable for working with large datasets, when compared to XG-Boost. It uses leaf wise splitting, rather than level-wise splitting as the other GBMs, but there is a chance of overfitting with LGBM. Though XG-Boost was not as fast as LGBM, but it is still fast when compared to other GBMs.

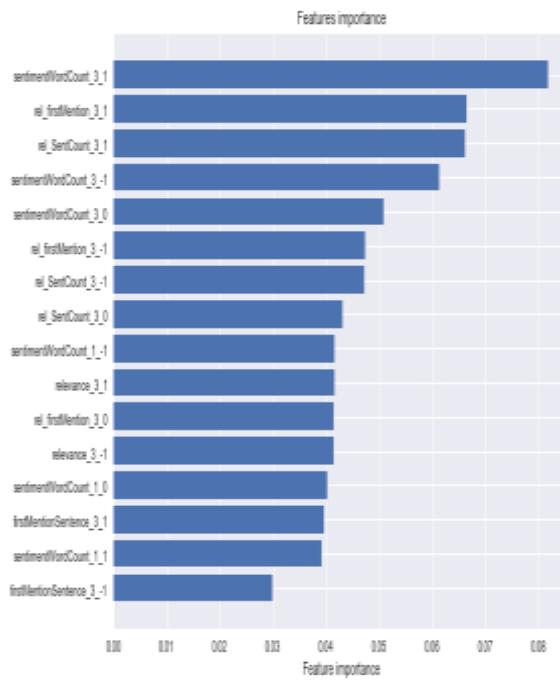


Fig 2: The feature importance graph given by XG-BOOST

Firstly, the authors have worked with LGBM and for the data used in this article, the model worked well for positive stock price movements and predicted up to 94% of stocks. However, the prediction of negative stock price movements was true only for 2% of the stocks. More particularly, it is useful for regularized and predictive classification. Secondly, the authors used XG-Boost for training the model and the predictions were stable on the data used in this article. Based on the results obtained the authors have observed good true positive and true negative rates in the prediction of stock prices. The authors have found that both positive and negative stock price movements had good prediction results for around 77% of stocks for the next day prediction and around 56% of stocks for a prediction of the next 10 days or 10 days in advance.

IV. Results and Analysis

A. Model Evaluation

The authors first trained the model using RNN, two types of RNNs were used in the process. The training through RNN using python is shown in table 3. While training with the first RNN, GRU and dense layers were used along with ReLU and Sigmoid activation functions. Four hidden layers were used in the process of prediction and the accuracy achieved was around 68.9%. While training with the second RNN, dense layer with ReLU and Sigmoid activation functions along with five hidden

layers are used in the prediction process. The authors have obtained 58.22% accuracy.

Table 3: Training through Rnn And Corresponding Accuracy

Attribute	Layer	No. of hidden layers	Activation functions	Accuracy
1	Gated Recurrent Unit (GRU) Dense	4	Rectified Linear Unit (ReLU) Sigmoid	68.9%
2	Dense	5	ReLU Sigmoid	58.22%

The authors then used MLP for training the model using python, no. of hidden layers was calculated by dividing the shape of the training set with 50 which is taken as the hidden layer sizes variable and activation function used was ReLU. The authors have calculated the next day, 2 days, 4 days, 6 days, and 10th day predictions in advance. The accuracies of training and testing through MLP is shown in the table 4. Based on the testing results, the next day prediction using MLP was found to be with 81.6% accuracy and the 10th day prediction was 54%.

Table 4: Training And Test Accuracy of Mlp

Day	Train accuracy	Test accuracy
1	81.9%	81.6%
2	76.5%	76.4%
4	69.4%	69.3%
6	64.8%	64.6%
10	55%	54%

The authors then used LGBM. Firstly, the authors tuned the parameters to obtain the optimal parameters which can be used for training using python. The optimal parameters obtained after parameter tuning are shown in table 5. Then, these are passed to the LGBM model for training and obtained a trained model. The authors have observed the accuracy of 53.08%.

Table 5: Optimal Parameters Of Lgbm

Parameter	Values of the parameter
n_estimators	2500
max_depth	6
colsample_bytree	0.859
min_child_samples	72
sub_sample	0.876
reg_lambda	0.1

LGBM did not provide the effective accuracy, so the authors have used the XG-Boost model for training using python. The process starts by tuning the parameters on the training set and obtain the optimal parameters. Since, the data used for the anticipation of stock price movements is time series data, Time Series Split from scikit learn is used to do cross validation with 5 folds inside Randomized Search CV to find the best set of optimal parameters. Time Series Split helps to do cross validation with time series data by maintaining temporal restrictions while creating folds. The optimal parameters found are shown in table 6 and are listed below along with the description.

- n_estimators: no. of trees to build
- max_depth: maximum depth of a tree
- subsample: percentage of data to be sampled before constructing the tree
- colsample_bytree: percentage of columns to be sampled before the tree construction
- min_child_weight: minimum value of sum of instance weight required in a child
- gamma: minimum loss minimisation needed to further partition the leaf node of a tree
- reg_lambda: regularization term on weights which determines how conservative the model is
- reg_alpha: the term of regularization on weights which determines how conservative the model is
- learning_rate: this is used to prevent overfitting in a model

Then, these parameters are applied on the test set. Lastly, calculate the results using XG-Boost model. The authors have observed the equal proportions of true positive, true negative, false positive and false negative values using XG-Boost for the next 10th day prediction. The accuracy obtained after training and testing with the XG-Boost model is shown in the table 7. The true positive rate of 55%, the true negative rate of 53% and an overall accuracy of 54% was obtained. A series of models were built to predict 1-10 days in advance. The model's next day prediction accuracy was about 77.01% and it decreased day by day gradually.

Table 6: Optimal Parameters of Xg-Boost

Parameter	Value of the parameter
n_estimators	5000
max_depth	8
subsample	0.7
colsample_bytree	0.8
min_child_weight	10
gamma	2
reg_lambda	1
reg_alpha	2
learning_rate	0.01

Table 7: Training and Test Accuracy of Xg-Boost

No. of days	Training accuracy	Validation accuracy
1	76.19%	77.01%
2	71.85%	72.73%
3	68.46%	69.01%
4	65.76%	66.26%
5	63.36%	63.75%
6	61.36%	61.62%
7	60.13%	59.65%
8	59.55%	59.85%
9	54.83%	53.13%
10	54.37%	53.40%

The final model selected after training all the models is XG-Boost. Because, GBMs are based on decision trees rather than hidden layers, they are much interpretable than neural networks. They are also fast in comparison with neural networks and fit quickly. For these reasons, MLP is not chosen as the final model, the accuracies obtained are also almost equivalent, and the computational time of MLP is much more than XG-Boost, so XG-Boost is chosen as the primary model.

B. Results Visualisation

Firstly, the accuracies for the next day prediction of all the models are compared and are shown in table 8.

Table 8: Accuracy Comparison

Model	Accuracy
Recurrent Neural Network (RNN)	68.9%
Light Gradient Boosting machine (LGBM)	53.08%
Multi-layer Perceptron	81.6%
Extreme Gradient Boosting Machine (XG - Boost)	77.01%

The accuracy comparison for 10 days in advance or the next 10 days is shown in table 9 for MLP and XG-Boost. Since they gave the highest accuracy, the predictions were done using these two models.

Table 9: The Accuracy Comparison For Next 10 Days

Model	Next day	2 days	4 days	6 days	10 days
MLP	81.6 %	76.4%	69.3%	64.6%	54%
XG-Boost	77.01%	72.73%	66.26%	61.62%	53.40%

The training and test accuracies of XG-Boost are plotted and are shown in figure 3. The authors have observed that the accuracies decrease gradually from next day to 8 days and there is a drastic decrease in the accuracy of the next 10th day prediction.

The true positive and true negative rates of XG-Boost are plotted and are shown in the figure 4. The authors have observed that the true positive and true negative rates decrease up to the next 6 days and there is a variation of the true positive rate and the true negative rate for the next 7th day to 10th day prediction. In the next 7th day prediction, the true positive rate increases and true negative rate decreases. In the next 8th day prediction, the true positive rate decreases and true negative rate increases, both meeting at a point. In the next 9th day prediction, the true positive rate increases and the next 10th day prediction it decreases and vice versa.

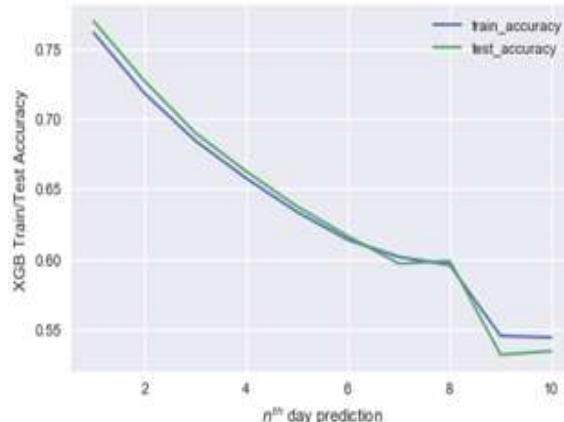


Fig 3: Training and test accuracy of XG-BOOST

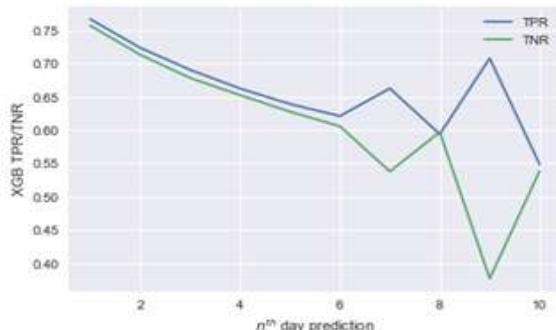


Fig 4: The true positive rate and the true negative rate of XG-BOOST



Fig 5: Flask app for visualisation

An innovative part of this article is the development of an interactive, flask-based web application in Data Driven Documents (D3) by the authors. Many researches done till the date have hardly done any visualization of the results. This interactive web application is built to show stock price and volume over time. This app also shows which news has more effect on the stock price movement on a given day. It consists of two pages: a front page that introduces the topic, also has an explanation of how to use the app, and provides information regarding the news features importance in the stock price prediction. It has a separate page for visualising the graph of particular asset. The figure 5 is the second page of the app which has six sections in it which are explained in detail.

1. The list of stocks is given from which the user can select a stock to view the corresponding information of that stock.
2. The stock price movement trend can be observed and the tool tip shows the expected and predicted stock price movement. The predicted arrow shows the direction our model expected to move and the expected arrow shows the direction which actually occurred.
3. The ticker shows the user volume and the actual price of the stock on a particular date. If the cursor is moved on the line plot the date changes.
4. The legend at the top can be used to choose the time period for which he is interested to see the stock price pattern.
5. The blue box allows the user to select the custom time window and also one can scroll over it.
6. Here one can see the list of news items for the date of interest. It also shows the sentiment value 1, -1, or 0 being positive, negative or neutral. It

also shows the urgency value that is 1 for alerts and 3 for articles. The colour of the news indicates the positive or negative effect on stock price movement. Green is for positive news and red is for negative news.

V. Conclusion

Currently, many researches focus on stock price prediction using the historical market data. Earlier researches using market data have produced accuracies of around 80.08% for forecasting the stock prediction on Tehran Stock Exchange data using Decision Tree model [10]. Our model using the news data produces accuracies around 77% for the next day prediction, proving that news plays an important role in stock price movement. Since, the news data has an impact for longer durations it can be used by investors to make long term investment decisions, because market data has random fluctuations. The future research can include seeing whether keywords within articles impact stock price movement or certain resources have much influence. To achieve this, we can use the API of News. The authors have used dataset downloaded from Kaggle which was spanned till 2016, so it would be better to see how the model reacts with the current data.

References

- [1] T. J. Dorsey, *Point, Figure & Charting*. Canada: John Wiley & sons, 2007.
- [2] (2018) Two Sigma. Using News to Predict Stock Movements. [Online]. Available: <https://www.kaggle.com/c/two-sigma-financial-news>.
- [3] G. S. Atsalakis and K. P. Valavanis, "Surveying Stock Market Forecasting Techniques – Part ii: Soft Computing Methods" *Expert Syst. Appl.*, vol. 36(3), pp. 5932-5941, 2009.
- [4] E. Basti, C. Kuzey and D. Delen, "Analyzing Initial Public Offerings, Short- term Performance Using Decision Trees and SVMs." *Decis. Support Syst.*, vol. 73, pp. 15-27, 2015.
- [5] S. G. Chowdhury, S. Routh, and S. Chakrabarti, "News Analytics and Sentiment Analysis to Predict Stock Price Trends" *International Journal of Computer Science and Information Technologies*, vol. 5(3), pp. 3595-3604, 2014.
- [6] A. Dutta, G. Bandopadhyay, and S. Sengupta, "Prediction of Stock Performance in the Indian Stock Market Using Logistic Regression" *International Journal of Business and Information*, vol. 7(1), pp. 105-136, 2012.
- [7] H. Gunduz, and Z. Cataltepe, "Borsa Istanbul (bist) Daily Prediction Using Financial News and Balanced Feature Selection" *Expert Syst. Appl.*, vol. 42, pp. 9001-9011, 2015.
- [8] S. Heston, and N. R. Sinha, "News versus Sentiment: Predicting Stock Returns from News Stories" *Finance and Economics discussion series*, 2016.
- [9] K. Ho and W. Wang, "Predicting Stock Price Movements with News Sentiment: An Artificial Neural Network Approach" *Artificial Neural Network Modelling*, Springer, pp. 395-403, 2016.
- [10] S. B. Imandoust, and M. Bolandraftar, "Forecasting the Direction of Stock Market Index Movement Using Three Data Mining Techniques: The Case of Tehran Stock Exchange" *International Journal of Engineering Research and Applications*, 4(Issue 6(version 2)), pp. 106-117, 2014.
- [11] I. P. Markovic, M. B. Stojanovic, and M. Bozic, "Stock Market Trend Prediction Using Support Vector Machines" *Facta Universitatis Series: Automatic Control and Robotics*, vol. 13(3), pp. 147-158, 2014.
- [12] L. C. Martinez, D. N. da Hora, de M. Palotti, J. R. W. Meira, and G. L. Pappa, "From an Artificial Neural Network to a Stock Market Day – Trading System: A Case Study on the BM&F BOVESPA" in *International Joint Conference of Neural Networks*, 2009, p. 2006-2013.
- [13] A. Mittal, and A. Goel, "Stock Prediction Using Twitter Sentiment Analysis" in *Conference Proceedings*, 2011.
- [14] A. Nagar, and M. Hahsler, "Using Text and Data Mining Techniques to Extract Stock Market Sentiment from Live News Streams" *International Conference on Computer Technology and Science*, 2012.
- [15] T. H. Nguyen, and K. Shirai, "Topic Modelling based Sentiment Analysis on Social Media for Stock Market Prediction" in *Proceedings of the 53rd Annual meeting of the Association for Computational Linguistics and the 7th International Joint Conference on Natural Language Processing of the Asian Federation of Natural Language Processing*, 2015, p. 1354-1364.
- [16] B. Pang, and L. Lee, "Opinion Mining and Sentiment Analysis" *Foundations and Trends in Information Retrieval*, vol. 2(1-2), pp. 1-135, 2008.
- [17] Y. Shykevich, T. M. McGinnity, S. A. Coleman, and A. Belatreche, "Predicting Stock Price Movements Based on Different Categories of News Articles" *2015 IEEE Symposium Series on Computational Intelligence*, 2015, p. 703-710.
- [18] W. Yu, B. Lea, and B. Guruswamy, "A Theoretic Framework Integrating Text Mining and Energy Demand Forecasting" *International Journal of Electronic Business Management*, vol. 5(3), pp. 211-224, 2007.

A Deep Learning Approach to Identify Missing Children

P.Vasanth sena

Department of Information Technology
Chaitanya Bharathi Institute of Technology
Hyderabad-500075, India
vasanthesena_it@cbit.ac.in

K.Sanjay Kumar

Department of Information Technology
Chaitanya Bharathi Institute of Technology
Hyderabad-500075, India
ugs17109_it.sanjay@cbit.ac.in

Prof. Sammulal Porika

Department of CSE
JNTU CEJ
Hyderabad-505501, India
sammulalporika@gmail.com

Dr.M.Venugopala chary

Department of Information Technology
Chaitanya Bharathi Institute of Technology
Hyderabad-500075,India
mvenugopalachari_it@cbit.ac.in

M.Banu

TejaDepartment of Information Technology
Chaitanya Bharathi Institute of Technology
Hyderabad-500075, India
ugs17322_it.teja@cbit.ac.in

Abstract: India is the world second most populous nation and children represent a greatest significance among them. Every year, unfortunately, a large number of children are missing. On an average 200 children are missing for each day. It becomes a tedious task for the police to identify missing children if the child is too young. Therefore, an application is required to identify and track them easily. To overcome this problem a deep learning approach is to be followed and used facial recognition to identify the missing child images. We adopted a transfer learning-based Convolution Neural Network(CNN) which is Residual Architecture (ResNet) model where it extracts high-level facial features. Child images are classified based on a trained KNN classifier.

Keywords: Deep Learning, Facial Features, Transfer Learning, Resnet Architecture

I. Introduction

Facial recognition is a prominent biometric tool that measures a variety of facial features. There are other common biometric tools like iris recognition, fingerprint detection which require voluntary actions i.e., for iris detection the user needs to stand in front of camera, and for fingerprint detection, the person has to place the hand on a fingerprint scanner. For finger print recognition, the person has to register their biometrics using finger print scanner. For face recognition, no human intervention is required that using a distance camera a person face can be recognized. Before recognizing faces, first camera detects face and then recognizes that face based on variety of facial features, system can recognize the person.[1]. Facial recognition identifies a person based on specific facial features. It

measures a wide variety of facial features which are commonly called nodal points on the face.

These features typically include the distance between the eyes, the width of the nose, edge detections, distance from the forehead to chin, and collects different measurements. This information is stored as a unique facial signature which is then compared to other known images in the database. To identify missing children there are many challenging factors i.e. if the child is missed for longer days, the texture of the skin will be changed. The Shape and texture of the skin will be changed with the aging effects and will be reflected in images. Therefore, feature descriptors are extracted which are invariant to the aging effects[2].

We proposed deep learning-based facial recognition which is invariant to these aging effects. CNN-based Resnet architecture is used to extract features based on the transfer learning approach. In transfer learning, a model is trained on a large data set say Image net for few days. Now, the knowledge of trained model can be used for the customized data which is of a similar kind. Transfer of knowledge generally includes leverage of weights or biases to the new model, so that there will be good results on the new model.

This paper is organized as follows. Section II describes the literature survey. Section III describes the System Architecture. Section IV describes the Proposed system followed by Section V which explains results and analysis. Conclusion and future work are described in the last section.

II. Literature Survey

In [3] Facial Features are extracted through HOG (Histogram Oriented Gradients) which is a

popular facial descriptor in object detection. Image is divided into spatial regions and each cell is of $N \times N$ pixel[4]. For each original image, calculated the gradient in the horizontal direction and vertical direction. For a function $f(x,y)$, the gradient is represented as the vector (f_x, f_y) . An Image is a discrete function of (x,y) and an image gradient can be calculated. At each pixel, image gradient horizontal (x-direction) and vertical(y-direction) are calculated.

These vectors have a direction $\text{atan}(\frac{f_y}{f_x})$.

The magnitude of the vector is. $\sqrt{(f_x^2 + f_y^2)}$

Gradient values are mapped to 0-255. Pixels with significant negative change will turn black, pixels with lot of positive shift will turn white and pixels that have no change will be gray. In this way, it represents each image in orientation and magnitude and extracts facial features. The HOG features are not invariant to aging effects and it is not invariant to the posture of different images. The limitation of this method is for large data sets it slows down the speed and gives less accuracy. Results of [2] gave better performance and accuracy.

In [1] Facial recognition is performed to recognize child images by using Principal Component Analysis(PCA). PCA performs dimensionality reduction to extract features from images. PCA algorithm is mostly used in data analysis and for making models like face recognition. PCA algorithm is based on eigen vectors and performs the multivariate analysis. It generates the internal structure of the data along with the direction and features of the data. PCA transforms the training set of images into a lower-dimensional picture. It uses an orthogonal transformation to a set of possibly A correlated images into a set of B uncorrelated images which are called principal components or eigen images. The transformation is defined such as the first principal component shows the most dominant features of the dataset and each succeeding component, in turn, shows the next most possible dominant features or directions, under the constraint that it be uncorrelated the preceding components. To reduce the calculations of principal components the dimensionality of the original dataset is reduced. Noise in the eigen images is discarded for better results. Since eigenfaces show the directions in the training set, and each proceeding eigen face shows fewer directions and more noise. Only a few first eigenfaces are selected whereas the rest of the eigenfaces are discarded. These eigen faces can safely represent the whole original training dataset because they depict major features. The whole training dataset images are represented in the form of eigen faces.

Each variable or image in the original dataset can be represented in the form of the weighted sum of generated eigen images. The weight vector is assigned for each image. PCA can be done by eigenvalue decomposition of a data covariance matrix.

Covariance is used to measure the relationship between two dimensions to perform statistical analysis and data analysis.. [1].The basic Covariance equations for two-dimensional data is

$$\text{covariance}(x,y) = \frac{\sum_{i=1}^k (x_i - \bar{x})(y_i - \bar{y})}{b-1}$$

In this equation, x represents the value of the pixel and \bar{x} represents the mean of all the values of x and k represents the total number of values. The covariance measures the relationship between the dimensions. The covariance Matrix can be described as

$$C_{i,j}^{K \times K} = \text{covariance}(D_i^T m_i, D_j^T m_j))$$

Where $C^{(k \times k)}$ represents the matrix with k rows and k columns and $[Dim]_x$ represents the x th dimension. Results are analyzed by using the Frontalface dataset collected at the California Institute of Technology and reported an accuracy of 91%

In[6],There is a website with the name FindFace that allows users to upload a photo and performs facial recognition which is developed by Ntech Lab, to correctly classify the images that are uploaded by the public. It generates an accuracy of 70 percent.

III. System Architecture

Our Proposed system consists of a web portal, where it takes the input as images from the public. When a child is missed, a complaint will be registered, and the recent photo of a child will be submitted to the police by the child's parents. If public had found any child in isolated place or crowded place, they can upload that child photo from any place at any time into the website and while uploading child photo, public should submit additional details like child skin tone, appearance, gender, location and remarks. After uploading details, the model starts searching that is there any matching photo in the database. If match has found with threshold accuracy, an alert in email or SMS will be sent to the concern police officer that particular child has found in this location. A Web portal is developed using Django

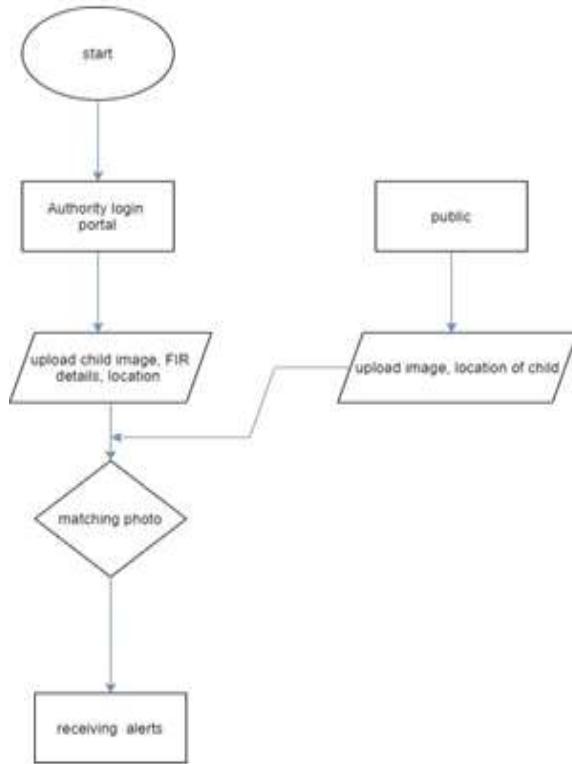


Fig 1: The Architecture of the proposed missing child identification

IV. Proposed System

We proposed a deep learning model for recognizing child images based on Transfer Learning. In transfer learning, a model is trained on a large data set and transfer the knowledge i.e., weights and biases to the customized models. With this approach, the learning process can be faster and more accurate. It is more reliable than Traditional CNN.

A. Convolution Neural Networks

Convolutional neural networks shortly known as CNN created a great hype in deep learning. CNN is mostly used for image classification. CNN detects patterns that are useful for image analysis. CNN has hidden layers called convolution layers and these hidden layers make actual CNN. The Convolution operation is applied on convolution layers. CNN can detect patterns in images because of these convolution layers. In each convolution, layer filters are applied. CNN has weights updated while training network. After applying a convolution function on the layer an activation function is also applied like ReLU called rectified linear units. CNN also comprises max pooling. In deep learning and machine learning models training part plays a key role. In plain networks like VGG-16 that is a regular network.

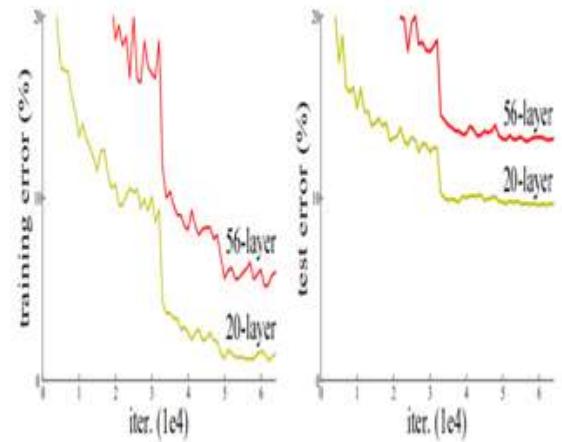


Fig 2: Comparison of error percentage in plain networks

The above figure explains about training and testing error of plain networks by plotting a graph from 20 layers network to 56 layers network. So, the number of layers increases from 20 to 56 layers even after many iterations the training error of 56 layers network is performing worse than 20 layers neural network in test error. The deeper we train the more error rate percentage.

So, we want to train our network more deeply because in missing child identification aging factor plays a crucial role meaning if the child was missed when he has 10 years old and found when that child turned into 18 years so in this situations our model should be able to recognize the person more accurately to do so we need a CNN architecture called residual networks.

B. Resnet Architecture

Residual networks are shortly known as resnets. To use resnets we need to build the residual block. This residual block comprises of input, weight layers on this weight layers filters are applied, activation function ReLU known as rectified linear units.

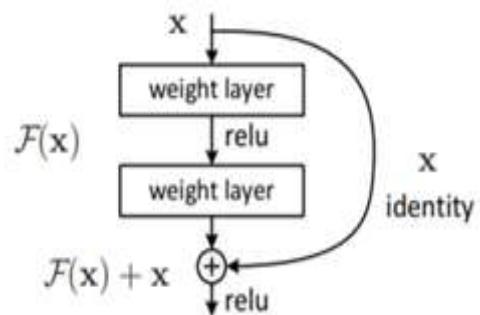


Fig 3: Block Diagram of ResNet Architecture

The above figure is known as residual block. Here x is the input given to weight layer filters are applied on this hidden layer. Resnets skips the connection in the network by performing regularization of various levels L1,L2 because when the layer output is zero that layer isn't useful so it skips layer if the layer output is non zero that is given to next layer performs activation function Relu on it and sums it this is how it skips connection between in-network

Deep Neural Networks are hard to train because of the vanishing gradient problem, as it requires updating the weights by using back propagation and chain rule of calculus. So while using the chain rule of calculus the repeated multiplication of weights will make the weights extremely small while reaching the earlier layers. Multiplication of derivation of values at each layer will lead to a small value while to earlier layers. This is called the Vanishing gradient problem. But in ResNet, there is a solution to the vanishing gradient problem. ResNet uses the concept of skip connections, using this skip connection we can resolve the vanishing gradient problem. In ResNet, original input is added to the output of the convolution block and this is called skip connection. It uses skip connection to resolve the vanishing gradient problem because some layers are getting skipped and the values are not reached to a very small.

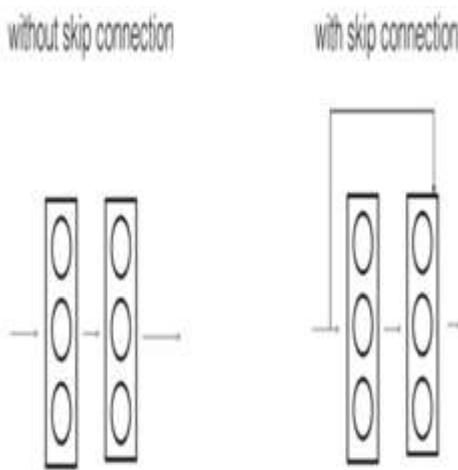


Fig 4: convolution layers without skip connection and convolution layers with skip connections

As shown in Fig 2, x is an input and traveled to each layer. $F(x)$ is loss function calculated based on Input and finally, we get output Y . In ResNet, actual input is added to the convolution block and therefore Y is given by

$Y = F(X) + X$, where $F(X)$ is loss function and x is input. The main idea of the Residual Networks algorithm is to make input and output equal and to do

this ResNet makes the value of $F(x)$ to 0 so that the value of input and output can be equal. The main intuition behind the algorithm is, the network will learn from the difference between values of input and output so that overall accuracy can be increased.

In Traditional algorithms, networks are trained based on the value of output (Y), but in Residual Networks are trained based on the value of loss function ($F(x)$) and its target is to make $F(x)=0$ then input, and output values become similar.

In ResNet 50, it consists of 50 layers including average pooling layers. In the first layer, it contains a filter size of 7×7 with such 64 filters and the value of stride is 2.

There are convolutional layers that are stacked on one another in ResNet50, In the first convolutional layer, it consists of a 1×1 filter with size 64

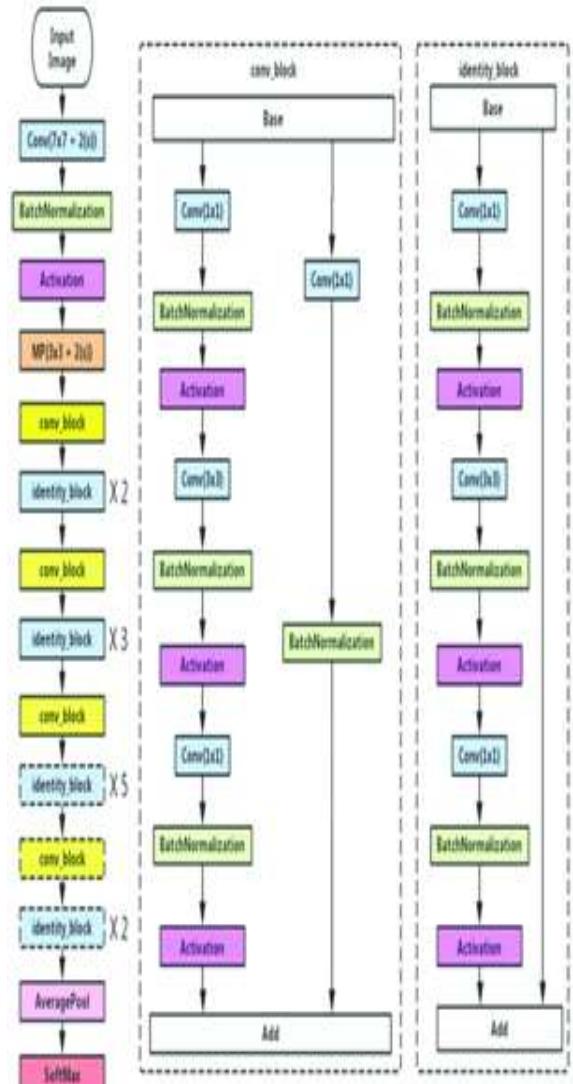


Fig 5: Layered Architecture of ResNet50

To reduce the size of an image on each layer, ResNet uses the following formula

$$r = \frac{n+2p-f}{s} + 1 * \frac{n+2p-f}{s} + 1$$

Where r= reduced size of image, p= size of padding f= size of filter s= size of stride. It consists of an Identity block and convolution block. When the size of an input image is equal to the size of the output image, then it uses an identity block to add actual input to the loss function. If the size of input and output is different then it uses a convolution block.

C. k-NN Classifier

Now after training the model for classifying images, we used k nearest neighbors' algorithm popularly known as k-NN face images are compared using this classifier here the task of the public is to upload the image of an innocent child who might be crying or staying in isolated places. In CNNSoftMax is replaced with k-NN trained with the feature vector of each image. Extracted feature vector array is used to train this classifier. k-NN relies on the distance between feature vectors in a cluster. To use KNN we need to apply Euclidean distance as the distance metric given below.

$$d(x, y) = \sqrt{\sum_{k=1}^m (x_k - y_k)^2}$$

V. Results

Our proposed model is tested on the FGnet dataset where it consists of 1500 images of 62 unique people. It consists of images of child images of different ages with different postures. The Accuracy of the algorithm is measured based on the ratio of missing child images correctly classified to the total images in the database.

$$\text{Accuracy} = \frac{\text{Number of missing child images correctly classified}}{\text{Total Number of child images in the database}}$$

The calculated accuracy of the proposed Resnet algorithm was approximately 92%

VI. Conclusion

Missing children are identified easily by using the deep learning techniques which include facial recognition based on CNN ResNet Architectures. The proposed algorithm will work well for different kinds of challenges like image posture,

aging effects, background variations in the images, and the size of the database. In Future, we will build an android application to track the missing children easily by adding a Bluetooth feature to give notification to nearby people.

References

- [1] Rohit Satle, Vishnuprasad Poojary, John Abraham, Shilpa Wakode, "Missing child identification using face recognition system", International Journal of Advanced Engineering and Innovative Technology (IJAEIT), Volume 3 Issue 1 July - August 2016.
- [2] Pournami S Chandran, Byju N B, Deepak R U, Nishakumari K N, Devanand P, Sasi P M "Missing child identification using deep learning and multi-class of SVM", 2018 IEEE Recent Advances in Intelligent Computational Systems (RAICS).
- [3] O. Deniz, G. Bueno, J. Salido, and F. D. la Torre, "Face recognition using histograms of oriented gradients", Pattern Recognition Letters, 32(12):1598–1603, 2011.
- [4] A. Albiol, D. Monzo, A. Martin, J. Sastre, and A. Albiol, "Face recognition using hog–ebgm," Pattern Recognition Letters, vol. 29, no. 10, pp. 1537–1543, 2008.
- [5] Sandeep Mishra and Anupam Dubey "FACE RECOGNITION APPROACHES: A SURVEY", International Journal of Computing and Business Research (IJCBR), Volume 6 Issue 1 January 2015
- [6] <https://en.wikipedia.org/wiki/FindFace>
- [7] Simonyan, Karen and Andrew Zisserman, "Very deep convolutional networks for large-scale image recognition", International Conference on Learning Representations (ICLR), April 2015.
- [8] Manal Abdullah, MajdaWazzan, Sahar Bo-saeed, "OPTIMIZING FACE RECOGNITION USING PCA," International Journal of Artificial Intelligence & Applications (IJAIA), Vol.3, No.2, March 2012.
- [9] Vasanth Sena P., Porika S., Venu Gopalachari M., "A Mining Framework for Efficient Leakage Detection and Diagnosis in Water Supply System." In: Kumar A., Mozar S. (eds) ICCCE 2020. Lecture Notes in Electrical Engineering, vol 698. Springer, Singapore. https://doi.org/10.1007/978-981-15-7961-5_101
- [10] Vasanth Sena P., Sammulal P. "An Optimal Heuristic for Student Failure Detection and Diagnosis in the Sathvahana Educational Community Using WEKA". In: Kumar A., Mozar S. (eds) ICCCE 2018. ICCCE 2018. Lecture Notes in Electrical Engineering, vol 500. Springer, Singapore.
- [11] P. Vasanth Sena and Dr. Sammulal P "A Survey on Leaks and Faults Detection & Diagnosis in Water Supply System" International Journal of Engineering, Science and Mathematics, Year 2018, Volume 7, Issue 2, pages from 174-180, Online ISSN : 2320-0294.
- [12] P Vasanth Sena, P Sammulal, Suresh Pabboju, D L Srinivasa Reddy, "A Mining Frame Work of CO-PO Attainment using Deep Learning Techniques" in International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-4S2, March 2020.

Session-A3:
Artificial Intelligence and Deep Learning

Implementation of a Privacy based Deep Learning Algorithm for Medical Data Analytics

Thirupathi Battu

Research Scholar

Department of Computer Science and Engineering
Osmania University, Hyderabad-500007, India
battuthirupathi2@gmail.com

Dr.D.Lakshmi Sreenivasa Reddy

Associate Professor

Department of Information Technology
Chaitanya Bharathi Institute Of
Technology(A), Hyderabad-500075, India
dlsrinivasareddy_it@cbit.ac.in

Abstract: Medical data classification is the most challenging research problem because it provides more excellent business value in any analytics setting. Classification is a method of labeling data that makes the analysis more cost-effective and reliable. The accuracy of the function, according to the study, may have a negative effect on classification performance. Since privacy is needed when a user shares a sample feature to collect appropriate features from a databank and vice versa, this study looks at how privacy affects the feature selection process. It should have no effect on classification efficiency if a privacy-preserving mechanism is used. The thesis work develops PPCS-MMDML, an integrated platform for privacy-based feature selection and efficient Medical data heterogeneous image set classification, with these concerns in mind. The PPCS selects a subset of features while maintaining privacy between the patient and the databank, and MMDML, a deep learning tool, efficiently classifies Medical data in a Medical data environment with limited running time. All proposed classification models and privacy-preserving mechanisms were tested qualitatively for classification accuracy and running time.

Key words: PPCS, MMDML, Medical data.

I. Introduction

Medical Data

Medical expression data can handle large amounts of data, and analytical skills can resolve the limitations of existing data processing systems [15]. The increasing use of sensors, the internet, heavy computers, and other technologies in a flying ratio has resulted in a rapid increase in data in today's digital world. The characteristics of medical data, such as velocity and length, have complicated the handling of the data by computing systems. Traditional data management, warehousing, and storage methods and processes fail to process such a diverse set of data. A distributed architecture file system manages medical data storage to address this complication..

Medical data is classified into the following categories..

- Structured data
- Unstructured data
- Semi-structured data

Deep Learning

Deep learning uses supervised or unsupervised methods to classify deep architectures and naturally include hierarchical illustrations [15, 18]. Lower layer notions can characterize upper layer notions, and upper layer notions can be used to characterize lower layer notions. Deep learning is a form of machine learning technique that learns by using representations. Consider an image that can be interpreted in a number of ways (such as a vector of pixels), but only a few of them are useful in deciding what the image is.

Need for Privacy

Instead of allowing medical data to be used productively by people, the exploding amount of data has multiplied unrecognized privacy breaches. For instance, Google, Amazon, and other companies are studying our online shopping habits and surfing habits. Social networking websites, such as Facebook, store and analyse private information about our lives and social relationships. Familiar video sites, such as YouTube, recommend our favourite videos based on our search history. Medical data's ability to collect, deposit, and reuse classified information for commercial benefit poses a threat to private information.

II. Literature Survey

Xiaojun Chen et al. proposed a novel function categories weight subspace and high dimensional data clustering technique. Data with a high dimensionality is divided into feature categories based on their common characteristics. They proposed two types of weights to simultaneously calculate the impact of feature categories and specific features in each cluster and an advanced optimization architecture to characterize the optimization activity..

Qinbao Song et al. proposed the Quick approach, which combines feature selection with fast clustering. It operates at two different speeds. In the first step, the features are partitioned into clusters using a graph-theoretic clustering technique. In the second pace, the most important features of the target class are chosen from each cluster for framing feature subsets.

For catching non-linear input-output dependency, Makoto Yamada et al. proposed a feature-wise Kernel zed Lasso technique. This method was created to address the FVM's inadequacy issue. The advantage of this new construction is that it essentially produces a globalized optimum outcome. It can be extended to include functionality with a high degree of dimensionality. This technique can classify non-redundant features and have a high statistical dependency on resultant values defined by kernel-based independence dimensions such as HSIC, NOCCO, etc.

According to a survey conducted by Zheng Zhao et al., existing feature selection activities fully select features that preserve sample homogeneity and are unified in a shared framework. This architecture was incapable of dealing with redundant functions. They developed a similarity preserving feature selection technique in an accurate and challenging manner based on these considerations.

Ciresan et al. [16] proposed a GPU-based CNN technique that uses online gradient descent to practice. The CNN varies in terms of how the convolution and subsampling layers are implemented and the methods used to train the network. The convolution layer runs convolution operations using different filter maps of equal size, while the subsampling layers perform averaging pixels using max-pooling to reduce the size of the advancing layer.

Rajat Raina et al. [66] have developed a parallel-based technique for speeding up networks for large-scale applications. The authors explore advanced (GPU) Graphics Processor Units' ability to learn large DBN and sparse coding simulations.

James Martens [56] developed a second-order optimization technique for training deep auto-encoders based on the "Hessian open" process. This approach can be used to overcome the under-fitting problem that is discovered when training deep auto-encoder neural networks for large models and datasets.

III. Existing Method

The number of existing methods for ensuring data privacy and graph security is

enormous. This segment examines a few existing approaches.

Privacy preserving aggregation

This method, which is based on homomorphism encryption [63], is ideal for data collection. When a group of people wants to distribute their data together, they use a standard public key to encrypt their own data. The cipher text from all individuals involved in the correspondence is then gathered and shared. The data is decrypted by the approved user using a unique private key. This privacy-preserving aggregation approach protects the privacy of individual data during the processing and storage of medical data. This approach's problem is that the cypher text gathered for one goal cannot be used for other goals. As a result, since medical data analysis is objective-specific, the standard privacy-preserving aggregation approach is ineffective.

Operations over encrypted data

Individual data encryption is used to protect confidential information, and the keywords associated with it are saved in third-party storage [47]. When the user has a need to read the data, the query can be used to retrieve it from storage. Operations over encrypted data ensure data protection, but the problem is that they take a long time to compute. It's also a difficult procedure. Medical data must be processed quickly and in large quantities. As a result, for medical data analytics, this approach is ineffective.

De-Identification

De-identification is a popular method for providing privacy assurance. Data must be virus-free, and only the bare minimum of information can be shared with others to protect an individual's privacy. Compared to operations over encrypted data and privacy-preserving aggregation approaches, the de-identification approach is more powerful and adaptable to data analytics [11]. However, there is a risk of providing external information to a hacker in a medical data environment in the de-identification process, resulting in privacy concerns. As a result, this approach is unsuitable for ensuring privacy in medical data.

IV. Proposed Methodology

PPCS-MMDML Algorithm

- a. **PPCS Working:** Determining the subclass of meaningful features for defining a classification layout is known as feature selection. In terms of the classification model, it rejects superfluous and mismatched functions. The PPCS [52] does

the same thing in a very good way by protecting privacy. This approach checks the privacy-preserving coined similarity of the user input image features with all image features available in the databank without any privacy negotiation. In other words, when measuring the PPCS of the function between the user and the databank, private information is not exchanged on both sides. The PPCS calculation's boundaries should be between -1 and 1, respectively. For angular values ranging from 0 to 180 degrees, the spectrum of cosine similarity values is considered. When the cosine angle of the image features vectors is zero, the PPCS similarity range between user input image features and databank image features is high. The features with the greatest similarity are counted up in an empty subset after PPCS is determined for all pairs of features. The MMDML classification method uses this new derived subset from PPCS as an input. Table 1 shows the steps in the PPCS algorithm.

$U_A = \text{User Image A}$ $\vec{u} = (u_1, u_2, \dots)$ $D_B = \text{Databank Image B}$ $\vec{d} = (d_1, d_2, \dots)$
Page 1: U_A Computation: ϵ, α, β are the given security factors Identify larger prime numbers p , Predefine $ h = \epsilon, h = \alpha$ Apply $\beta = 0$ Select a big random number ϵ

and $+2$ random numbers $r_i = 1, 2, \dots +2$, with $ r_i = p$ For every $i = 1, 2, \dots +2$ $= (r_i \cdot a + b) \mod p \neq 0$ Find for Determine $\beta = \sum r_i$ Maintain β as secret Issue $(\vec{u}, \beta) \rightarrow U_A$
Page 2: D_B Computation (Computed for all databank images with respect to input) Apply $\beta = 0$ For every $i = 1, 2, \dots +2$ $= (r_i \cdot a + b) \mod p \neq 0$ where r_i is a random number with $ r_i = p$ End for $\beta = \sum r_i$ and $\beta = \sum r_i$ Issue $(\vec{d}, \beta) \rightarrow D_B$

Page 3: U_A Computation Determine $\beta = \sum r_i$ Determine $\beta = \sum r_i = \frac{(r_i - \bar{r})}{n}$ $\cos(\vec{u}, \vec{d}) = \frac{\vec{u} \cdot \vec{d}}{\sqrt{n}}$
--

Table 1: PPCS Algorithm for User and Databank

V. Tools and Techniques

On an Intel(R) Core(T.M.) i5-2410M CPU @ 2.30GHz and 16GB RAM, the proposed approach is implemented using Matlab2012a and Hadoop. The Matlab2012a system is used to pick features while preserving privacy using PPCS. After the features have been chosen, the MMDML is designed using the Hadoop tool to reduce the run time for Classification. 6.4.1 Collection of data The output of PPCS-MMDML is validated using data from OSIRIX viewer [62] and the Mammographic Image Analysis Society (MIAS) [74]. All images used in PPCS-MMDML are 1024 x 1024 pixels in size. Parameters like runtime analysis and classification accuracy for brain, bone, and breast cancer disease justify the efficiency of PPCS-MMDML, which are dependent on the values of h and h , which are dependent on the network parameters and. As a result, an iterative approach is used to find the local best solution. The stochastic sub-gradient descent method was chosen over the other 94 traditional methods for calculating the optimised values for the MMDML classifier because it considers manifold margin, allowing for efficient class-specific and discriminative data analysis..

VI. Results and Discussions

Table 2 shows the computational comparisons of the existing MMDML and the proposed PPCS-MMDML for various datasets. When compared to the existing MMDML process, the PPCS-MMDML method takes less time to execute various datasets.

S.No	Datasets	Running time ($\times 10^5$ in ms)	
		MMDML	PPCS-MMDML
1	Bone Cancer	1.7	1.4
2	Brain Cancer	2.1	1.8
3	Breast Cancer	2.8	2.2

Table 2: Running time analysis of PPCS-MMDML

As compared to the existing MMDML for bone, brain, and breast cancer datasets, PPCS-MMDML takes just 1.4, 1.8, and 2.2×10^5 ms (milliseconds). The runtime analysis of PPCS-MMDML and the existing MMDML is shown in Figure 2.

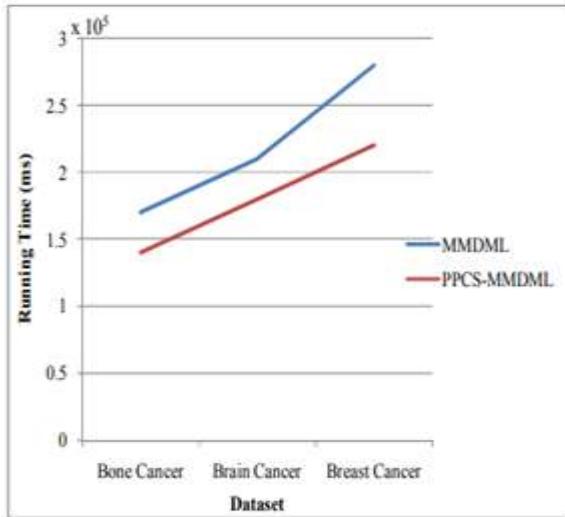


Fig 3: Running time analysis of PPCS-MMDML

The performance analyses of the existing MMDML and the proposed PPCS-MMDML in three cancer disease datasets are shown in Table 3. For bone, brain, and breast cancer disease, the PPCS-MMDML accuracy figures are 74.2, 72.6, and 77.8 percent, respectively. The comparison study shows that the proposed PPCS-MMDML outperforms the existing MMDML by 7.7%, 4.1 percent, and 6.2 percent for Classification of bone, brain, and breast datasets, respectively.

S.No	Datasets	Classification Accuracy (%)	
		MMDML	PPCS-MMDML
1	Bone Cancer	66.5	74.2
2	Brain Cancer	68.5	72.6
3	Breast Cancer	71.6	77.8

Table 3. Classification accuracy analysis of PPCS-MMDML

VII. Conclusion

The study focuses on the need for a privacy-based deep learning algorithm in medical data analytics. The idiom Medical data require the ability of the developing model to deal with length, velocity,

veracity, variety, and value characteristics. Four works introduce a privacy-based deep learning algorithm for medical data analytics while keeping these characteristics in mind. Medical data classification was the analytics task used in this study. Classifying data in the face of the medical data environment's problems and difficulties is crucial and challenging. The analysis is carried out using four proposed works for addressing the privacy and classification problems in the medical data sets.

In a medical data environment, the LNTP-MDBN deep learning scheme outperforms the other research works in terms of Deep learning is a form of machine learning technique that learns by using representations. Consider an image that can be interpreted in a number of ways (such as a vector of pixels), but only a few of them are useful in deciding what the image is. Running time and classification accuracy. Also, compared to the existing privacy mechanism in medical data, the PPCS with p-stability performs well, and the addition of this privacy mechanism has no impact on classification results.

VIII. Future Scope

In the future, this work can be extended in the following aspects:

- Integrating PPCS-LNTP-MDBN for effective privacy-based deep learning algorithm for Medical data analytics.
- Perform online learning for Classification.
- Real-time applications for different datasets.

References

- [1] Z. Zhao, L. Wang, H. Liu and J. Ye, On similarity preserving feature selection, *IEEE Trans. Knowledge and Data Engineering*, 25(3), (2013), 619–632.
- [2] M. Yamada, W. Jitkrittum, L. Sigal, E.P. Xing, and M. Sugiyama, High dimensional feature selection by feature-wise kernel zed lasso, *Neural computation*, 26(1), (2014), 185–207.
- [3] J.Q. Gan, B.A.S. Hasan and C.S.L. Tsui, A filter-dominating hybrid sequential forward floating search method for feature subset selection in high dimensional space, *Machine Learning, and Cybernetics*, 5(3), (2014), 413–423
- [4] L. Deng and D. Yu, *Deep Learning: Methods and Applications*, NOW Publishers, (2013).
- [5] Q. Song, J. Ni, and G. Wang, A fast clustering-based feature subset selection algorithm for high-dimensional data, *IEEE Trans. Knowledge. Data Engineering*, 25(1), (2013), 1–14.
- [6] D. C. Ciresan, U. Meier, J. Masci, L. M. Gambardella, and J. Schmidhuber, Flexible high-performance convolution neural networks for image classification, In Proc. Int. Conf. Artif. Intell., (2011), 1237-1242.
- [7] J. Martens, Deep learning via Hessian-free optimization, In Proc. Int. Conf. Mach. Learn., (2010), 735-742.

- [8] R. Raina, A. Madhavan, and A. Ng, Large-scale deep unsupervised learning using graphics processors, In Proc. Int. Conf. Mach.Learn., (2009), 873-880.
- [9] S.Suthaharan, Machine Learning Models and Algorithms for Medical Data Classification, Springer, (2016)
- [10] B. Brahim and L. Mohamed, Robust ensemble feature selection for high dimensional data sets, In Proc. IEEE Int. HPCS Conf., (2013), 151-157.

A Review of Wi-Fi Security Protocols and Detailed Discussion on WPA3

Jithender Reddy Machana

Vasavi College of Engineering,
Hyderabad-500089, India.
1m.jitenderreddy@staff.vce.ac.in

Ashrith Kotha

Vasavi College of Engineering,
Hyderabad-500089, India.
21602-18-735-067@vce.ac.in

Sumanth Pulluru

Vasavi College of Engineering,
Hyderabad-500089, India.
1602-18-735-049@vce.ac.in

Abstract: Wireless local area networks (WLANs) using which we avail internet services are becoming popular as they are quick, less expensive and user friendly. As the usage of personal devices, such as mobiles and smart watches, that connect to the Internet with the help of Wi-Fi increases, wireless attacks on user devices are becoming more critical. So with demand for security requirements, the Wi-Fi Alliance(WFA) has been working for years to provide uncompromised security. It's the latest contribution is Wi-Fi Protected Access-3(WPA-3). In this paper, we make a threefold contribution. Firstly, we discuss the earlier protocols Wi-Fi Equivalent Privacy(WEP), WPA. Secondly, we present the WPA2 protocol along with the faults. Thirdly, we elaborate the necessity of WPA3, it's features and mechanism. Subsequently, we discuss some security threats and the ability of WPA3 to mitigate them. The spellbinding part of the paper is that we can find that WPA3 still doesn't address all the existing issues and faults in its previous version WPA2.

Keywords: WEP, WPA, WPA2, WPA3, WFA, security threats

I. Introduction

The 802.11 WLAN standards specify the physical and data link layers of the OSI network model. MAC (Media Access Control) layers of the 802.11a, b, and g are considered similar. Each of the top layers utilizes the services of the underlying layers. Traditional Wired networks are in general more secure than these Wireless LANs. With no security measures, these WLANs are more vulnerable to attack by capturing the traffic, injecting the malicious software on the network. It is essential to implement secure methods for authentication and encryption of data/traffic, so authorized users or devices can access that network. Privacy of Users is achieved by protection with encryption. In 802.11, WLANs encryption is optional, but with no encryption, any other standard wireless device can read all data traffic in the network, which is considered a threat to data privacy. There have been developments in security approaches since the

inception of such an idea. Three generations of security protocols were present until recent years:

- Wired Equivalent Privacy
- Wi-Fi Protected Access)
- Wi-Fi Protected Access, Version2

They have two templates such as personal and enterprise. Security features of WPA evolved constantly to include stronger protections through encryption and new security policies as the security landscape changes.

In June 2018 Wi-Fi Alliance introduced Wi-Fi Certified WPA3, the next generation of Wi-Fi security. The advent of WPA3 brings along the improvised security with key features like individualized encryption and easy connect, an option that eases IoT devices, screen less devices to connect easily to the network.

II. Brief Overview of WEP and WPA

Wired Equivalent Privacy (WEP)

WEP is designed to secure wireless networks. This security protocol is designed to provide a wireless network with the same standard of confidentiality as experienced in a wired network. A security protocol is intended to provide data integrity and encryption. Integrity ensures that message is not manipulated while encryption prevents other users from knowing the message content. WEP uses wireless security that is achieved by WAP with a (64 or 128) shared key.

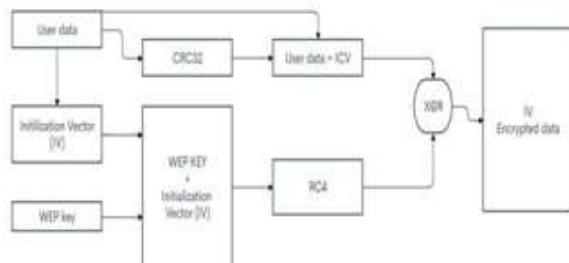


Fig 1: Flow chart describing Wired Encryption Protocol (WEP) process.

Firstly, a 32-bit (CRC32) is employed to perform Integrity Check. Secondly, RC4(Rivest Cipher 4) is an encryption algorithm generating (40 or 104) bits WEP key along with Initializing Vector of 24 bits. The former was to provide data integrity while the latter was to encrypt. This is just a level next to plain-text passwords. Also, a single key is used for encryption of all devices[1]. Practically, WEP is vulnerable to attacks and tools can attack in minutes.

Wi-Fi Protected Access (WPA)

WPA is based on the IEEE 802.11i standard and is a better solution to address shortfalls of WEP. This is based on the same hardware as of WEP but the software needs to be updated. The two major components of WPA are TKIP and 802.1x port-based authentication. WPA uses TKIP(Temporary Key Integrity Protocol).

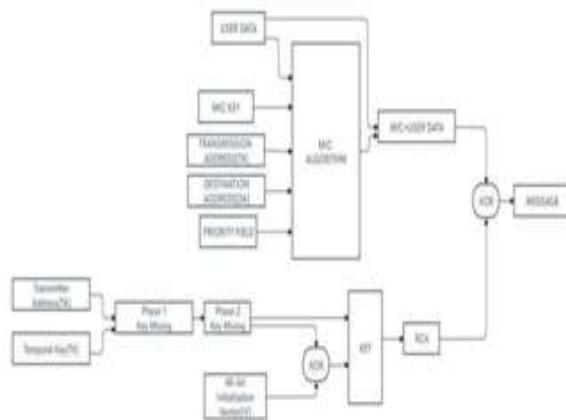


Fig 2: Flow chart describing Wired Protected Access(WPA) process.

Though TKIP uses the same RC4, it is implemented in hardware, IV was added to 48 bits. WPA improved data integrity. It uses MIC which is more efficient algorithm compared to MIC used in WEP. It depends on the data and few additional inputs, such as Source Address, Receiver Address. Hence, it is very much hard to snatch a message with MIC vector. This enables devices to authenticate packets they receive. In 802.1x port- based authentication provides a framework in which device connecting to the network(wired or wireless) need to be authenticated before being granted access.WPA has two types of authentication namely WPA-PSK and WPA-Enterprise.WPA protects good enough against users without key.WPA employs weak encryption algorithm RC4 rather than using Advanced Encryption Standard (AES). The hackers can capture data of the network protected with WPA and decrypt them.

III. Wi-Fi PROTECTED ACCESS-2(WPA-2)

WPA2 the predecessor of our main entity WPA3 is discussed here in a concise manner to understand the need for WPA3.WPA2 is backwards compatible with WPA. WPA2 improved significantly over WEP and WPA. WPA2 protocol uses AES(Advanced Encryption Standard) for data integrity and encapsulation. It replaces MIC with Cipher Block Chaining Message Authentication Code Protocol (CCMP). Since TKIP and RC4 are replaced there is a need for change in hardware as well as software. There is not much impact on network throughput using WPA2 than WPA.

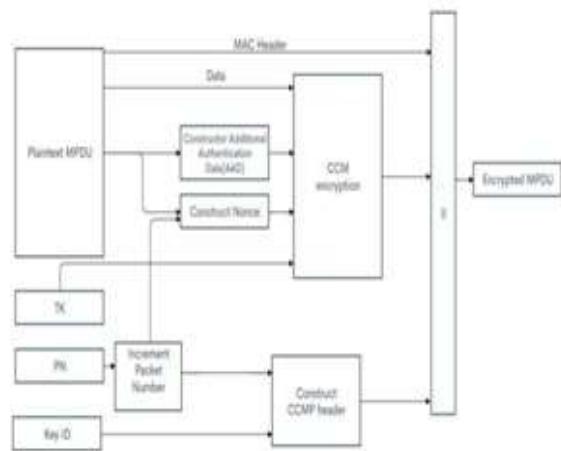


Fig 3: Flow chart describing the Wired Protected Access 2 (WPA2) process.

The Four-Way Handshake

In WPA2 protocol the four-way handshake mechanism generates encryption keys used to encrypt data that is sent over Wireless medium. As soon as we click on SSID(Service Set Identifier) of the authenticator in supplicant it goes through the process from authentication to association. A four-way handshake is used to establish another key called the Pair wise Transient Key (PTK). PMK, AP (Access Point) nonce, STA nonce (Snonce) are used to generate PTK, AP MAC address, and STA MAC address[3]. Here begins the mechanism.

1. Firstly, the access point sends EAPOL(Extensible Authentication Protocol Over LAN) message with ANonce (random number) to a device to generate PTK.
2. Once the client receives it creates PTK. Next, the device sends its SNonce. The client sends EAPOL to WAP with MIC. After receiving SNonce PTK is generated for unicast traffic encryption.

3. Later, EAPOL message is sent to the client including GTK (Group Temporal Key).
4. Finally, supplicant acknowledges the installation of PTK and GTK with an EAPOL. Now, the encrypted transmission initiated.

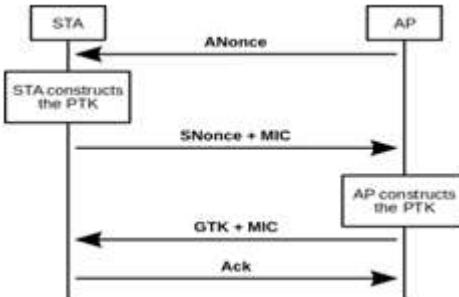


Fig 4: Four-way handshake process [3]

PTK=PRF[
PMK+Anonce+Snonce+MAC(A)+MAC(S)]
Here PRF is a pseudorandom function.

Vulnerabilities of WPA2

Though WPA2 has bridled major vulnerabilities with WEP and WPA, WPA2 still has drawbacks.. WPA2 requires a higher amount of processing power compared to WPA. So, WPA2 cannot be implemented in legacy devices. The major disadvantage is with the four-way handshake which can be heard by using KRACK(Key Reinstallation Attacks) attack. The attacker captures the 4-way handshake and hashed values of messages are decoded which clearly provides required devices information. The WPA2-personal passphrase is cracked performing brute-force-attacks and the rogue user tries to guess the password. WPA2 devices are prone to dictionary attacks. Another point of concern is, if cracked, the attacker can even access the data before cracking also i.e., forward secrecy is not being maintained. The same is being observed with WPA2-Enterprise which uses a pre-shared key. Also, WPA2 did not provide any solution to spoofed access points. WPA2 did not meet the security requirements of Open Wi-Fi and smart devices (IoT devices).

IV. Wi-Fi Protected ACCESS-3(WPA-3)

It has known that the previous generation WPA-2(IEEE 802.11i) is not secured though its cryptography is efficient (with AES encryption) its flawed in 4- way handshake. With a single crack, we can crack all other keys, which, means it maintains no Forward Secrecy (FS). Wi-Fi Alliance has released WPA-3 after it has seen WPA-2 as the flawed version. WPA-3 gives us indefectible protection against brute-force attacks. The protection allows for only one change to crack password [6]. Its available in 2 forms:

- WPA3-Personal: It replaces PSK with Simultaneous Authentication of Equals(SAE), improves protections against attacks, including message forging, key recovery.
- WPA3 Enterprise: It provides authentication and uses link- layer encryption.

WPA3 can be read in another way, which covers 4 enhancements: OWE/Enhanced Open, SAE/WPA3-Personal, 192-bit security/WPA3-Enterprise, DPP/Easy Connect. However, to understand all these constituents, it is required to have basic cryptographic foundations especially, the Diffe-Hellman key generation(Man In The Middle will no be able to generate common secret key). It is used in SSH,TLS, IPSec and now in OWE, WPA3, DPP. The keys generated (common secret) can be deleted from both side parties, Forward Secrecy(FS) is maintained, so the recorded messages can't be decrypted in the future which is possible in WPA2. The above-mentioned protocols are described below.

OWE/ Enhanced Open

Enhanced Open is a new security for public networks. OWE stands for opportunistic wireless encryption, which is basis for enhanced open. Authentication is not provided by enhanced open. OWE is defined in the Internet Engineering Task Force (IETF) RFC8110 specification. This users of this protocol has benefits as data encryption in open networks, and even network providers has benefits as there are no passphrases which are public to be maintained and shared [7].

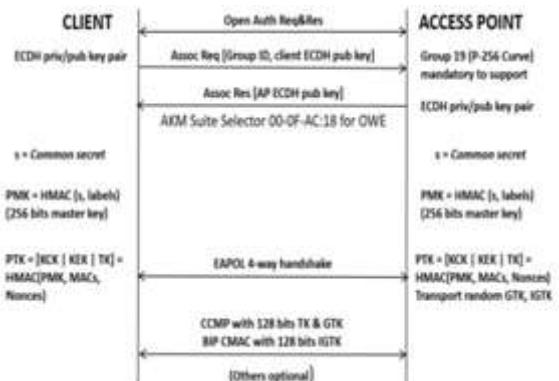


Fig 5: OWE message flow [10]

The priv, s, PMK, PTK, KCK, KEK, TK, PTK are private keys which are not open to all. The actual message flow contains 2 messages. The client sends an association request as the first message which includes Group ID(the scheme used FFC/ECC the Diffe-Hellman schemes) and the public key generated on the client-side. The AP also does the

same by sending Association response as the second message, then the common secret is generated. The Unique key will be assigned to each client for each session. There is no authentication provided. The key s is used to derive PMK(Pairwise Master Key). Later using this generated PMK, EAPOL 4-way handshake takes place, during which KCK(key for integrity protection), KEK(key for transporting Group Transport Keys GTKs), TK(the Encryption key). The CCMP protocol uses these keys for the encryption of data, data confidentiality & integrity which occurs the same as in WPA-2, except the PMK generated here is not transported between 2 parties over the air. We can say OWE is a direct application of ECDH(Elliptical Curve Diffe-Hellman).

Even though authentication is absent the encryption is better (in HTTP browsing) than not. Since there is no Access Point authentication, the Honey pot/ Evil twin threat is not solved by OWE.

SAE/ WPA3-Personal

Simultaneous Authentication of Equals is an secure authentication method based on password[8]. It is another form of Dragonfly Key Exchange(DKE), which is defined in RFC 7664. DKE is based on Diffe-Hellman Key Exchange using finite cyclic groups. The primary or elliptical curve are some such groups[8].

It's aim is using MAC address and a password authenticate a client. After connection an exchange of this protocol happens. For a successful connection both client and AP generate keys which are cryptographic in nature from which all session keys are derived. So cracking a session key doesn't affect other session, unlike WPA-2[9].

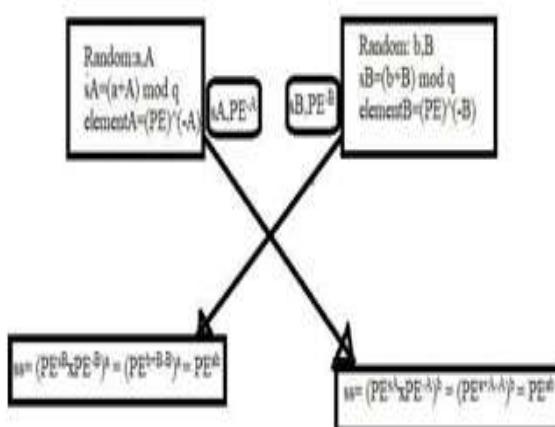


Fig 6: Dragon-Fly Protocol- Commit Phase [6]

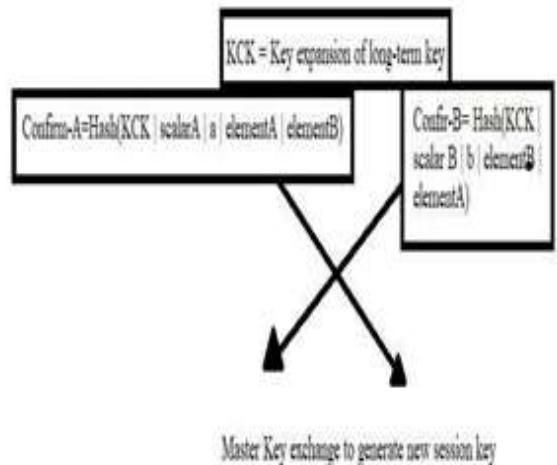


Fig 7: Confirmation Phase[6]

```
Implementation of DRAGONFLY method:
import hashlib
import random
import sys
import libnum

q=131
text="Hello"

a=random.randint(1,1000)
b=random.randint(1,1000)
c=random.randint(1,1000)
d=random.randint(1,1000)

sa=a + a
sb=b + b

PE = int(hashlib.md5(text.encode()).hexdigest(), 16)

elementA = libnum.invmod(pow(PE,a),q)
elementB = libnum.invmod(pow(PE,b),q)

PEa = pow(PE,sa,q)
PEb = pow(PE,sb,q)

print("password:",text)
print("Client generates two random values")
print("a:\\" ,a)
print("A:\\" ,A)
print("b:\\" ,b)
print("B:\\" ,B)

print("Client calculates elements")
print("Element A:",elementA)
print("AP calculates elementB")
print("Element B:",elementB)

sa1 = pow(PEa, * elementA,b,q)
sb1 = pow(PEb, * elementB,a,q)

print("They exchange values and calculate a secret share")
print("Client share:\\" ,sa1)
print("AP share:\\" ,sb1)
```

Fig 8: Implementation of Dragon fly in Python3[6]

```
1 Password: hello
2 Client generates two random values
3 a: 692
4 A: 46
5
6 AP generates two random values
7 b: 513
8 B: 632
9
10 Client calculates elementA
11 Element A: 94
12
13 AP calculates elementB
14 Element B: 58
15
16 They exchange values and calculate a secret share
17
18 Client share: 105
19 AP share: 105
```

Fig 9: Sample Output

The only difference is the value of public parameter ‘g’(in Diffe-Hellman scheme) based on password and MAC, which is known as PWE, but the value of another public parameter ‘p’ is still taken from the standard set. If we observe the same process takes place even in OWE, except that the parameters both are derived from the standard set. Now the Diffe-Hellman scheme generates a new PMK. This is integrated into 802.11 messaging as follows:

The initial 802.11 messaging in OWE has only 2 messages i.e., request and response, that count in SAE have gone to 4. To support this key exchange the new Algorithm with number 3 is introduced. The client sends the initial message “Authentication Commit” which includes the GroupID of ECDH, it’s public key with algorithm number 3. Any eaves dropper cannot see that private key. In the process, the actual authentication happened and PMK is generated through Diffe- Hellman generation. Then it performs the standard association request/response using special Authentication Key

Management(AKM)[11]

When we use SAE either password or any derived information is found in communication channel. So attacker cannot steal any authentication information. But the threat of Online Dictionary attack is still not deterred and prevented by SAE because anyone can make a guess of password for many times to connect. The only measure is limit the rate of attempt, give alerts for failed attempts.

192-bit Security/ WPA3-Enterprise

This provides better protection for enterprise data using large number of bits security protocols.

The aim is to offer security for the entire protocol stack, which includes hand-shakes and ciphers.

The 192-bit security mode ensures the right combination of cryptographic tools are used for security within a WPA3 network[7]. Government offices, and institutions have greater security with WPA3-Enterprise.

This new security is based on ‘Suit-B’ instructions of NSA.[12].

Though the paper does not discuss this scheme in detail but it is enough to say that this scheme highly increases the network security.

DPP/ Easy connect

Easy connect defines Device Provisioning Protocol(DPP). It defines a secure method for Wi-Fi

devices to join a network without knowledge of authentication details such as password.

It is designed for various devices which don’t have keyboard, screens, UIs etc, but we can securely configure them to join Wi-Fi. WFA has defined two roles: Configurator (the device that makes the configuration) and Enrollee(IoT device, smart appliances, APs and others that get configured to join secure Wi-Fi).

A network operator chooses a device with rich UI as a configurator which is also the central point of configuration. This device should be capable of scanning a Quick Response code and running the DPP. All other devices are enrollees. Since public action frames were used for authentication messages, so existing access points can be used by devices.

DPP progresses in three phases: Authentication, Configuration, Network Access. All the security principles in these 3 phases are based on Discrete Logarithmic Problem, which is used in Diff-Hellman Key Generation.

1. Authentication

DPP authentication protocol is used in this phase. The configurator reads the QR associated with Enrollee which contains ECDH static public key, MAC Address, configuration channels, Serial Number. The Enrollee holds the private key corresponding to the static public key, this key shouldn’t be disclosed.

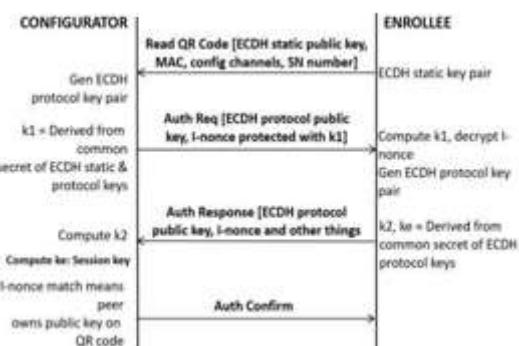


Fig 11: DPP AUTHENTICATION PROTOCOL

Apart from mentioned Out Of band(OOB) bootstrapping method with QR code, we can also employ the in-band method using PKEK.

2. Configuration

DPP configuration protocol is used in this phase. After Authentication phase, the Enrollee requests for its configuration details to connect, the configurator responds with configuration object which may contain WPA2-PSK to connect WPA2

network or SAE(password) to connect to WPA3 network. These two configuration request and response messages are protected by the session key generated in the previous phase.

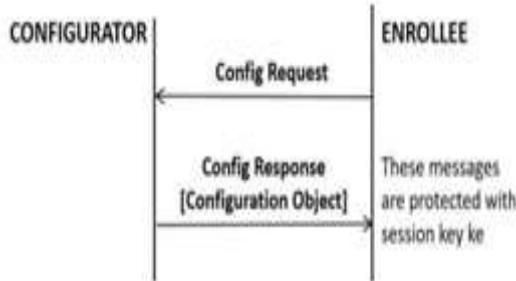


Fig 12: DPP configuration protocol

3. Network Access with Connector

Firstly the enrollee sends the peer discovery request with it's a connector to AP, then the AP verifies the connector against its own and sends back the peer discovery response with its connector, so the enrollee can validate that it has been done by the same configurator. Then they get the Diffe-Hellman key and the rest process is familiar.

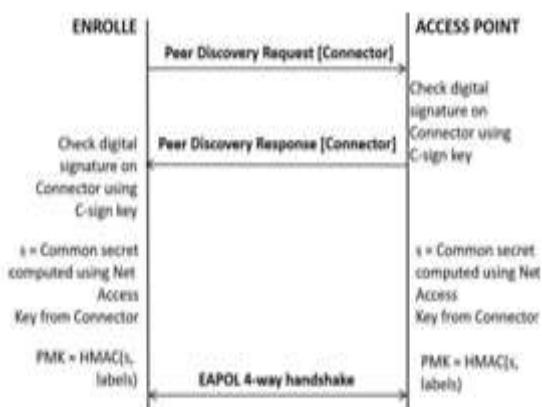


Fig 13: Network access connector

V. Security Evaluation and Analysis of WPA-3

Some of the vulnerabilities are presented in this section. The ability of WPA3 to solve the problem is also tabulated and discussed.

Attack	Solved by WPA3
Deauthentication	Yes
Handshake Capture Dictionary Attack	Yes
PMKID Hash Dictionary Attack	Yes
Rogue Access Point	Partially
Evil Twin Attack	No
Handshake Capture En/Decryption	Yes
KRACK Exploit	Yes
ARP Spoofing	Partially
SSL Stripping	No
DNS Spoofing	NO

Table 2: WPA3-security evaluation

We will go through the 2 of the above-mentioned attacks in analytical fashion and determine the capability of WPA3 in mitigating that attack.

1. KRACK Exploit

This attack is based on the loophole in four-way handshake mechanism of resending the 3rd message.

Let us assume that any attacker after capturing a session gets succeeded in request for resend of 3rd message from AP, and reset the key stream then he may decrypt that session data but not the previous which maintains the forward secrecy. But a router supporting WPA3 can be configured to prohibit this retransmission of messages which makes this attack not feasible.

2. DNS Spoofing

If an attacker obtains access and can place himself between client and Access Point, the protection is compromised. Here in this attack the attacker places himself between a client and Domain Name Server.

When a client sends the HTTPS requests, a Man in the Middle(MITM) attacker can change those requests to HTTP form and redirect to target Server, and then he has access to the returned page from server. So now the Secure Sockets Layer encryption cannot protect data entered by client. The client here doesn't suspect the server and it's response, this

makes the attack possible. This is not solved by WPA3.

VI. Discussions

The Wi-Fi security requires wholesome tools and implementations to maintain user data privacy. Through WPA3, WFA brought new capabilities that support the way the world works today. Enabling user data protection for personal network increase Wi-Fi user experience and dependence on Wi-Fi.

WPA3 built upon WPA2 to bring a next level of security for both personal and enterprise network environments with efficient security protocols. Focus on cryptographic consistency, password-based authentication, and 192-bit security escort the market into the next age of connectivity. Based on the analysis done till this point, below table is built.

FEATURES	WPA2	WPA3
ENCRYPTION	WPA2 uses the AES standard.	AES-GCM encryption & Elliptical Curve Cryptography of CNSA Suit B.
SESSION KEY SIZE	128-bit	192-bit
HANDSHAKE PROTOCOL	PSK exchange protocol	SAE(Dragon Key Exchange) with Forward Secrecy feature.
WIRELESS CONNECTION PROTOCOL	Wi-Fi Protected Setup (WPS)-vulnerable	Wi-Fi Easy Connect using Device Provisioning Protocol (DPP)-Secure
VULNERABLE TO KRACK ATTACKS	Yes	No, due to SAE key exchange.
VULNERABLE TO DNS SPOOFING	Yes	Yes

Table 3: Comparison of WPA2 and WPA3

The availability of some of features of WPA3 is abundant. Android 10 introduces support for Wi-Fi Enhanced Open standards[14]. WFA proposed two transition modes for this: WPA2/WPA3 transition mode, OWE transition mode. Android 10 also introduces support for DPP [13]. WPS was deprecated in Android 9. Android 10 supports WPA-3 Easy Connect only in initiator mode, it doesn't support responder mode.

VII. Conclusions

WPA-3 is the new generation of Wi-Fi security protocols. In this paper, we discussed by briefing about Wi-Fi Equivalent Privacy (WEP), Wi-Fi Protected Access(WPA), the earlier generations of Wi-Fi Security protocols. The paper in later sections covered the WPA-2 protocol, its mechanism along with the faults in the protocol. The WPA-3 protocol is highlighted by discussing in detail about it, mentioning the functions, its enhancements. This paper also covered some Dragon Fly key generation technique, 4-Way handshake Key exchange technique to understand the protocols working. In the end, some security analysis has been done to test the capability of WPA-3 in theory. This scheme addressed many of the issues present in WPA2, which includes off-line dictionary attacks, de-authentication and the KRACK vulnerability, but still it did not solve some of the major vulnerabilities in Wi-Fi networks. This paper discusses the present status of WPA-3 in an organized manner.

VIII. Acknowledgment

The authors gratefully acknowledge the contribution and provisions of Vasavi College of Engineering to the paper.

References

- [1] Gray A. Donabue, Network Warrior, 2nd ed., Page no.515.
- [2] A.H. Adnan et al., "A comparative study of WLAN security protocols: WPA, WPA2," 2015 International Conference on Advances in Electrical Engineering (ICAEE), Dhaka, 2015, Page no.165-169 July 2016.
- [3] Wikipedia.2020."IEEE 802.11i-2004" April 5, 2020. Available: https://en.wikipedia.org/wiki/IEEE_802.11i-2004
- [4] M. A. Abo-Soliman and M. A. Azer, "A study in WPA2 enterprise recent attacks," 2017 13th International Computer Engineering Conference (ICENCO), Cairo, 2017, Page no. 323-330 February 2018.
- [5] D. Harkins, "Simultaneous Authentication of Equals: A Secure, Password-Based Key Exchange for Mesh Networks," 2008 Second International Conference on Sensor Technologies and Applications (sensorcomm 2008), Page no. 839-844 September 2008.
- [6] Prof. William Buchanan, "Dragonfly Protocol - Zero Knowledge Proof ".Available: <https://asecuritysite.com/encryption/dragonfly>
- [7] Discovery-Wi-Fi/Security,"<https://www.wi-fi.org/discover-wi-fi/security>".
- [8] Harkins, Dan (Aug 20, 2008). "Simultaneous Authentication of Equals: A Secure, Password-Based Key Exchange for Mesh Networks". 2008 Second International Conference on Sensor Technologies and Applications (Sensorcomm 2008).ISBN 978-0-7695-3330-8 – via IEEE Xplore
- [9] Prof. William Buchanan, "How a Dragonfly aims to fix Delicate Wi-Fi Wings"<https://medium.com>

- /asecuritysite-when-bob-met-alice/how-a-dragonfly-aims-to-fix-delicate-wi-fis-wings-f26d82798010
- [10] Hemanth Chaskar, Hewlett Packard Enterprise Company, https://d2cpnw0u24fjm4.cloudfront.net/wp-content/uploads/WLPC_2019_WPA3-OWE-AND-DDP_Hemanth-Chaskar.pdf
- [11] IEEE P802.11s/D1.07, September 2007, https://www.cise.ufl.edu/~nemo/tmp/Draft_P802.11s_D1.07.pdf
- [12] Pablo Nogueri, WPA-3:Improved Wi-Security, <https://www.teldat.com/blog/en/wpa3-wi-fi-network-security-wpa3-personal-wpa3-enterprise/>
- [13] Wi-Fi Easy Connect, Android Open Source Project <https://source.android.com/devices/tech/connect/wifi-easy-connect>
- [14] WPA3 and Enhanced Open, Android Open Source Project, <https://source.android.com/devices/tech/connect/wifi-wpa3-owe>

The Deep Learning Algorithm for Animal Detection

Thirupathi Battu

Research Scholar

Department of CSE

Osmania University

Hyderabad-500007, India

battuhruday@gmail.com

Dr.D.Lakshmi Sreenivasa Reddy

Associate Professor

Department of IT

Chaitanya Bharathi Institute of Technology

Hyderabad-500075, India

dlsrinivasreddy_it@gmail.com

Thatikonda Soma Shekar

Research Scholar

Department of CSE

Osmania University

Hyderabad-500007, India

soma.ts@gmail.com

Abstract: It is essential to inspect wild animals in their natural habitat. This project aims to create a wild animal detection algorithm. Manually identifying species can be difficult due to a large number of individuals. This algorithm categorizes animals based on their images, allowing us to keep a closer eye on them. Pet identification and classification, as well as tracking and theft, can help avoid animal-vehicle collisions. This is possible thanks to the use of advanced deep learning algorithms.

Keywords: Deep Learning Algorithms. Classification, Animal Detection.

I. Introduction

Machine learning is a form of artificial intelligence that allows computers to learn and improve without having to be programmed. The method of designing computer programmes that can access data and learn on their own is known as machine learning. In order to make informed decisions in the future, the learning process begins with an interpretation of data, such as examples, previous models, or recommendations. The main aim is for computers to self-train and learn from their errors without requiring human intervention..

Convolutional Neural Networks(CNN) is a form of deep neural network that can be used to analyze visual images. Deep neural networks are a group of algorithms that have been used to precisely place new records for a variety of problems. In comparison to other image classification algorithms, CNNs need very little preprocessing. The benefit of convolutional neural networks is that they don't need any prior experience or human involvement in feature design (CNN). Video and Image recognition, image identification, recommendation systems, medical image processing are only a few of the areas where they're used.

Ecosystem science includes studying wild animals in their natural environment. Excessive resource use is causing rapid, innovative, and important changes in the Earth's ecosystems due to the enormous increase in human population and economic development..

Human activity has impacted natural life populations, habitat, and behavior in an increasing region of the land surface. More tragically, many wild animals have become extinct, and many species have been reintroduced to new areas where they can deplete human resources.

II. Literature Survey

Animal detection systems are designed to prevent injuries caused by collisions with animal vehicles. This results in death, injury, and property damage. Animal detection systems are designed to avoid collisions caused by animal vehicles. This results in death, disability, and property damage.

A. Template Matching Algorithm for Animal Detection

This paper proposes reviews of various object detection algorithms. The proposed system is effective and a minimal number of false positives and negatives.

B. Using deep learning to recognize, count, and describe wild animals in camera trap photos

In this research, deep learning is used to predict the location and behaviors of wild animals. The ability to collect camera trap image data involuntarily and reliably, as well as a motion sensor for monitoring wildlife movements, are discussed in this paper. Extracting data from these images, on the other hand, remains a time-consuming and physically challenging process. It's worth noting that deep

learning can be used to retrieve such data automatically.

A Deep convolutional neural network was trained to identify, count, and explain the behaviours of 48 breeds out of the 3.2 million breeds in the Snapshot Serengeti data set. The network would automatically recognise animals with a 93.8 percent accuracy. Furthermore, if the system only classifies self-assured images, 99.3 percent of the data is automatically identified as an animal. However, the precision is still 96.6 percent, saving 3.2 million photos for more than 8.4 years (over 17,000 hours). This finding emphasizes the importance of using deep neural networks to extract data from camera trap images. The results of this study indicate that this technology can be used to gather data in many animals' natural environments in a cost-effective, meaningful, and real-time manner.

Block Diagram

A. Convolutional Neural Network

A Convolutional neural network (CNN) is a form of artificial neural network that processes large amounts of data using a perceptron. CNN's can help with image recognition, natural language processing (NLP), and any other cognitive feature. A convolutional neural network is made up of an input layer, an output layer, and several hidden layers (CNN). A few of these layers have been transformed into subsequent layers using mathematical models.

- Raw pixel values for the red(R), green(G), and blue color channels will be present in the input image (B).
- The next layer, CONV, is given a name. In local areas, this layer tests the neuron output connected to the input layer. Each one measures a point where the weight and a remote location related to the input layer intersect.
- The wise unit activation function is applied to the RELU layer, which is the third layer. This has no bearing on the volume size.
- The POOL layer is the next layer, which performs spatial dimension (width and height) sampling, resulting in sizes like [16x16x12].
- The FC layer is the last layer (i.e., fully connected), and it calculates the class scores, which results in the size amount. Every neuron in this layer is linked to all weights in the previous series, just like traditional neural networks.

B. Convolutional Layer

As shown in Figure 1, a convolutional layer extracts features from an input image. Convolution maintains the relationship between pixels by learning

image features from small squares of input image data. This mathematical technique uses two inputs, such as an image matrix and a filter. Edge detection, blurring, and sharpening can all be done by convolution image data with different filters.

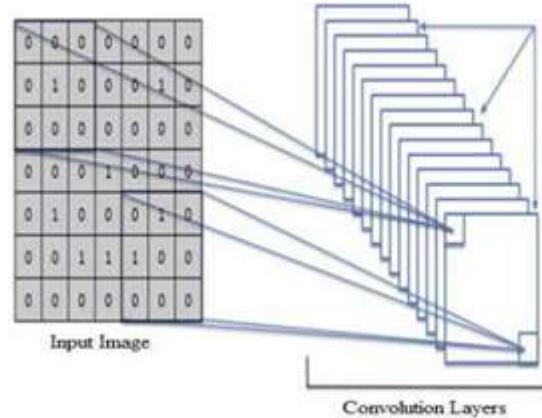


Fig 1: Convolutional Layer

C. Pooling

A pooling layer can minimize the number of parameters when a large image is used as input. For maximum pooling, the largest element from the revised function map is used. The aim of max pooling is to reduce the size of an input image by downsampling it. Figure 2 illustrates this.

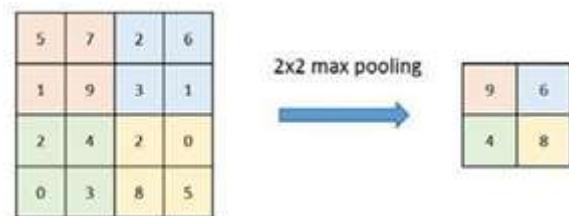


Fig 2: Pooling Layer

D. Flattening

Flattening is the process of converting a two-dimensional array into a single long and continuous linear vector. It took the convolutional layers' contribution and flattened it so that it could construct the next layer for the final classification with a single, long feature vector. Figure 3 illustrates this..

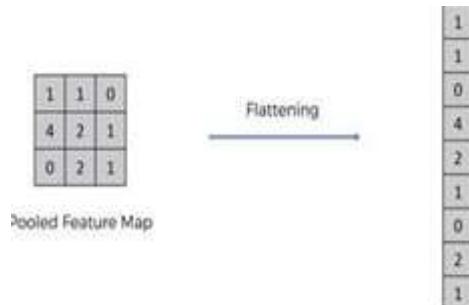


Fig 3: Flattening Layer

E. Fully connected

Figure 4 depicts the fully linked layers, which are hidden layers within a pioneering neural network. This is a specific form of a hidden layer that can be found in the CNN. This is used to merge features into more attributes that forecast outputs more precisely.

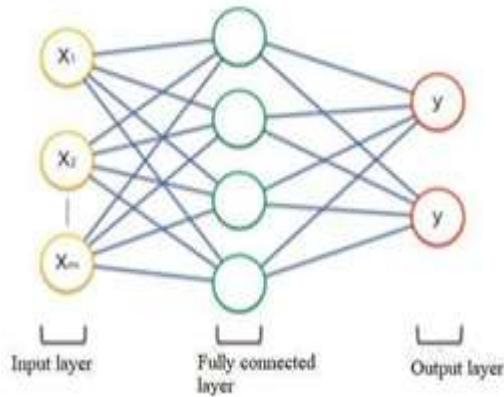
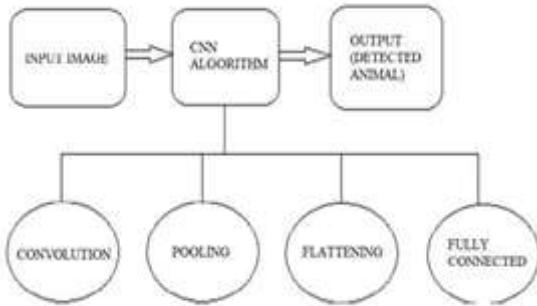


Fig 4: Fully Connected Layer



The block diagram of the deep learning algorithm for animal detection is shown in Figure 5.

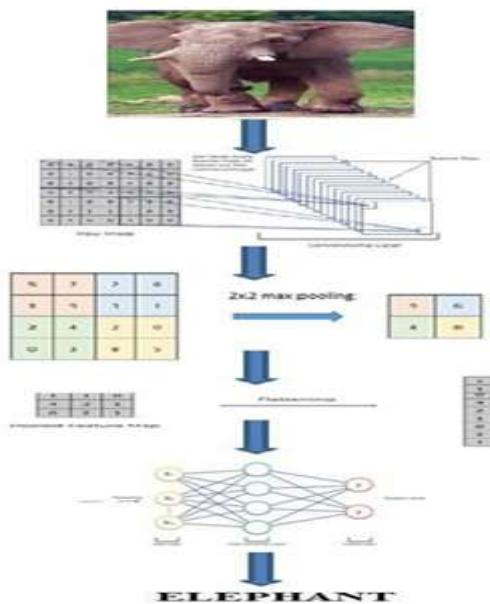


Fig 6: shows the flow diagram of animal detection

III. Dataset

A. Train Dataset Elephant Train Dataset

The dataset in question is a list of image data that includes a variety of animal photographs. The dataset is divided into two parts: train and test, with a 75:25 split.



Fig 7: Elephant Train Dataset



Fig 8: Cheetah Train Dataset

B. Test dataset Elephant Test Dataset



Fig 9: Elephant Test Dataset

Cheetah Test Dataset



Fig 10: Cheetah Test Dataset

IV. Result

A. Detection of Elephant

```

Epoch 1/5
2/2 [=====] - 5s 210ms/step - loss: 0.2051 - acc: 0.9881 - val_loss: 0.1879 - val_acc: 0.9879
Epoch 2/5
2/2 [=====] - 5s 210ms/step - loss: 0.0735 - acc: 0.9940 - val_loss: 0.7344 - val_acc: 0.9389
Epoch 3/5
2/2 [=====] - 5s 210ms/step - loss: 0.0239 - acc: 0.9984 - val_loss: 1.0609 - val_acc: 0.9423
Epoch 4/5
2/2 [=====] - 5s 210ms/step - loss: 0.0239 - acc: 0.9989 - val_loss: 1.7209 - val_acc: 0.9495
Epoch 5/5
2/2 [=====] - 5s 210ms/step - loss: 0.0245 - acc: 0.9997 - val_loss: 1.1048 - val_acc: 0.9721

```

Fig 11: Accuracy of Detected Elephant



Fig 12: Detected Elephant

B. Detection ofCheetah

```

Epoch 1/5
2/2 [=====] - 5s 210ms/step - loss: 0.2051 - acc: 0.9881 - val_loss: 0.1879 - val_acc: 0.9879
Epoch 2/5
2/2 [=====] - 5s 210ms/step - loss: 0.0735 - acc: 0.9940 - val_loss: 0.7344 - val_acc: 0.9389
Epoch 3/5
2/2 [=====] - 5s 210ms/step - loss: 0.0239 - acc: 0.9984 - val_loss: 1.0609 - val_acc: 0.9423
Epoch 4/5
2/2 [=====] - 5s 210ms/step - loss: 0.0239 - acc: 0.9989 - val_loss: 1.7209 - val_acc: 0.9495
Epoch 5/5
2/2 [=====] - 5s 210ms/step - loss: 0.0245 - acc: 0.9997 - val_loss: 1.1048 - val_acc: 0.9721

```

Fig 13: Accuracy of Detected Cheetali

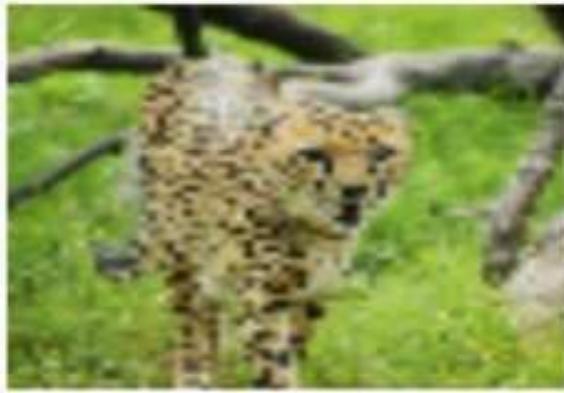


Fig 14: Detected of Cheetali

V. Conclusion

To detect wild animals, this project employs the Convolutional Neural Network (CNN) algorithm. The algorithm successfully classifies animals with a high degree of precision. It also produces results that can be used for other purposes, such as identifying wild animals that have developed a human habit, preventing wildlife poaching, and even preventing human-animal conflict.

VI. Future Scope

When the animal is identified, this function can be further enhanced by sending a message to the local forest office as a warning. It may also be used to reduce tension between humans and animals, as well as animal accidents.

Reference

- [1] Burghardt, T., Calic, J.: Real-time face detection and tracking of animals. In: Neural Network Applications in Electrical Engineering. pp. 27[32]. IEEE(2006).
- [2] Felzenszwalb, P.F., Girshick, R.B., McAllester, D., Ramanan, D.: Object detection with discriminatively trained part-based models. IEEE TPAMI 32(9),1627-1645(2010).
- [3] He, K., Zhang, X., Ren, S., Sun, J.: Deep residual learning for image recognition. In: CVPR. pp. 770-778(2016).
- [4] Kamencay, P., T. Trnovszky, M. Benco, R. Hudec, P. Sykora and A. Satnik. Accurate wild animal recognition using PCA, LDA and LBPH, In: 2016 ELEKTRO. StrbskePleso: IEEE, 2016, pp.62–67.
- [5] WU, J. L. and W. Y. MA. A Deep Learning Framework for Coreference Resolution Basedon Convolutional Neural Network. In: 2017 IEEE 11th International Conference on Semantic Computing (ICSC). San Diego: IEEE, 2017, pp.61–64.
- [6] P.M. Vitousek, H.A. Mooney, J. Lubchenco, J. Melillo, "Human domination of Earth's ecosystems", Science, vol. 277, no. 5325, pp. 494-499, 1997. (ICSC). San Diego: IEEE, 2017, pp.61–64.
- [7] G.C.White,R.A.Garrott,AnalysisofWildliferadio-trackingdata, Elsiever,2012.
- [8] B.J. Godley, J. Blumenthal, A. Broderick, M. Coyne, M. Godfrey, L. Hawkes, M. Witt, "Satellite tracking of sea turtles: Where have we been and where do we go next?", Endangered Species Research, vol.4, no.1-2,pp.3-22,2008.
- [9] Gomez., A. Salazar, F. Vargas, towards automatic wild animal monitoring: Identification of animal species in camera-trap images using very deep convolutional neural networks,2016
- [10] WU, J. L. and W. Y. MA. A Deep Learning Framework for Coreference Resolution Basedon Convolutional Neural Network. In: 2017 IEEE 11th International Conference on Semantic Computing (ICSC). San Diego: IEEE, 2017, pp.61–64.
- [11] P.M. Vitousek, H.A. Mooney, J.Lubchenco, J. Melillo, "Human domination of Earth's ecosystems", Science, vol. 277, no. 5325, pp. 494-499, 1997. (ICSC). San Diego: IEEE, 2017, pp.61–64.
- [12] G.C.White,R.A.Garrott,AnalysisofWildliferadio-trackingdata,Elsiever,2012.
- [13] B.J. Godley, J. Blumenthal, A. Broderick, M. Coyne, M. Godfrey, L. Hawkes, M. Witt, "Satellite tracking of sea turtles: Where have we been and where do we go next?", Endangered Species Research, vol.4, no.1-2,pp.3-22,2008.
- [14] A. Gomez., A. Salazar, F. Vargas, towards automatic wild animal monitoring: Identification of animal species in camera-trap images using very deep convolutional neural network,2016

Smart Farming using IOT and Machine Learning

Sandeep Kalari

Student of MCA final year,

Department of MCA

Chaitanya Bharathi Institute of Technology(A)
Gandipet, Hyderabad, Telangana-500075, India.

sandeepkalari14@gmail.com.

Dr.B.Indira

Assint. Professror,

Department of MCA

Chaitanya Bharathi Institute of Technology(A)
Gandipet, Hyderabad, Telangana-500075, India.

bindira_mca@cbit.ac.in.

Abstract: We are living in a world of digitization, where technology plays an important role in all real-world applications. The role of Technology in the agriculture sector is increasing day by day. Technology played a crucial role in replacing the conventional mode of agricultural practices. However, the agriculture sector is witnessing a lot of problems and has affected production capacity. To overcome this, recently hydroponics is introduced. The limitation in this type of environment is to maintain the temperature, water level, sunlight, PH, and humidity values at a specific level. Manual monitoring is a very complex task and if they are not monitored and maintained properly the plants may die or yield less production. Our work is to guide farmers in efficient harvesting with the help of technology. For this purpose, we propose an easily accessible IOT (Internet of Things) based monitoring and wireless controlled system. Through this IOT system, farmers can irrigate their crops by the usage of water level management, sunlight monitoring, and temperature values and ensure that every plant gets sufficient water and sunlight. IOT is used to transfer the retrieved data from various sensors like temperature sensor, water level sensors to the mass storage via the cloud, and a mobile app is used to communicate the current status to the user by using Twilio, Mail gun API's and Telegram- chat bot so that monitoring and maintenance will be easier and appropriate actions can be taken automatically to maintain the various parameters like temperature, water level, and sunlight.

Keywords: Bolt-IOT module, bolt-cloud, Machine Learning, Twilio, Mail gun, telegram-bot, Temperature sensor, Water level sensor, Buzzer, LED light, VM Virtual Box, Ubuntu, Python3.

I. Introduction

Currently in agriculture sector the main problem is insects that eat plants and simultaneously effecting plants with diseases. Because of this problem, farmers have no other option but to use pesticides. The chemical fertilizers are killing bacteria and insects that are effecting plants. These hazardous chemical fertilizers are causing adverse effects. Simultaneously, it is affecting the health of consumers who are consuming those farm products.

Other, major problem in today's conventional farming is losing its share of land due to urbanization. On the other hand, day by day the population is increasing and the quality of food products is decreasing. So, to face all these challenges hydroponics system is the best solution in the current situation. Hydroponics refers to the art of growing plants in water without soil. Nutrients for the plants are supplied to the roots in the form of a solution that can be supplied either manually or automatically by using the Bolt-IOT device and Machine learning algorithms. Hydroponics can be cultivated both in greenhouse and glasshouse environments[3].



Fig 1: Sample Images for hydroponics Environment [10].

But in this type of setup, there is a big threat to the whole system failure or when plants do not get sufficient natural resources like sunlight, water, nutrients, and temperature which in turn will affect, quality of the vegetables or fruits. Manually it is hard to maintain this complex setup. So, by using IOT and machine learning technologies, we can create a fully automated environment that will constantly monitor the flow of water, minerals in the water, temperature of indoor system etc., and we can also maintain

security with the help of this IOT setup. Finally, this will continuously monitor the whole system, if there is any problem with these readings, immediately IOT based system will notify the farmer with the alert messages. This customized app is used to see all the information that is provided by sensors and the same can be displayed in that app. User can check that mobile app for the information. The data that is sent by the sensors will be stored in the cloud and that will analyze data to send alert messages. If any anomaly occurs in the data, API like mail gun is used for sending mail and Twilio is used for sending SMS messages. In addition to that by creating a messaging bot and channel in telegram messaging app, it will make easy for a big number of stakeholders to join that group and to get notified whenever there is an alert message.

II. Literature Review

In this literature review we will discuss about how hydroponics can be implemented by using IOT in various approaches:

Monitoring air quality of indoor hydroponics like carbon dioxide, carbon monoxide by using a gas sensor including bolt IOT devices and also how to improve the air quality for the good health of students? Is presented in the study by Pallavi et al. [1].

The research of Dania Eridani et al. [2] design and application with Arduino based of automatic NFT (nutrient film technique) in hydroponics with the help of TDS (Total dissolved solid) sensor. This system can maintain a level of nutrients at all the time if decrease in nutrient level it will automatically add the nutrients in the water.

Hydroponics is all about sending nutrients to plants. How this part is done? Why it is so important in an indoor hydroponic system? Is explained in [3] by Dr.D.Saraswathi et al. which is called an indoor nutrient film technique.

In current research Chris Jordan G. Aliac et al. [4] used raspberry pi, analog to digital converter (ADR), water pump (used to control the inflow of the system) and firebase real time database for implementation of hydroponic system.

Power saving by using smart pumping of water whenever roots are dry then water has to pump to the roots with combination of nutrients. This automatically saves the water and electricity is proposed by a Carlos Ramos et al. [5] research.

This hydroponics system includes a huge amount of investment. To protect this type of system from intruders is also equally important. By using

face recognition machine algorithm if that face does not match to the database immediately send a message to mobile. This kind of research is developed by himanshu et al. [6]

Fuangthong Mathawee and Part Pramokchon states that fuzzy logic control is used in the decision-making process of pH and EC(Electrical Conductivity). Their experiment adjusts the EC and PH level to optimum range of green oaks and this fuzzy logic better control the adding nutrients to plants [7].

Herman and Nico Surantha [9] presented the experiments done with lettuce and bok choy plant that grows with fuzzy logic and nutrient supply. It has more quality compared to manual way of monitoring whole system.

III. System Overview

This whole model talks about how the system is measuring the water level and temperature values and sending them to the farmer. This process is explained in figure 2.

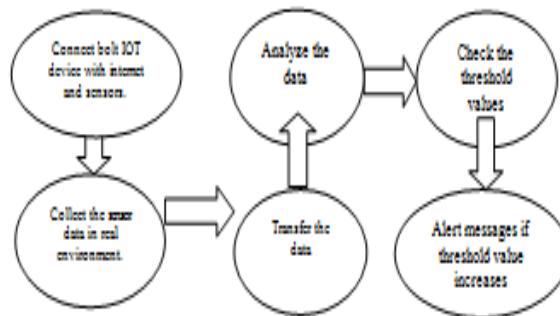


Fig 2: System design

A. Connect bolt-IOT device

Connecting bolt-IOT device to sensors and the internet or WI-FI is the first task in this model. For establishing a communication between device and sensors through internet.

B. Collect the data

Collection of data by sensors is the primary task in the current model. This data supposed to be real time environment data. For example, if we are sitting in a room and need to know the brightness it is possible know the values that sensor is sending to us.

C. Transfer the data

In step-B, sensors are continuously generating the data and it has to send that data to someplace like a cloud.

D. Analyse the data

After sending the data to cloud it has to provide some meaningful results. This data has to be analyzed in the cloud environment to get results.

E. Check the threshold values and send alert messages

In a cloud, the data will be analyzed and the results are also monitored in the cloud. By programming support like python3 and java script if any parameter value exceeds the threshold value it has to send automatic alert messages or triggers buzzer sound or switching on LED lights. Mainly, it is sending the alert messages by using protocols like Twilio, Mail gun, and telegram chat bot messages.

IV. Hardware and Software Modules

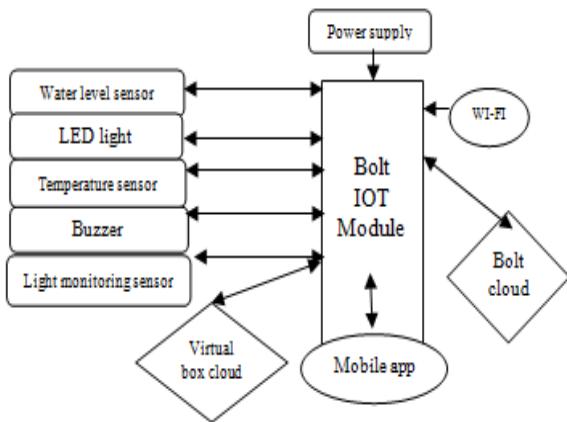


Fig 3: Architecture design.

A. Hardware module design

Bolt-IOT device should connect with a continuous power supply and an internet connection. Sensors like temperature sensor, light monitoring sensor, and water level sensor are connected to the bolt-IOT device. Buzzer and LED light can also be connected to the device which is shown in Fig. 4. So basically, the sensors are connected to the breadboard because there are multiple things to execute at once which is shown in Fig-10. Actually, the power to the sensor will be obtained from ‘A0’ that is an analog pin of the bolt-IOT. In the water level sensor, the input connection is the ‘+’ pin is for ‘3V3’ pin and ‘-’ is for ‘GND’ (ground), and ‘S’ pin is for ‘A0’ pin. Likewise, we need to connect for a temperature sensor and sunlight sensor. If sensor’s output value crosses a limit then buzzer must be triggered. Buzzer is connected to the device as follows: it’s ‘-’ pin to ‘0’ in device and ‘+’ pin to ‘GND’ pin. Here the condition to get alert and buzzer is both sensors and buzzer have to be interconnected with the help of connectors and same holds for a LED light alert.

B. Software module design

In software development for the Fig. 4 is first we use a virtual box as a cloud by using Ubuntu virtual server where execution happens by using python3 and also by using different libraries which are available in python3. We use bolt cloud for prediction purpose by using polynomial regression which is a machine learning algorithm. Prediction points are available in Fig .6 and we can monitor sunlight using the bolt-IOT mobile app as shown in Fig. 5.

Coming to the actual program, suppose the temperature value, sunlight value, and water level value records a value greater than threshold automatically it has to trigger a message to telegram as shown in Fig. 9. For this we need to create two programs: one is for specifying the configuration of bolt-IOT API key, device id, telegram chat id and telegram bot id and thresholds for the sensors. The second program is for reading the sensor value and sending alerts. For this we need to import some libraries like bolt iot, Json, requests, math, etc. Next is collection of data and analyze the data, in this process temperature sensor value which measures in Celsius degrees should be calculated by using this formula:

Temperature_value = ((seneor_value*100)/1024). [11] Because in the sensor_value variable the data will be always in analog mode which will automatically converts into digital data by ADR (Analog Digital Converter). Digital data gives 0 and 1 data values up to 0 to 2n-1 here ‘n’ value is up to 10 bit i.e., for ADR 210 – 1 the highest value is 1023. Here the digital value is in between 0 to 1023. So, we need to change that digital value according to our requirements. For example, sensor_value=334 then the approximate value of temperature value is 32 degrees Celsius. However, the water sensor and sunlight sensor values need not be modified. Also if the water level increases in the tank our buzzer will be activated and sends a message to telegram. For temperature prediction visualizer, we can write code in java script directly on bolt-IOT cloud.

Sample Algorithm for reading temperature and sending alert messages:

1. Min_temp = 30, this is minimum temperature threshold in Celsius degrees.
2. Max_temp = 50, maximum threshold value in Celsius degrees.
3. response = myboltanalogRead(pin)
4. data = json.loads(response)
5. sensor_value = int(data["value"])
6. sensor_value = get_sv('A0')
7. Temperature_value = int((seneor_value*100)/1024)

8. if Temperature_value > sensor_value or Temperature_value < sensor_value:
9. if a temperature value crosses the threshold then send alert message to telegram chat bot.

Sample Algorithm for monitoring water level alert messages:

1. Threshold_value = 750
2. response = myboltanalogRead(pin)
3. data = json.loads(response)
4. sensor_value = int(data["value"])
5. if sensor_value > Threshold_value
6. Sensor value crosses the threshold value then send an alert message to telegram chat bot

V. Output Results

In this section, we discuss the working of the project that we have done and evaluate the output results.

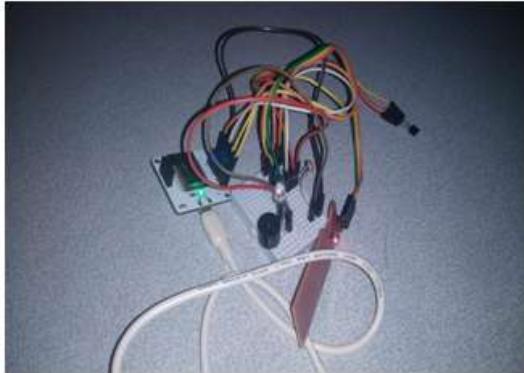


Fig 4: Hardware Connection.

Fig. 4 shows the connection of hardware which consists of a bolt-IOT device, Temperature sensor, light monitoring sensor, water level sensor, Buzzer, LED light, connectors, and breadboard.

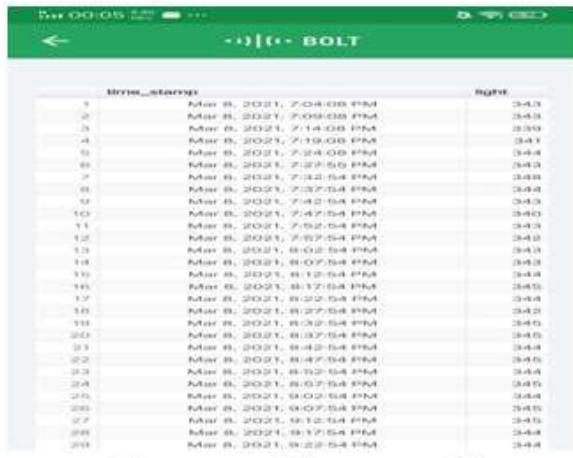


Fig 5: Light Monitoring graph.

In Fig. 5 first measure the sun light using the sensor in indoor and outdoor form and how data is received to bolt mobile app after that we will look into temperature prediction.

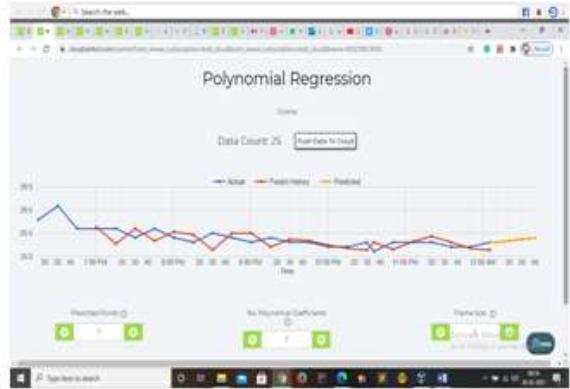


Fig 6: Machine Learning prediction Graph.

Fig 6. Describes different variables of the machine learning chart and also includes data points.

A. How Prediction points work?

The prediction point value specifies the Visualizer that, how prediction has to be done on the required number of future data points. By default, the visualizer gives the values including the data collection time in the product's hardware connection. In other words, if we fix the product to acquire the data for every 4 minutes and choose 5 prediction points, the prediction happens in the visualizer and gives output with 5 values and predicting 20 minutes of future temperature.

B. Number of Polynomial coefficients

Polynomial Visualizer processes the given input time-dependent data and gives the output as the coefficients of the function form: which most closely represents the trend in the input data. This value notifies the Visualizer how many elements should be present in the function that is the value of n. The formula for the polynomial regression algorithm is shown below [8].

$$\text{data}(t) = (C_n * t^n) + (C_{n-1} * t^{n-1}) + (C_{n-2} * t^{n-2}) + \dots + (C_1 * t^1) + C_0$$

C. Working with Frame Size

In this, the previous values are used in the visualizer prediction of the future temperature values. For instance, if we increase the value of frame size by 6, then the visualizer will use the past 6 values to predict the future course of temperature value. For this prediction 1-2 degree Celsius margin of error can be expected.



Fig 7.: Sample message from Twilio.

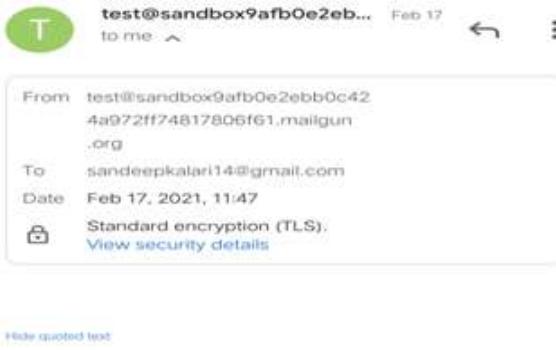


Fig 8: sample message to mail using mail gun.

Fig. 7 and 8 explains how Twilio and mail gun protocols are used in the software to send messages as text and as well as mail. Suppose if any threshold has been increased then immediately these are used to send alert messages to the users.

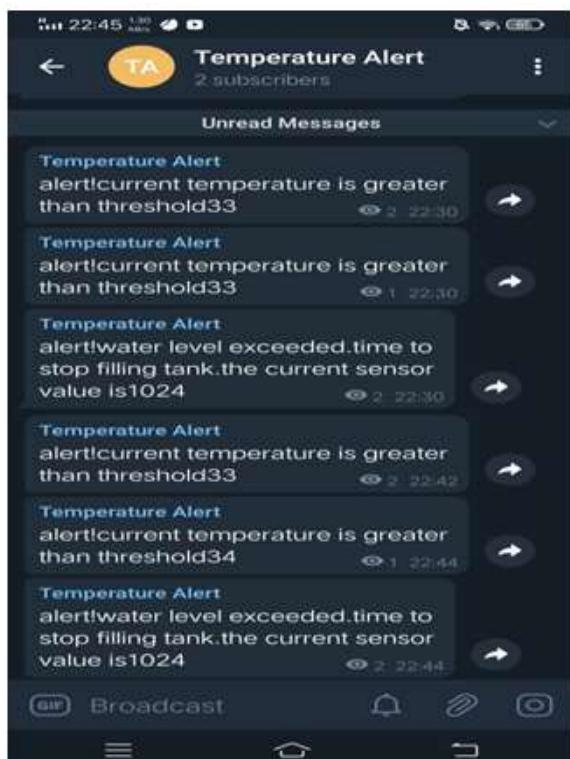


Fig 9: Telegram alert message system.

Fig. 9 shows the alert messages those are sending to the telegram chat app. This type of chat should contain their own telegram messaging bot and personal channel. In this telegram channel you can see on the above figure that alerting messages if threshold increased in temperature or water level. However, it is easy to use and also free of cost.

```
ubuntu@ubuntu:~/test$ sudo python3 water_alert.py
[sudo] password for ubuntu:
temperature value is 34
water level sensor value is 316
sun light level 359
temperature value is 34
water level sensor value is 316
sun light level 359
temperature value is 34
water level sensor value is 315
sun light level 360
temperature value is 32
water level sensor value is 1024
sun light level 349
alert!water level exceeded the threshold value
this is the telegram response
("ok":true, "result": {"message_id": 85, "sender_chat": ("IA")-100143042936, "title": "Temperature Alert", "username": "Temperature_Alert_using_int", "type": "channel"}, "chat": ("IA")-100143042936, "title": "Temperature Alert", "username": "Temperature_Alert_using_int", "type": "channel"}, "date": (161324033, "text": "alert!water level exceeded.time to stop filling tank.the current sensor value is1024"))
this is the telegram status True
```

Fig 10: Output Screen from Ubuntu server

In Figure 10, we see that the python3 program is running on Ubuntu server with the help of a virtual box cloud and if any anomaly occurs in any sensor value then the program is instructed to send the alert messages in telegram as shown in figure 8.

VI. Applications

- a. **Temperature sensor**
 - Pharmaceutical Companies.
 - Chemical Industries.
 - Hospitals.
- b. **Water level sensor**
 - Apartment water tanks.
 - Aquaponics type agriculture.
 - Water level in dams.
- c. **Light monitoring sensor**
 - Light monitoring in smart home.
 - Smart gardens.
- d. **Buzzer**
 - Fire alarm system.
 - Security alert system.

VII. Conclusion

In conclusion, hydroponics is the best method to this date, out of all other technological advancements in the agriculture sector regarding climate changes and in the production of organic food with a fast rate of output. Also, this system consumes less water, gives pesticides free environment, and occupies less geographical area. By

the proposed system we can continuously monitor the parameters like sunlight, water level and temperature. Future temperature can be predicted by using machine learning algorithms like polynomial regression and the alert text email, telegram messages are sent using Twilio, mail gun, and telegram messaging app if any value crosses the preset threshold value. On the other hand, this type of system has its own drawbacks like we can't provide exact minerals that are available in soil and it includes huge investment cost. Although, these cons don't outweigh the pros of the proposed system. Furthermore, we will make complete automation in hydroponics system by using pH sensor, humidity sensor, and minerals monitoring sensor and also for improving security we will build a laser type IOT system which can be operated by mobile app this can be maintained from anywhere in the world.

References

- [1] Pallavi Asthana, Sumita Mishra, "IoT Enabled Real Time Bolt based Indoor Air Quality Monitoring System" 2018 International Conference on Computational and Characterization Techniques in Engineering & Sciences (CCTES).
- [2] Dania Eridani, Olivia Wardhani, Eko Didik Widianto, "Designing and Implementing the Arduino-based Nutrition Feeding Automation System of a Prototype Scaled Nutrient Film Technique (NFT) Hydroponics using Total Dissolved Solids (TDS) Sensor" Proc. of 2017 4th Int. Conf. on Information Tech., Computer, and Electrical Engineering (ICITACEE), Oct 18-19, 2017, Semarang, Indonesia.
- [3] D.Saraswathi;P. Manibharathy;R. Gokulnath;E. Sureshkumar;K. Karthikeyan, "Automation of Hydroponics Green House Farming using IOT" 2018 IEEE International Conference on System, Computation, Automation and Networking (ICSCA).
- [4] Chris Jordan G. Aliac;Elmer Maravillas, "IOT hydroponics management system" 2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM).
- [5] Carlos Ramos;Leonel Nóbrega;Karolina Baras;Luís Gomes, "Experimental NFT hydroponics system with lower energy consumption" 2019 5th Experiment International Conference (exp.at'19).
- [6] Himanshu Jaiswal;Karmali Radha P;Ram Singuluri;S Abraham Sampson, "IOT and Machine Learning based approach for Fully Automated Greenhouse" 2019 IEEE Bombay Section Signature Conference (IBSSC).
- [7] Mathawee Fuangthong, Part Pramokchon, "Automatic control of electrical conductivity and PH using fuzzy logic for hydroponics system" 2018 International Conference on Digital Arts, Media and Technology (ICDAMT).
- [8] Rajesh Kannan Megalingam, Gowtham Kishore Indukuri, Dhumsapuram Sai Krishna Reddy, Esarapu Dilip Vignesh, Vedha krishna yarasuri, " Irrigation Moniting and Prediction System Using Machine Learning" 2020 International Conference for Emerging Technology (INCET).
- [9] Herman, Pallavi Asthana, "Intelligent Monitoring and Controlling System for Hydroponics Precision Agriculture" 2018 International Conference on Computational and Characterization Techniques in Engineering & Sciences (CCTES).
- [10] Images referenced from google images on hydroponics farm. Image Urban kissan indoor hydroponics kit.<https://cloud.boltiot.com/> and bolt mobile app.

Internet of Things Applications Enablement its Challenges and Trends

Vivek Veeraiah

Department of R&D,
Computer Science, BGSIT,
Adichunchanagiri University
Karnataka-571418, India
vivek@EdVista.in

Dr. G. K. Ravikumar

Department of R&D,
Computer Science, BGSIT,
Adichunchanagiri University
Karnataka-571418, India
ravikumargk@bgsit.ac.in

Abstract: Internet of Things has acquired a remarkable attention in today's world. The world is becoming smarter in all aspect by using IoT technology. Internet of Things is one of the emergent technology and it is influencing our life. In this technology different types of devices are interconnected with each other through network to offer services in our daily life. The IoT devices are embedded with sensors where the generated data is shared through internet. This technology has gained attention in various fields like healthcare, smart home, automobiles, etc. The IoT has attained a significant attention in various countries. The devices used in IoT assures to convert various approach of life. This paper highlights an overview of the application enablement of IoT and discusses the challenges and trends of IoT.

Keywords: IoT, Sensor, Internet of Things, Applications, Challenges, Trends

I. Introduction

The Internet is been used everywhere in today's scenario. The technology is connected with internet with wide variety of appliances which is called as Internet of Things. Communication among the physical and digital world is linked with Internet of Things. All the IoT build products are internet supported appliances like home automation "smart home". The healthcare services are transforming the life by using medical devices which are connected to network like wearable fitness device and health monitoring device. The IoT technology which can be seen in smart cities, automobiles, intelligent traffic systems, etc. IoT technology are also implemented in agriculture, industry, and energy production. However the IoT has many issues and challenges that must be considered and addressed for the benefit of realization. The new technology (IoT) has been used in various areas. The standard Internet Protocol is used to connect computers through the networks with the internet system. There is a rapid transformation undergoing in the world with the technology of IoT where different objects are interconnected and data is generated. The data which is stored can be used to analyse valuable information. The actual term "Internet of Things" was proposed by Kevin Ashton in 1999 [1].

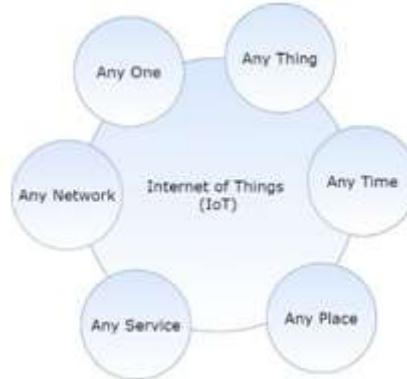


Fig 1: Internet of Things

The information from any devices is accessed by the support of IoT technology. The internet is used to communicate among the devices from anyplace at any time and provide any services. The concepts of Internet of Things is shown in figure1. Many applications like smart healthcare, smart homes, smart cities, smart energy, waste management, transportation and monitoring types can used IoT features. This research paper focuses on the application of IoT used in various fields with advantages and disadvantages.

This paper is organized as follows: Section II Related Work, Section III Applications of IoT, Section IV components of IoT, Section V Challenges, Section VI Future of IoT in India, a brief conclusion in Section VI.

II. Related Work

The IoT overview with highlighting on technologies, protocols, and application are discussed in various papers. "IOT is not just a concept but can prove to be a revolution in advancing technology to change the lifestyles of human's altogether" [2]. "The IoT is enabled by the latest implementations like RFID, smart sensors, communication technologies" [3]. "Internet of things and its applications related to future technologies and challenges help in exploiting the most advanced communication technologies to support added services for administration" [4]. The authors of inc42 [5] and wire19 [6], has discussed the recent trends and analysis of automobile industry.

III. Applications of IoT

The intelligent applications are developed in various areas. All applications are not yet readily available. The new dimension of ‘Things’ is communicating and integration between applications and humans is the concept of internet of things. Several applications of IoT in different areas of day-to-day life which broadly contains environment domain, industry domain etc., shown in figure 2. The applications of IoT are “home automation”, “fitness tracking”, “health monitoring” and “smart cities”.

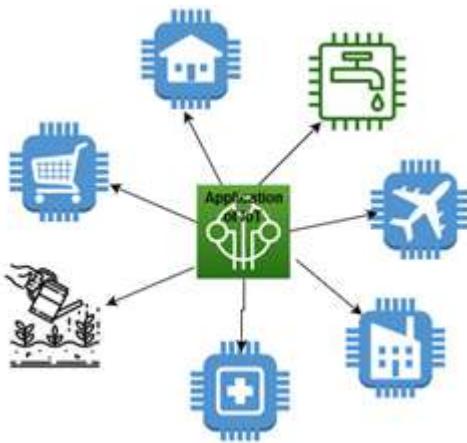


Fig 2: Applications of IoT

1. Intelligent Buildings

The intelligent building concepts are home automation, automatic energy metering, and wireless monitoring. The high level offices and luxury apartments the home or building automation technologies are been deployed. Benefits and possibilities of smart homes has been discussed in the research [7]. The applications become much broader when the cost of wireless communications become cheap and plenty with established technology. The “smart metering” is widespread for calculating consumption of energy and transmitting the electronic information to the energy provider. Fully interconnected smart environment in modern home with entertainment systems, general purpose computing platforms which is combined with sensors within a building. Temperature controller sensors are used for automatic adjust the level of room temperature by optimizing the use of energy for heating and cooling. Exceptional situations can be detected for assisting elderly people’s everyday activities by providing additional values for monitoring the human activities. The sensor networks can measure accurately the environmental parameters like temperature, humidity, light etc. The networked identifiable wireless devices which are connected with physical sensors to measure the parameters in building and homes. To control exact climate the energy control systems are used for the building. To

monitor the status and change settings of any device the input from the user is controlled by the device in the building. The thermostats settings for the fridge can be changed by using the touch screen monitor. Using mobile phone the home lights can be automatically switched on/off by setting the time while entering the building.

2. Healthcare

In healthcare area the IoT applications are emerging. The mobile phones are used with the RFID-sensor is used as a platform to monitor the medical parameters. By introducing IoT techniques to the field of healthcare the service quality has improved and also the cost is reduced. Few IoT devices are used to track the health specification like BP, blood glucose, body temperature, etc. The smart beds are used in the hospitals to monitor the patient’s occupation and check when the disabled patient is trying to get up [8].

3. Logistics and Supply Chain Management

Supply change management used internet of things technology. The RFID technology is used to find the presence of items on the smart shelves and track items [9]. The real time stock monitoring, tracing out of stock can be done using the technology [10]. To optimize the logistics of supply chain process the data from the retail store is used. If stock details from the retailers are directly known to the manufacture then the right amount of items will be produced and shipped by avoiding over or under production.

4. Manufacturing

Production process can be optimized in the manufacturing industry by using information technology by embedding smart devices. The entire production lifecycle can be monitored by using IoT technology. The items are tagged to the containers to gain the status of the shop floor and status of production. To improve logistics the input data is sent for scheduling the production. Intelligent manufacturing solutions and self-organizing can be considered for manufacturing.

5. Agriculture

The agriculture sector is one important think where the IoT techniques are used. This devices help the farmers to know about the environment around them. The IoT used in agriculture is to increase the productivity to minimize the wastage of water and maximize the yield [11]. The smart farming uses IoT techniques for farming operations, organic farming. The IoT technologies are providing uninterrupted

monitoring from planting through harvesting and to reach our homes [12].

IV. Components of IoT

The sensors and actuators are the physical devices which are used to interact in the digital world. Every appliance and devices of IoT are interconnected to the network. The devices of IoT are embedded with sensor, actuator and processor. In the physical environment the sensor and actuator are the IoT devices which interact with each other. The stored data which is collected from the sensors are useful for analysis. The actuator device is used to find the changes of the environment like the air conditioner temperature controller. The remote server are also used to store and process the data which is send by the sensors or other devices.

V. Challenges

The IoT technology advances in communication and processing of data and it is accessible form any place. The data which is stored for analysis is a challenge where the data should be accurate and proper. The data collected from the various devices should be handled properly these are the challenges on communication. The IoT devices are wireless which is connected with the network and the communications between it is also challenging as it is installed geographically dispersed locations. The high rate of misrepresentation and unpredictability in the wireless channels are often challenging. It is important to see that reliable data communications without too many retransmissions should be performed. Thus the communication technology is an integral study of IoT devices. The huge amount of data is generated due to vast usage of IoT devices which in turn is creating the scope for handling and analysing the big data. IoT is creating lot of research avenues due to its vast data and newer technologies both in terms of hardware and software. The security and privacy is also challenges as many devices are connected and there are chances of cyber-attack [13].

VI. Future of IoT in India

Internet of Things in India, the market potential is likely to reach USD 9 billion in the coming years. The demand for IOT in INDIA are rapidly growing to the tune of 31 times to reach 1.9 billion. Around 3.1 billion people are connected to the network in the populations of 7.6 billion in the world. Approximately 24 % of people belong to India those who are connected through internet. There is a change in the way where things are connected with IoT technology by everyone, everything and everywhere. The IoT start-ups in India are roughly 70% which has emerged in the field of healthcare and

manufacturing shown in figure3. Through this technology the lifestyle of people changes when they are smart buildings and smart homes. In India the smart city initiatives planned are more than 100. The focus is to involve the communication between people, people to machine and also machine to machine. The entire world wants to get connected to the internet though the smart phones, computers, smart watches, refrigerators, air-conditioning. This can be done through the internet of things. The government is taking initiatives like “Digital India” and “Make in India”. The smart cities are connected though IoT devices to manage the traffic, healthcare etc.



Fig 3: India IoT market size

a. Automobile Industry IoT Trends and analysis

The authors of inc42 have discussed the trend of automobile industry [5]. The largest industry in the world is the automobile manufacturing industry. The IoT techniques are implemented in this industry. The idea of self-driving cars has taken a hold across the globe. The IoT devices installed inside the vehicles will grow up to 250 Mn by this year. The self-driving technology is already implemented in many countries. The IoT devices which come in-built are navigation systems like Google Maps where the information is send and received through internet. The entertainment systems also will help the customers to listen music on spotify or steam a video. The predictive maintenance for cars is one more technology will be introduced by next year. It comprises of IoT sensors in vehicles that monitor functional metrics of the vehicle. IoT sensors will also be used to transmit information about a car to its manufacturer.

b. Healthcare IoT Trends and analysis

The internet of things in Healthcare market is expected to reach USD 172 billion in the coming years at a CAGR of 20.8%, as per mordorintelligence

[14]. The paper based health care treatment has changed to IoT technology for monitoring the remote patients and store the patient data. Health care therapeutic tools are used for tracking wellness for athletes and dosing remainder for patients. The healthcare systems are connected with IoT devices to the internet for patient tracking or equipment tracking. The various devices are “wearable external medical devices”, “implanted medical devices”, and “stationary medical devices”. IoT supports solutions to value the outcomes from the sensor of a device to monitor a patient remotely. To monitor the pulse rate, heartbeat, and other health related data there are wearable devices.

VII. Conclusion

This paper presents an overview of IoT applications and challenges that has to be encountered in day-to-day life. The IoT technology has enabled the communication between objects and human using internet to make a smart and intelligent planet. The communicating technique has become very easy from anywhere, anytime, anyway, anything by using IoT. The IoT technology is showing signs of development in many fields. However a lot of challenges are there to take place in the field of various applications. In this paper the trends and analysis in some of the areas are discussed. In future IoT is going to be considered as the core part of existence for humans to communicate with machines. This technology is definitely going to impact the human life in unimaginable way over the next decade. Change is the order of the day. All the human race must embrace and harvest the best outcome of IoT to make this world truly a Global Village.

References

- [1] D. Singh, G. Tripathi, Antonio J. Jara, “A survey of Internet of Things: a g Vision, Architecture, Challenges and Services”, IEEE World Forum on Internet of Things (WFIoT), 2014.
- [2] Li, S., Da Xu, L., & Zhao, S. (2015), The internet of things: a survey, *Information Systems Frontiers*, 17(2), 243-259.
- [3] Komal Batool, Muaz A. Niazi, “Self Organized Power Consumption Approximation in the Internet of Things”, IEEE International Conference on Consumer Electronics (ICCE), 2015.
- [4] D. Yang, F. Liu and Y. Liang, "A survey of the internet of things," in Proceedings of the 1st International Conference on E-Business Intelligence (ICEBI2010), 2010, pp. 358-366.
- [5] www.inc42.com/resources/automotive-iot-devices-market-trends-and-analysis-2020
- [6] www.wire19.com/future-of-iot-in-india-current-market-trends-and-use-cases
- [7] A. Taylor, R. Harper, L. Swan, S. Izadi, A. Sellen, M. Perry. Homes that make us smart. *Personal and Ubiquitous Computing*, Vol.11, Number5, June2007.
- [8] Mari Carmen Domingo, “An overview of the Internet of Things for people with disabilities”, *Journal of Network and Computer Applications*, vol. 35 pp: 584–596, 2012.
- [9] B. C. Hardgrave, M. Waller, and R. Miller, *RFID's Impact on Out of Stocks: A Sales Velocity Analysis*. Research Report from the Univ. of Arkansas, 2006.
- [10] T. W. Gruen, D. S. Corsten, and S. Bharadwaj, *Retail Out of Stocks*. Technical report, 2002.
- [11] Patil, V. C., Al-Gaadi, K. A., Biradar, D. P., and Rangaswamy M. (2012). Internet of things (IoT) and cloud computing for Agriculture: An overview, *Proceedings of Agro-Informatics and Precision Agriculture (AIPA 2012)*, India, 292-296.
- [12] Y. Liu, H. Wang, J. Wang, K. Qian, N. Kong, K. Wang, L. Zheng, Y. Shi, D. Engels, “Enterprise-Oriented IoT name service for agricultural product supply chain management.” *International Journal of Distributed Sensor Networks* August 2015 vol. 11 no. 8
- [13] S. Chen, H. Xhu, D. Liu, B. Hu, H. Wang, “A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective.” *IEEE Internet of Things Journal*, VoL. 1, No. 4, August, 2014.
- [14] www.mordorintelligence.com/industry-reports/internet-of-things-in-healthcare-market.

Decision Support Tool for Examination Questions according to Bloom's Taxonomy

Dr. G. N. R. Prasad

Sr. Asst. professor

Department of MCA

Chaitanya Bharathi Institute of Technology (A),
Hyderabad, Telangana-5000075, India.
gnrprasad_mca@cbit.ac.in

Abstract: The cognitive domain in the Bloom's Taxonomy is that the benchmark for developing tests and assessments; therefore, there's a requirement to conduct a meticulous survey of those subjective and objective question papers to gauge the degree of Blooms Taxonomy incorporated in them. These question papers don't systematically assess the gradual stages of learning proposed in Bloom's Taxonomy leading from the lower degrees like remembering, understanding, applying, to the upper degree like analyzing, evaluating and creating[2]. Intelligent analysis tool for Bloom's Taxonomy (IBT) is a tool developed to assist the faculty to adopt the cognitive domain of Bloom's taxonomy in the preparation of examination question paper. The tool is also helpful to improve the metacognition skills of the disciple. This paper presents how to improve the qualities of teaching and learning, and how to develop and implement Bloom's taxonomy. It was noted during this research that the tool is not only useful for preparing queues at different cognitive levels, but also helpful for updating questions to a different cognitive level when the similar keyword of Bloom exists on the other level. Using python, IBT Tool is developed. It uses file oriented concept. Accepts the question paper in a document form as an input. Reads the question and identifies the level of blooms and corresponding question will be updated.

Keywords: Bloom's taxonomy; Python;
Examination questions;

I. Introduction

Written examination is the most customary method used by any educational institution for the evaluation of students. Question is only element reveals the subject knowledge of the student and also question or problem plays a very important important part in exertions to test the students' Per semester, average cognitive scores are assessed.. Effective style of questioning is always an issue to help students attend to the desired learning outcome[3]. The Taxonomy of Educational Objectives, known as Bloom's Taxonomy [1] is one of the most recognized learning theories in the field of education. Educators often use Bloom's

Bhavani Uddagiri

MCA IV semester,

Department. of MCA

Chaitanya Bharathi Institute of Technology (A),
Hyderabad, Telangana-5000075, India.

Taxonomy to create learning outcomes [2]. Bloom's Taxonomy is the standard for developing tests and assessments.

The goal of this paper is to propose a rule-based approach to determining the Bloom's cognitive taxonomy level of examination issues using natural language processing. The examination questions will be examined and each question will be classified on the basis of Bloom's cognitive taxonomy level. This helps the academics to develop adequate examination questions as required. The test questions are discussed and each matter is classified according to Bloom's cognitive taxonomy levels.

The categories of recall, understanding, apply, analyse, assess and create are included in the latest flora taxonomy version. The recall allows us to recall facts, terms, basic concepts and answers in memory of previously learned material. This is an understanding of the acts and ideas through the organisation, comparison, translation, interpretation, description and key ideas. Problems in new contexts are solved by applying learned experience, facts, methods, and laws in new ways. The analysis examines and divides information into portions through the identification of reasons or causes. Find inferences and evidence to encourage widespread use. In the evaluation, opinions are presented and defended by evaluating information, validating ideas or working quality based on a range of criteria. This creates information in a different way through the combination of elements in a new design or the proposed alternative solutions.

II. Related Work

Most work has been done to identify exam questions based on Bloom's taxonomy. However, there has been no effort to use natural language processing methods to solve this issue. Chang & Chung presented an online objective test system to classify and analyse the cognitive level of Bloom's taxonomy to English questions [5]. The machine acknowledges the query of the exam as content, which would then be segmented. This scheme has a database of different verbs in Bloom's taxonomy. The index contains lower case verbs and capital letters. The method then contrasts the entire verb tenses

found in the questions. Where a keyword is included in the test object, the same query belongs to the keyword. Weight for the question is added whether one of Bloom's categories shares the same verb.

Table: The First version of Bloom's Taxonomy Cognitive Domain and it's verbs

COGNITIVE LEVEL: BLOOM'S TAXONOMY OF EDUCATIONAL OBJECTIVES					
The cognitive domain of learning involves mental operations or thinking skills. There are six major categories in the Cognitive Domain of Bloom's Taxonomy (1956). The levels and the verbs used for stating specific behavioral learning outcomes are listed below.					
KNOWLEDGE	COMPREHENSION	APPLICATION	ANALYSIS	SYNTHESIS	EVALUATION
(Remembering, Recalling terms, facts, and details without necessarily understanding the concept)	(Understanding, Summarize and describe main ideas in own words without necessarily relating it to anything)	(Transferring, Applying or transfer learning to over life or to a context different than one in which it was learned)	(Relating, Breaking material into parts, describe systems and relationships among parts)	(Creating, Creating something new by combining parts to form a unique solution to a problem)	(Evaluating, Expressing own opinion, judge w/ value based on expressed criteria, ideas, methods)
Count Define Dive Identify Label List Locate Name Outline Point Quote Recite Record Repeat Recognize Select State Write What is the definition of... Can you recite... When... Where... Who... How many...	Associate Classify Convert Describe Differentiate Discuss Distinguish Estimate Explain Interpret Match Paraphrase Predict Recognize Select Summarize Translate In your own words, explain... what steps are required... Describe the time of... what do you think he would say about...	Apply Build Calculate Classify Compare Complete Contrast Construct Demonstrate Illustrate Modify Operate Practize Relate Report Solve Use Give an example that has affected you... Or when... what would result if... How would the be different if... When these concepts are mixed see...	Analyze Categorize Compose Deduce Detect Diagram Differentiate Distinguish Group Inter Investigate Prioritize Relate Research Separate Sort Transform What factors distinguish... Or when... How would the be different if... When these concepts are mixed see...	Adapt Assimilate Combine Compare Compose Create Design Formulate Generalize Integrate Invent Organize Plan Prepare Prescribe Revise Specify In your opinion... Choose between... and defend your answer...	Accept Appraise Assess Compare/Contrast Critique Determine Evaluate Facilitate Grade Judge Justify Measure Rank Recommend Reject Select Test In your opinion... Choose between... and defend your answer...

III. Research Methodology

In this paper, a normative approach is adopted when the question items are classified into the cognitive level of Bloom. The test items are a collection of exam questions in the subjects for the first half of the year obtained from the department of computer applications CBIT. The course includes 70 exam questions and 30 questions in the test set. Test items are only addressed by written final examination. Test items are only addressed by written final examination. With the help of the developed rules, the system automatically classify each question into its respective verbs from Taxonomy. This work excepted the trouble level of each issue as a measurement factor in the determination of the category of questions.

1. Rules Development

This research uses a rule-based approach to determine the category of a question based on the taxonomy of the Bloom. The rules are drawn up from a training set of 60 questions for the programming subjects. The rules are applied under two conditions:

- The rules shall differentiate the appropriate keyword according to the category of each question.
- If the keyword is used by more than one group, assist in choosing the appropriate group. For

example, Summarize may fall under Synthesis or Comprehension category.

The question patterns show that most of them start with a verb after analysing all the questions in the training set. Only a few begin with the Wh+ pronoun, a determiner, preposition or subordinate conjunction, a substance and an adverb. Specific patterns from the question item should be identified before rules can be applied.

Sample Code in Python

```
str_a =("define, choose find, how, relate, recall, select,show,tell, spell,where,which, what,when,who,why, label, list, match, name, omit ")
```

```
str_b=("infer, interpret, extend,illustrate, outline, relate, rephrase, show,summarize,translate, contrast,demonstrate,explain, classify, compare")
```

```
str_c=("apply,build,choose,construct,develop,experience with,identify,interview,make use of,model,organize,plan,select,solve,utilize")
```

```
str_d=(" assume, analyze, classify, categorize, conclusion, compare, discover, contrast, distinguish, dissect, examine, divide, inference, function, list, inspect, relationships, motive, survey, simplify, test for, take part in, theme")
```

```
str_e=("agree,appraise,assess,award,choose,compare, conclude,criteria,criticize,decide,deuct,defend,determine,disprove,estimate,evaluate,explain,importance,influence,interpret,judge,justify,mark,measure,opinion,perceive,prioritize,prove,rate,recommend,rule on,select ,support,value")
```

```
str_f=("adapt,build,change,combine,compile,compose,construct,create,delete,design,develop,discuss,elaborate,estimate,formulate,happen,imagine,improve,invest,makeup,maximize,minimize,modify,original,organize,plan,predict,propose,solution,solve, suppose,test,theory")
```

```
str_g=input("enter ur string")
switch(str_g==str_a || str_b || str_c || str_d || str_e || str_f)
{
    case 1:
        print("remembering category")
    case 2:
        print("understanding category")
    case 3:
        print("applying category")
    case 4:
        print("analyzing category")
```

```
case 5:  
    print("evaluating category")  
  
case 6:  
    print("creating category")  
  
case 7:  
    print("creating category")  
default:  
    print("the question does not fall in this  
categories anymore")  
}
```

IV. Conclusion

Bloom's Taxonomy is a system used by educators to categorise learning goals for students. The method of preparing of test papers is a big role in the process of schooling. In this paper, the use of the cognitive levels as defined in Bloom's taxonomy has established an automated model to categorize examination issues. The combination of the rules established and Bloom's taxonomy has shown that this paradigm works well for categorising questions. Teachers can conveniently examine previous study papers using this model and get thoughts on the preparation process for upcoming tests. In addition to the model, the query paper may be quantitatively adjusted and modified. We plan to extensively analyse our approach to current approaches in our future work. We have presented a concept to automate the categorization process by Bloom's taxonomy based on its cognitive levels. Rules may be formed to improve the results' accuracy. More rules are developed and tested for future work to improve the efficiency of the system. We have therefore been mainly interested in further testing in the near future.

References

- [1] Bloom, B. S.; Engelhart, M. D.; Furst, E. J.; Hill, W. H.; Krathwohl, D. R. (1956). Taxonomy of educational objectives: The classification of educational goals. Handbook I: Cognitive domain. New York: David McKay Company.
- [2] Anderson, L., & Krathwohl, D. A. (2001). Taxonomy for learning, teaching and assessing: A revision of Bloom's Taxonomy of Educational Objectives. New York: Longman.
- [3] Swart, A.J. (2010). Evaluation of Final Examination Papers in Engineering: A Case Study Using Bloom's Taxonomy, IEEE Transactions on Education, (May 2010) Vol. 53, No.2 257-264.
- [4] Swart, A.J. (2010). Evaluation of Final Examination Papers in Engineering: A Case Study Using Bloom's Taxonomy, IEEE Transactions on Education, (May 2010) Vol. 53, No.2 257-264.
- [5] Cutrone, L., & Chang, M. (2010). Automarking: Automatic Assessment of Open Questions, 2010 10th IEEE International Conference on Advance Learning Technologies. -147.

Session-B3:
Natural Language Processing and
Computer Vision

Automated Attendance Using: Facial Recognition

Vijay Kumar

Department of Computer Science

Kakatiya Institute of Technology & Science
Warangal, Telangana-506015, India

Janith Adavala

Department of Computer Science

Kakatiya Institute of Technology & Science
Warangal, Telangana-506015, India

Devendar Maddeboina

Department of Computer Science

Kakatiya Institute of Technology & Science
Warangal, Telangana-506015, India

Abstract: Taking Attendance manually may be a very tedious job and wastes tons of your time too. The prevailing biometric attendance also wastes tons of your time because it isn't automatic and also requires the involvement of the scholars too. The work described aims at automating the entire process. The camera installed will take an image of the entire classroom, followed by detecting individual faces within the image, recognizing the scholars then updating their attendance. The images are going to be captured twice, once at the start of the category and once at the end to make sure that the scholar has attended the entire class.

Keywords: Facial Recognition Facial Detection
Image Processing Database

I. Introduction

Understudy participation is a significant part of the preparation cycle on the college. By going to class, understudy prepared to get important data from the instructor, all together that the researcher prepared to improve information and comprehension towards a particular field or possibly a few abilities. Support and perception of going to records assumes a significant part at stretches the examination of execution of any association. The point of creating going to the board framework is to mechanize the regular way of taking joining in. Mechanized Attendance System plays out the exercises of participation stamping with no human investment. The procedures can be utilized for picture acknowledgment. The proposed framework plans to beat the traps of the overall frameworks and gives highlights, for example, identification of faces, extraction of the highlights, discovery of extricated highlights, and examination of understudies' participation. The framework coordinates strategies like as picture contrasts, basic pictures, shading highlights and falling classifier for include identification.

Biometrics techniques are utilized for an identical reason since an all-encompassing time now. Despite the fact that it's successful, it's as yet not totally solid for reason for identifying a person. Attendances of every understudy are being kept up

by each school, school and college. Observational confirmations have demonstrated that there's a major relationship between's understudies' attendances and their scholastic exhibitions. There was likewise a case expressed that the researchers who have helpless participation records will by and large connect to helpless maintenance. Accordingly, personnel must keep up appropriate record for the participation. The manual participation record framework isn't productive and expects longer to revamp record and to compute the regular participation of each understudy. Consequently there's a necessity of a framework which will address the matter of understudy record game plan and understudy normal participation count.

II. Objectives

The objectives are as follows

1. To form the entire process automated.
2. Location of interesting face picture and accordingly the other normal segments like dividers, foundation, and so on
3. Extraction of remarkable trademark highlights of a face helpful for face acknowledgment.
4. Location of appearances among other face characters like facial hair, displays and so forth
5. Powerful acknowledgment of exceptional appearances during a group.
6. Robotized update inside the information base without human intercession.

III. Literature Survey

The first step is to capture an picture. Picture handling is ordered into two kinds. They are,

1. Simple picture handling
2. Advanced picture handling

Two dimensional simple signs are handled by simple picture measure. Computerized picture measure is that the utilization of PC calculations or picture measure on advanced pictures. Advanced

picture measure is performed on a 2 dimensional picture by a data handling framework. Facial acknowledgment innovation could be another methodology of build up individuals. It works by choosing faces out of a group, getting the estimations and assessment it to the photos effectively present inside the information. The manual procedure will be supplanted via programmed going to framework that is takes heaps of your time and is hard to deal with. As a rule, there are 2 unit celebrated ways to deal with HFR, for example highlight based and splendour based methodology. The component essentially based methodology utilizes key reason choices of the face, for example, edges, eyes, nose, mouth, or elective exceptional attributes. In this way, the computation strategy exclusively covers a few segments of the given picture that are removed predecessor. On the contrary hand, the splendour principally based methodology figures all parts of the given picture. It is additionally assigned to as comprehensive based or picture based methodology.

IV. System Requirement

Software

1. Net beans IDE/ Eclipse IDE
2. Advanced Java (Applets, JSwing)
3. MySQL Database

Hardware

1. Digital Camera

V. Implementation

The initial step is that, the staffs are given their own Username and Password to Log-in. Subsequent stage is, the instructing picture and their alternatives zone unit hang on inside the data. At that point, testing picture alternatives zone unit contrasted and the training pictures. When the picture is distinguished, the participation will be enrolled. At long last, the participation subtleties of the understudy are shipped off staff and parent through E-Mail.

1. Login.
2. Staff & Student Information.
3. Update Attendance.
4. Feature Extraction.
5. Feature classification

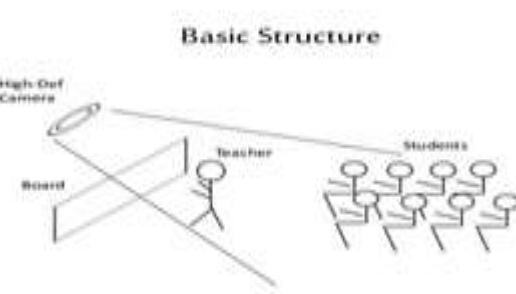


Fig 1

In this system a high definition camera captures two images, one at the start time of the class and other at the end time of the class. If the student recognized both at the start and end time of the class then only his/her attendance will get updated.

VI. Methodology

Image Acquisition

Pictures will be non-inheritable by facial-filter innovation from camera that catches pictures of higher calibre and assurance. Pre-processing.

Pre-processing

First picture is edited from non-inheritable picture. At that point edited pictures are reshaped to certain pixels for face acknowledgment. These reshaped pictures zone unit renewed from RGB to dark level.

Database (DB)

It stores the pre-processed pictures for any process and results.

Template Matching

It looks at coordinate formats against entrance layouts. In trademark one single from an outsized data, facial output isn't in this way successful as iris examine. At the point when enormous scope facial-examine recognizable proof ventures, quantities of matches' territory unit came.

Face Recognition

For face acknowledgment or identification it analyzes choose facial parts from the picture and face data, it distinguishes or confirms somebody in picture.

Face info Generation

Unique face information comprises of photos of all understudies having five pictures for

every understudy. With alteration in force of daylight and fluctuated outward appearances, initial info pictures area unit non-inheritable at varied interval of your time. After capturing the image, subsequent method is to discover the faces. CNN algorithmic program is employed to discover individual face pictures from whole image. Face detection is employed to see the situation of the faces within the room image and extract sub-images for every face. After detection, the image process cleans up the individual facial image for easier recognition of the face.

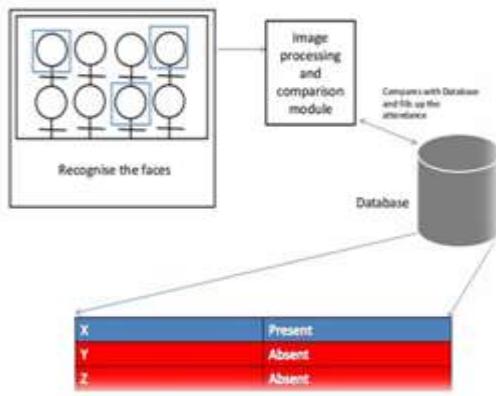


Fig 2

VII. Algorithm

CNN Algorithm

Usage of CNN rule

1. To do information processing
2. In deep learning.

Advantages of CNN rule

1. Speed and performance is sweet.
2. Distinctive moving objects.
3. Identity verification.

For implementing the sensible attending system exploitation face recognition system, we've got to follow the subsequent steps within the same order. Those steps area unit as follows:

Train the system, Test image, Face detection, Alignment, Face cryptography, Recognition, Store attending information.

VIII. How Do We Create Database

After detection and processing of the images the next step is to compare individual face images with the images in the database. Dataset is created only to train the system. The database includes names of the students and registration number for each

student corresponding to their images of different varieties. For better precision least of 10 pictures of every understudy should be caught. At whatever point understudy's information and pictures are utilized to make a dataset, profound learning applies to each face to figure highlights and store in understudy face information record to review that face in acknowledgment measure. This cycle is applied to each picture taken during enrollment.



Fig 3

Architecture and working of Database

In this system, the frontend side consists of elements which are based on java script and server side consists of. An IPC connect is created to impart between these two stacks. The pictures caught by the camera are shipped off the framework for additional examination, the information picture is then contrasted and a bunch of reference pictures of every understudy and imprint their participation. Whenever faces are identified and perceived with the current information base, framework computes participation for the perceived understudies with the particular subject ID continuously. Furthermore, a dominate sheet is produced and saved by the framework naturally. The adjacent figure shows the structure of a typical database which consists of student ID, student registration number, student face images with different variations.

Advantages

1. Better Security features than other biometrics.
2. Eradicate manual work and make it automated.
3. It can be easily integrated with existing equipments.
4. Facial Recognition is cost-minimal and effective.

Disadvantages

1. Poor image quality affects the accuracy rate.
2. If the picture is less than the required one then it affects the accuracy rate.
3. If the memory is less then it affects the process.
4. If someone changes his /her physical appears like victimization spectacles, dynamic hair conjointly affects the accuracy of the identity verification.

IX. Conclusion

The machine controlled under study participation framework utilizing face acknowledgment procedure works pleasantly. This can replace standard technique, which takes tons of your time and is tough to take care of. Absolutely, it's improved for higher outcome strikingly by observing in element extraction or acknowledgment strategy. It could facilitate popularity method for a lot of strong.

X. Future Scope

Automated attending System makes the full method of attending machine-controlled that saves each time and energy. Automatic face recognition may be a biometric technology whose demand and usage is being increasing day-by-day at a bigger pace. A lot of analysis during this on automatic face recognition and detection will more improve accuracy rate, and create all transactions straightforward and secure.

References

- [1] Rajat Kumar Chauhan (2018), Smart Attendance System Using CNN, International Journal of Pure and Applied Mathematics, 119(15).
- [2] Navesh Sallawar (2017), Automatic attendance system by using face recognition, International Research Journal of Engineering and Technology (IRJET), Volume 04, Issue 04.

Comparative Study of Single Image Super Resolution Techniques

Hruday Tej Akkaladevi

Department of Computer Science and Engineering
Chaitanya Bharathi Institute of Technology(A)
Hyderabad-500075, India
hruday.tej.akk@gmail.com

Dr. A Nagesh

Professor, Department of computer science and
Engineering
Mahatma Gandhi Institute of Technology
Hyderabad-500075, India
anagesh_cse@mgit.ac.in

Prof. N. Rama Devi

Department of Computer Science and Engineering
Chaitanya Bharathi Institute of Technology(A)
Hyderabad-500075, India
nramadevi_cse@cbit.ac.in

Abstract: Super-resolution is a technique for constructing high-quality images. Single Image Super-Resolution has become a trendy topic in the field of image reconstruction and restoration. From identifying criminals to restoring old artifacts, and understating the olden sculptures, super-resolution has been of great use for human development. And there have been many solutions and architectures developed to provide promising results in increasing the resolution of images, every architecture has its pros and cons and the quest for obtaining more photorealistic images is still going on. The objective of the work is to study and compare single image super-resolution techniques. In this paper, the comparison of a few of the famous and traditional Single image super-resolution techniques which can convert low-resolution images into high-resolution images and also test out their efficiencies to provide some insight on how those architectures work to produce good results. Here first the discussion of popular interpolation techniques followed by the explanation of how convolutional neural networks and GANs took up the spotlight in providing more promising results for super-resolution in image reconstruction and restoration.

Keywords: Super Resolution(SR), Nearest Neighbour Interpolation, Bicubic, SRCNN, SRGAN, SRResNet.

I. Introduction

The goal of single-image super-resolution (SISR) algorithms is to generate a higher resolution (HR) image from a low-resolution (LR) image input. Reconstructing a high-resolution image from its low-resolution image is a long challenging task in the field of computer vision. This task becomes even more difficult when a single low-resolution image available as input to recreate its high-resolution image. The need for high resolution is common in computer vision [1] applications for better performance in pattern recognition and analysis of images. High resolution is of importance in medical

imaging for diagnosis. Many applications require zooming of a specific area of interest in the image wherein high resolution becomes essential, e.g., surveillance, forensic, and satellite imaging applications. The super-resolution techniques are divided into two categories, which are multi-image super-resolution and single image super-resolution. In this paper, the single image super-resolution techniques are discussed.

The paper is organized as follows. Section two presents single resolution techniques literature and in section three single resolution techniques are compared.

II. Single-Image SR Approaches

The single super-resolution approaches that are classified into three categories based on the application point of view are, interpolation-based, reconstruction based and example-based. In this paper, the interpolation-based and example-based approaches are reviewed and compared. The different interpolation techniques, presented in the literature for the super-resolution of the images are the nearest neighbor interpolation, bi-cubic interpolation, super-resolution conventional neural network, super-resolution residual network, and super-resolution generative adversarial network. The nearest neighbor interpolation approach is the simple and easiest method among them.

Here we study the various models developed to tackle the single image super-resolution task. We discuss the implementations and methodologies of various models in an incremental manner. Initially, interpolation techniques were devised to tackle this problem, but due to their inefficiency more complex mathematical techniques were introduced, and to reach the state of art results the deep learning and predictive models have come into the picture and all the details of the models will be discussed further. Specifically, we describe the model then show its methodology and state its pros and cons and the results would be compared in a tabular model in the

final section. And in certain models, as the authors of that work devised, we would also try to tune the parameters and get inference from the results. We start with Nearest Neighbor Interpolation, followed by the discuss Bicubic Interpolation, next we check out SRCNN, then we optimize it to form SRRNet, and finally, we examine the SRGAN.

Nearest Neighbor Interpolation

Nearest Neighbour Interpolation is the most basic model introduced in the field of single image super-resolution. Basically how the nearest neighbor interpolation works is, an input low-resolution image is taken and then it is enlarged by a particular scale, suppose the input image is 2×2 and it is enlarged by a scale of 5 it would become a 6×6 image [4], due to this enlargement there would be gaps formed, and these gap values are filled by determining the pixel value of the nearest pixel to the gap [7]. It has to be noted that this methodology does not predict or map any value, it just copies the values of the nearest pixel [4]. Because of its non-interpolative nature, this nearest neighbor technique is used when small variations in the pixel values are needed to be retained. For one-dimensional nearest-neighbor interpolation, 2 grid points are necessary for the interpolation function, and for two-dimensional nearest-neighbor interpolation, 4 grid points are essential for the evaluation of the interpolation function. There are some pros and cons to this methodology as stated in the work of [4]. As this interpolation method is very simple and fast, it is very helpful in smaller upscaling factors and minor changes in images. But as this method is very simple, it would not be helpful in higher upscaling factors. And as there is no prediction or estimation involved in this technique, as this method just copies the pixel values, the results obtained would not be satisfactory enough because the important features of the images like edges and shapes might be lost and not retained. After all, the image would be highly smoothed.

BiCubic Interpolation

As the results produced by Nearest Neighbour and Bilinear interpolations are not good for high scaling factors, as it fails to retain some crucial information by making it redundant [4]. While upscaling a low-resolution image using the above-mentioned interpolation techniques, Features like edges and borders are lost by smoothing them or making them distorted, which makes them vulnerable to failure in edge detection mechanisms. So to tackle this the bicubic interpolation technique has been introduced, when the input image is upscaled by some numerical factor which in turn creates gaps in the image, in the Bicubic interpolation technique those gaps are filled with the help of the nearest 16 neighbors. Next, the grey level value or color of a

pixel is determined from the weighted average of the 16 closest pixels to the specific input coordinates. So here instead of depending on one nearest neighbour in nearest-neighbour interpolation and 4 nearest pixels in bilinear interpolation, this technique depends on 16 of them with which the important features are retained and preserved and thus produces a sharper image instead of a smoother one. Using the nearest 16 pixels would help to produce an information-rich image with sharper edges and more clarity compared to the nearest neighbours and bilinear interpolation. The only drawback of this technique is that it is computationally expensive and slower compared to other techniques.

Super Resolution Convolutional Neural Network

With less promising results obtained and more computational time, there is a need for a faster and more efficient methodology that can yield promising output. And with the increasing trend in using Convolutional Neural Networks due to their success in image classification, they have been used even in the domain of Super-Resolution and it turned out to be a good fit for the task. Chao Dong et al.[2] has proposed a model which can learn an end-to-end mapping from the input low-resolution image and its high-resolution image. The developed model is called SRCNN [2] which aims at optimizing end-to-end mapping of the input noisy and low-resolution image to high-resolution image. So, in the super-resolution convolutional neural networks, initially, the input image is taken and enlarged/upscaled to the desired size with some scaling factor using Bi-Cubic Interpolation. This interpolated image is denoted as Y, which is a low-resolution image. Now the authors Chao Dong et al [2]. aimed to create image F(Y) from Y such that it is closest to the ground truth X. The neural network learns mapping via the following steps:

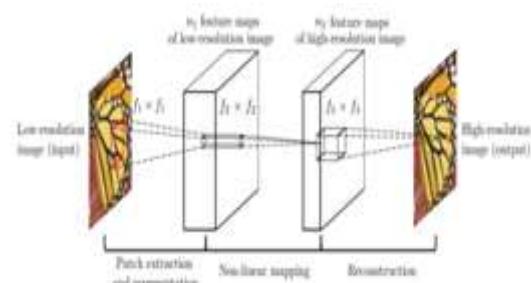


Fig 1: Architecture of SRCNN as stated in the work of Chao dong et al. [2]

- Patch Extraction and Representation:** One of the efficient tricks in image restoration is to properly extract patches and representing them as a set of pre-trained bases. This step is very similar to the one in the convolutional neural network, where there is an input image and a

filter/kernel/feature extractor is applied, then element-wise multiplication is performed, then a set of feature maps are obtained as output. So basically the aim is to find the patches in the input image that are matching or overlapping patches in the filter/kernel, and then a stride that determines how many units to shift the filter after every submatrix multiplication operation. In the implementation of this technique, the optimization of these bases would result in the optimization of the network. The filters/kernels can also be trained to extract features faster and efficiently. So mathematically the first layer can be expressed as F1:

$$F_1(Y) = \max(0, W_1 * F_1(Y) + B_1) \quad (1)$$

Here, W1 and B1 are the filter/kernels and biases respectively, and '*' denotes the convolution operation that is mentioned above. And W1 corresponds to n1 filters of dimensions $c \times f1 \times f1$, here c means the number of channels in the input image i.e. if the input image is grayscale then the value of c is 1 and if it is a coloured image then the value of c is 3 (Red, Green, Blue), f1 is the spatial size of the kernel used. W1 applies n1 convolutions on the image, and each convolution has a kernel size $c \times f1 \times f1$. The output of this operation would contain a set of n1 feature maps which have been extracted with the convolution process. And then, B1 is represented as an n1-dimensional vector whose every element corresponds to a filter. After this step, an image is produced as output and this output image may contain some linearity, and it would be very inappropriate for the neural network to learn these linearities, so to introduce non-linearity a Rectified Linear Unit is applied on the filter responses i.e., the feature maps.

2. **Non Linear Mapping:** As stated in the work [2], After the n1 dimensional features for each patch are extracted from the previous step, here each of these n1 dimensional feature vectors are mapped to a 2-dimensional feature vector. It is similar to using a 1×1 filter/kernel and performing convolution operation as shown in the above step. The 3×3 or 5×5 filters can also be used instead of the standard 1×1 filter. The operation on the second layer is

$$F_2(Y) = \max(0, W_2 * F_1(Y) + B_2) \quad (2)$$

So, in this function W2 is made up of n2 number of filters, each of size $n1 \times f2 \times f2$, and B2 would be the n2-dimensional vector. Here more intermediate convolutional layers can be added which could increase the performance, but this can also increase the complexity of the model and also the training time of the model, but the

advantage would be that the deeper structures and features in the images can be inspected by adding additional layers. In a nutshell, this operation non linearly maps each high dimensional vector or feature map into another high dimensional vector, these vectors would contain another set of feature maps.

3. **Reconstruction:** As mentioned in the work of [2], in this operation, all the above generated high-resolution are aggregated or combined in a patch-wise representations to generate the final high-resolution image which would be as close as possible to the ground truth. In the traditional reconstruction methods, the output image would be the average of the predicted overlapping high-resolution patches. The averaging function can be considered as a pre-defined filter on the feature maps. It is to be noted that the positions of these feature maps are flattened. With this intuition, the final convolutional layer is defined as :

$$F(Y) = \max(0, W_3 * F_2(Y) + B_3) \quad (3)$$

(As already mentioned the ReLU is applied to remove the non-linearities after the feature extraction.) where W3 corresponds to c filters of size $n2 \times f3 \times f3$, and B3 would be the bias like a c-dimensional vector. All of the steps are mentioned in a pictorial format in figure 1.

In the training phase of the model, As the end-to-end mapping is performed between the low-resolution input image and high-resolution image, there has to be a certain criterion or a measure informing how well the fit is in a particular epoch, so making use of certain loss functions to measure the quality of the fit would be a good approach. The mapping function F depends on the parameters $\Theta = \{W_1, W_2, W_3, B_1, B_2, B_3\}$. To get a good and accurate fit the loss function has to be minimized, loss function is nothing but the measure of how much of the crucial information is lost. So reducing the loss function becomes an important task. And the loss can be measured with the help of per-pixel mean squared error(MSE) loss function. The loss function is defined as follows :

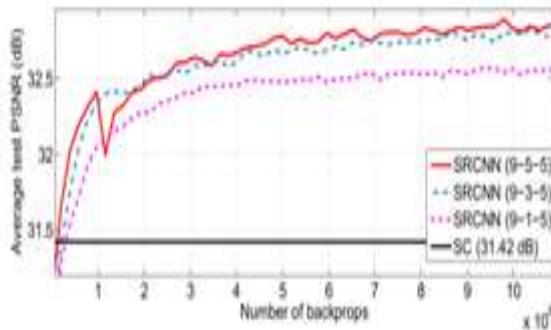
$$L(\Theta) = \frac{1}{n} \sum_{i=1}^n \|F(Y_i; \Theta) - X_i\|^2 \quad (4)$$

Here, n is the number of training samples. This technique just takes the mean of the square of the difference of the predicted and the ground truth values. PSNR (Peak signal-to-noise ratio) is a widely used metric for measuring the restoration quality of the image [5]. PSNR is partially related to the perceptual quality of the image generated so, it gives us an option to make the model adapt

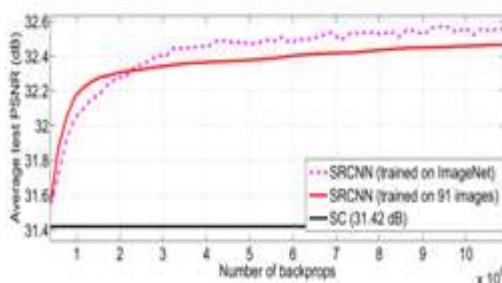
to this metric. With the mean squared loss function, a high PSNR values are obtained. As the model is trained for a higher PSNR value the model achieves satisfactory results when evaluated with metrics like SSIM(Structural Similarity Index). The model can be further optimized and the loss function can also be further minimized by use of stochastic gradient descent along with standard backpropagation technique. Stochastic gradient is being used because it highly optimizes the training time and makes the convergence faster. Here in stochastic gradient, the weights of the network are updated as follows:

$$\Delta_{i+1} = 0.9 \cdot \Delta_i - \frac{\eta \cdot \partial L}{\partial W_i}, \quad W_{i+1}^l = W_i^l + \Delta_{i+1} \quad (5)$$

Now, for the comparative analysis and inference of the model hyperparameter tuning is done to check its performance. This deep learning architecture work efficiently with a huge data set, but here for comparative analysis, a smaller data set containing 91 high resolution and a larger dataset of 395,909 images



from ILSVRC 2013 ImageNet detection training partition have been used. In the training phase, the input images are taken and smaller $f_{\text{sub}} \times f_{\text{sub}} \times c$ pixel sub-images are randomly cropped from them. The sub-images are preferred over patches because



they do not require any averaging or normalization as the post-processing. In order to arrange the low-resolution images (input images), A Gaussian kernel is applied on the high-resolution image to make it blurry, and then subsampling is done by an upscaling factor and then it is upscaled by the same factor using

bicubic interpolation, then this input is fed to the network. The size of the sub-images used for training is $f_{\text{sub}} = 33$, Here the dataset of 91 images are divided into 23,800 sub-images, these are extracted from the actual original images with the help of stride of 14. Now hyper parameter tuning is performed and tradeoff can be examined between model performance and the training speed, also try to derive a relation between them. The defaults of the networks as stated in the work of Chao Dong et al [2]. is set as $f_1 = 9, f_2 = 1, f_3 = 5, n_1 = 64, n_2 = 32$.

In the tradeoff shown in figure 2, the model is observed as how fast it can converge with different datasets. Now tuning the [2] filter number and studying the behaviour of model shows that by sacrificing the training time of the model, it can achieve better results by increasing the width of the network or by increasing the number of filter. As stated in the work of Chao dong et al. [2], defaults set are $f_1 = 9, f_2 = 1, f_3 = 5, n_1 = 64, n_2 = 32$, two experiments have been conducted and the results are shown in figure 3.

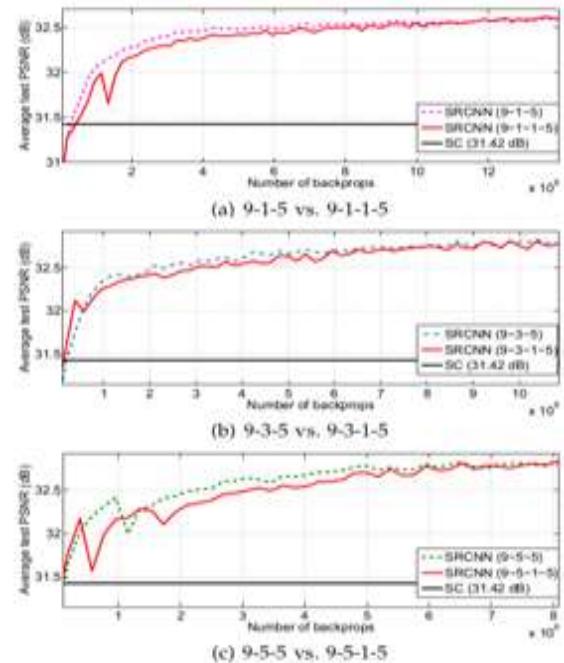


Fig 2: The tradeoff obtained as shown in work of Chao Dong et al [2].

First with the larger network with $n_1 = 128$ and $n_2 = 64$.

Second with the smaller network as $n_1=32$ and $n_2=16$.

The results obtained will backup that statement that by increasing the width of the network the performance of the model increases.

$n_1 = 128$		$n_1 = 64$		$n_1 = 32$	
$n_2 = 64$	$n_2 = 32$	$n_2 = 16$			
PSNR	Time (sec)	PSNR	Time (sec)	PSNR	Time (sec)
32.60	0.60	32.52	0.18	32.26	0.05

Fig 3: The results obtained as mentioned in the work of Chao Dong et al [2].

Now, the filter size is tuned [2] and the model's sensitivity to the filter size and performance are examined. In the previous experiments, the chosen filter size is $f_1 = 9$, $f_2 = 1$, and $f_3 = 5$, and the network could be denoted as 9-1-5. To be consistent with the sparse coding based techniques the size of the middle filter is kept as 1 and the other two filters are tuned to $f_1 = 11$ and $f_3 = 7$ (denoted as 11-1-7) and keeping all other factors the same, upscaling has been performed with a factor 3, the results achieved are 32.57 dB, which is higher and better than the model's performance when using the actual parameters. This proves that the model with a larger filter can capture finer structural details of the input image. Experiments have been conducted by enlarging the middle filter i. 9-3-5 and ii. 9-5-5. The convergence curves, as shown in figure 4, show that a larger filter size can significantly improve the quality of the output image and the PSNR values obtained in i. and ii. are 32.66dB and 32.75 dB respectively. Making use of the neighborhood information can be very helpful in the mapping stage of the model. If the model's width is further increased its deployment time increases as well as the training time.

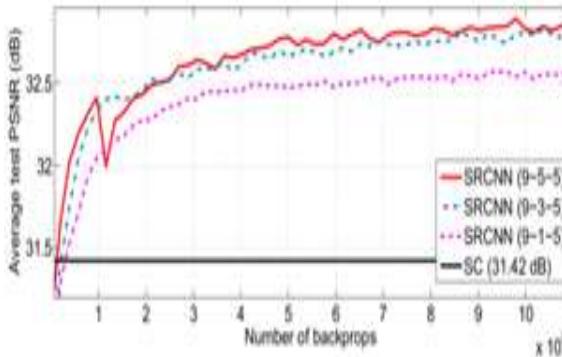


Fig 4: The tradeoff results shown in work of Chao Dong et al [2].

The sensitivity of the model to the number of layers has also been studied in the work of Chao Dong et al. [2]. Work by He and Sun [6] clearly tells us that the Convolutional Neural Network can benefit by increasing the number of hidden layers. The model is also tested by adding a non-linear mapping layer in between, which has $n_{22} = 16$ filter with size $f_2 = 1$. While evaluating the models (i.e., 9-1-1-5, 9-3-1-5, 9-5-1-5), the initialization scheme and learning rate of the added layer are kept the same as the

default. From the convergence graphs shown in figure 5, the models are taking a longer time to converge, but given time these new models gradually catch up and converge. So, increasing the depth of the network in the super-resolution domain might not yield better results.

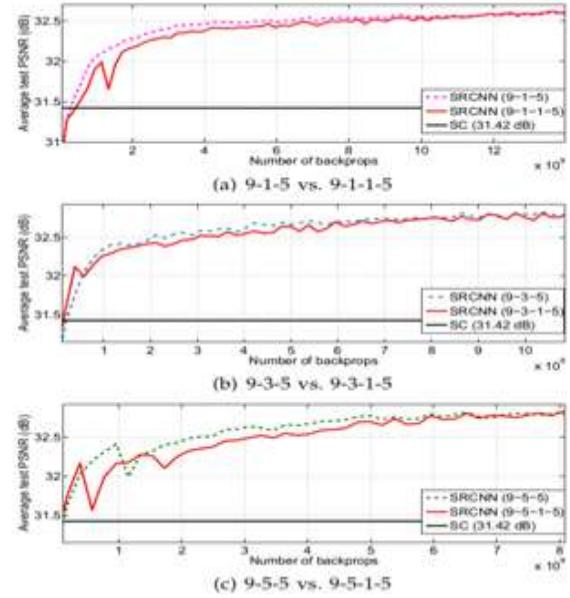


Fig 5: (a), (b), (c) shows the comparisons between three layer and four-layer networks as shown in the work of Chao Dong et al [2].

D. SRResNet and SRGAN

Even though there has been a breakthrough in the efficiency, accuracy, and speed of the single image super resolutions which have been achieved through faster and deeper convolutional neural networks one caveat still lingers, that is the loss of finer texture details and minute important parts of the image when upscaled with a bigger scaling factor. The mainstream traditional CNN's have been trying to improve the resolution by minimizing loss functions when upscaled like mean squared error, but this lacked high-frequency details and would not yield satisfactory results when being upscaled. The generative models have been bringing a breakthrough in the deep learning problems, So in the work of [3] a Generative Adversarial Network-based super-resolution model has been proposed to tackle the problem mentioned above. This SR-GAN is the first-ever architecture to achieve the state of the art results even when the image is upscaled by the factor of 4. Extending the previous discussions of loss functions and their importance further, a new loss function named perceptual loss is proposed which is a combination of adversarial loss and content loss. Initially an SRResNet model has been developed from optimizing the previous SRCNN model which generates realistic images, to improve this further

another neural network is added to the SRResNet model together to form a GAN, which outperforms the SRResNet and SRCNN models.

1. SR ResNet: After the unsatisfactory results of interpolation methods there was a need for the predictive models, then came the CNN which learned the end to end mapping from the input image to the output, even though it is a state of the art technique it failed to retain certain crucial and finer structural information. Then came a necessity to develop an even deeper model with [3] residual and skip connections so that the finer details could be retained properly. Thus came this [3] SR ResNet model in the work of Christian Ledig et al [3]. This SR ResNet model is optimized for the Mean Squared Error which is as shown below :

$$l_{MSE}^{SR} = \frac{1}{r^2 WH} \sum_{x=1}^{rW} \sum_{y=1}^{rH} \left(I_{x,y}^{HR} - G_{\theta_G}(I_{x,y}^{LR}) \right)^2 \quad (6)$$

G denotes the generator function which can generate high resolution image from the low resolution input. ImageNet dataset which is a collection of 350k images has been chosen to train the ResNet model. The architecture is named as Generator in the figure 6. The SRGAN and SR ResNet uses the same generator architecture, but in SRGAN neural network named discriminator comes into the picture which classifies the images as real or fake. Other than that everything else remains same.

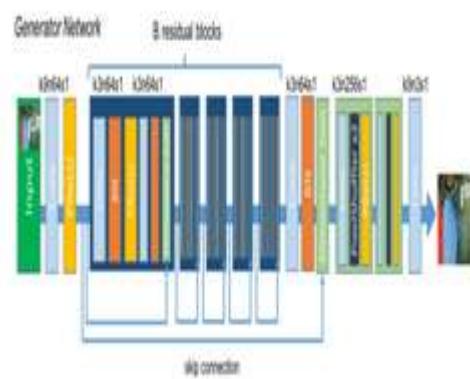


Fig 6: The Generator architecture as designed in the work of Christian Ledig et al [3].

As the previous Models used a shallow network it could not catch finer details so here a deeper denser model has been proposed which contains a B number of residual blocks, those blocks are bypassed by skip connections. These skip connections have been introduced to relieve the networks from modeling the identity transformation.

The Generator model is proposed in the form of block layout as suggested in the work of Johnson et al. [8], finer details of the picture are spotted and retained using two convolutional layers which contain small 3×3 filters and 64 feature maps which are then followed by batch normalization layers (which help in faster convergence, lesser complexity) and Parametric ReLU activation function. Then the subpixel convolutional method is used to upscale the feature maps effectively. Choosing the right number of residual blocks plays an important role in the performance of the model. In the work of Christian Ledig et al. [3] the author has tried to tune the number of residual blocks, and the experiments showed that the more the number of these residual blocks, more is the more efficient and better are the output results, and also these skip connections help the network to converge faster and also help in the ease of complexity of the network. Then for the scope of this work, 16 is chosen as the right number of residual blocks, because it is giving off a good trade-off between the time, computational complexity, and model performance.

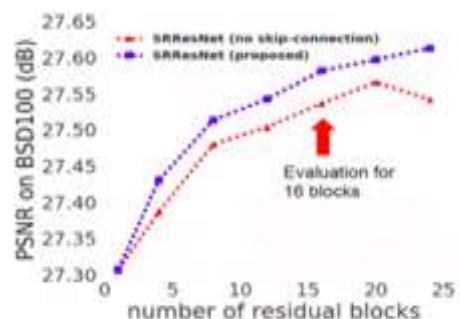


Fig 7: the trade off between number of layers and models performance as stated in the work of Christian Ledig et al. [3]

Even though the quality of the images has been improved and enhanced, compared to the interpolation techniques, still the images look somewhat artificial and not up to the mark. This is because of the optimization over the mean squared error. MSE is not the best optimizer because there can be many distorted images but evenly matched concerning the mean squared error. A GAN based model tries to overcome this caveat in which the generator model remains the same but another neural network named discriminator will be introduced to the pipeline and a new loss function is devised to overcome the drawbacks of MSE.

2. SRGAN: First let us understand what are GANs, GANs are generative model architecture introduced by Ian Goodfellow in 2014. Generative Adversarial Networks are the latest trending topic in deep learning which managed to solve many complex problems that seemed

very complex for the traditional deep learning techniques. Here the basic working of the GAN is explained. GAN is a neural network architecture where 2 neural networks are used instead of one, where one is the generator and the other is the discriminator. As the name suggests the Generator tries to generate random samples and gives them to the discriminator, the job of the discriminator is to check and tell whether the generated image is real or fake. The generator tries to prepare a meaningful distribution from the random noise and the discriminator tries to classify it as real or fake, these networks work in an adversarial environment i.e. they compete against each other, and they keep on getting better. There are pros and cons of using generative adversarial networks, the best things about using a GAN is perceptual loss function is the main optimizer, instead of a traditional MSE. But, GAN's are very sensitive to the hyperparameter tuning, and there is another concept called Mode collapse where the generator only generates certain class samples this generally occurs due to imbalanced classes. In the training phase the low-resolution images obtained by applying a gaussian filter to the high-resolution image, then it is downsample by a factor of r. Now, our goal reduces down to restoring this degraded image into a high-resolution image denoted as ISR which is as close as possible to its respective high resolution version. The actual high-resolution image is denoted as IHR and ILR are the low-resolution equivalents that are obtained by performing the gaussian filter and other operations mentioned above on IHR. So considering an input with C number of color channels, the ILR can be represented as a real-valued tensor with the dimensions $W \times H \times C$ and IHR, ISR can be denoted by $rW \times rH \times C$ respectively. In the work of Christian Ledig et al. [3] a generator function G is devised such that it estimates a Super Resolved and upscaled image given a Low-Resolution image. To tackle this [3] has proposed a feed-forward Convolutional Neural Network (G θ G) as a generator, and the parameters would be {W1:L ; B1:L} where W and B denote the weights and biases of an L layered deep neural network. The perceptual loss function used here would be used to optimize the network. The generator function in this work of Christian Ledig et al. [3] is as below:

$$\hat{\theta}_G = \arg \min_{\theta_G} \frac{1}{N} \sum_{n=1}^N l^{SR}(G_{\theta_G}(I_n^{LR}), I_n^{HR}) \quad (7)$$

In this work, the special loss function named perceptual loss is derived which is a weighted combination of various loss components like adversarial loss, content loss, etc, these individual

loss components help the model to recover the distinct desirable characters. The generator network is same as the network used in SRResNet which consists of 16 residual blocks and also skip connections, and with the proposal of GANs by Ian Goodfellow et al. [9] a discriminator network D θ D is introduced in the framework. With the definition of GAN devised as a mini max problem in [9], it is even used in this architecture and the mathematical formulation is given as G θ G:

$$\begin{aligned} \min_{\theta_G} \max_{\theta_D} & \mathbb{E}_{I^{HR} \sim p_{train}(I^{HR})} [\log D_{\theta_D}(I^{HR})] + \\ & \mathbb{E}_{I^{LR} \sim p_G(I^{LR})} [\log (1 - D_{\theta_D}(G_{\theta_G}(I^{LR})))] \end{aligned} \quad (8)$$

Now coming to the Adversarial Architecture, As mentioned the main aim of the architecture is to develop a Generative model G whose aim is to try to bypass or fool the discriminator D which tries to classify whether the generated images are real or fake. With the help of this methodology, the model G would learn to generate the images that are very similar to the ground truth to get the acceptance of discriminator D, in a similar fashion, the discriminator D would learn to accept the solutions that are very close to the ground truth only, instead of some intermediate and half-hearted results. Due to this technique the output obtained are very satisfactory and very close to the ground truth, which opposite to the solutions that are yielded by minimizing pixel-wise mean squared error approach. The architecture of the Generator G remains the same as that of the SR ResNets consisting of 16 residual blocks, having intermediate skip connections, and usage of 2 convolutional layers with small 3x3 filters and 64 feature maps, then followed by batch norm layers and Parametric ReLU activation layer. Now coming to the architecture of Discriminator, it is designed by following the principles set by Radford et al.[10] and use Leaky-ReLU activation, with the learning rate as 0.2 and avoiding max-pooling throughout the model. The Discriminator is developed to solve the maximization problem. The Discriminator is designed with 8 convolutional layers to catch the features with an increasing number of 3 x 3 filter kernels, the increasing factor would be 2 and it is increased from 64 to 512 kernels similar to the VGG network, where the convolution size is kept the same and the kernel size remains the same among the blocks but in between the blocks the kernel size keeps on increasing by a factor of 2, starting from 64 it would keep increasing till 512. With the help of strided convolutions, the image resolution decreases each time the features get doubled. Then finally 512 feature maps are followed by 2 dense layers and a final sigmoid activation function to classify whether the image is real or fake.

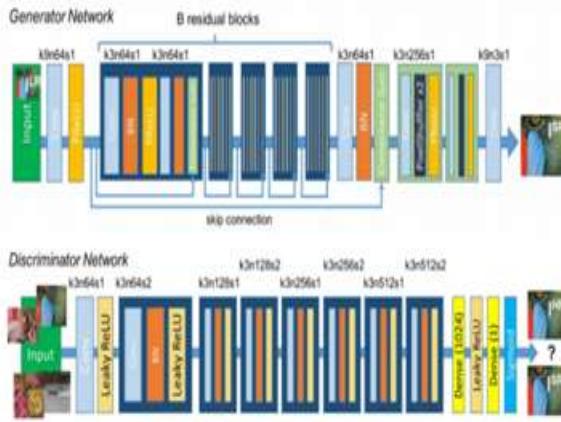


Fig 8: Architecture of GAN as stated in work of Christian Ledig et al. [3]

Now coming to the loss functions used in this architecture. A need for a new loss function I^{SR} has arrived due to failure of MSE hence, the authors of this work have proposed a new perceptual loss function which is very essential for the performance of the generator. To improve over the MSE loss function, with the help of the work of Johnson et al. [8] and Bruna et al. [11] and perceptual loss is devised which can assess the solution concerning perceptually significant characteristics or features. The perceptual loss is derived as the weighted sum of content loss and an adversarial loss. The loss function used in this architecture is given by [3].

$$I^{SR} = \underbrace{I_X^{SR}}_{\text{content loss}} + \underbrace{10^{-3} I_{Gen}^{SR}}_{\text{adversarial loss}} \quad (9)$$

perceptual loss (for VGG based content losses)

Let us first discuss about the content loss, the pixel wise MSE loss is calculated as shown in the previous SR ResNet loss function equation, and this would be the most widely used optimization. Even though achieving good PSNR values the output often lacks in high frequency content which leads to blurry and smooth images. So, instead of relying on pixel wise MSE error as stated in the work of Christian Ledig et al. [3], VGG loss function is devised, which is based up on the ReLU activation function of VGG-19 architecture. In the perceptual loss function we consider the Euclidean distance which refers to the distance between the actual referenced image I^{HR} and the upscaled image ($G(\theta_G)(I^{LR})$) and it is formulated as :

$$I_{VGG/i,j}^{SR} = \frac{1}{W_{i,j}H_{i,j}} \sum_{x=1}^{W_{i,j}} \sum_{y=1}^{T_{i,j}} \left(\phi_{i,j}(I^{HR})_{x,y} - \phi_{i,j}(G_{\theta_G}(I^{LR}))_{x,y} \right)^2 \quad (10)$$

Now discussing about the Adversarial Loss, it tries to bias our model to produce the images that

are close to or lie in photo realistic images, by trying to pass by the discriminator. It is based on the probabilities of the discriminator.

$$I_{Gen}^{SR} = \sum_{n=1}^N -\log D_{\theta_D} \left(G_{\theta_G}(I^{LR}) \right) \quad (11)$$

Here, $D_{\theta_D}(G_{\theta_G}(I^{LR}))$ means the probability that the reconstructed image($G_{\theta_G}(I^{LR})$) is a photo realistic image. After examining the network, its architecture and working now, the training process and data preparation process needs to be studied. Using the data set of ImageNet which contains about 350 thousand images, the model is trained on NVIDIA Tesla M40 GPU. The low-resolution images are obtained from downscaling the high-resolution images with the factor of $r = 4$ using bicubic kernel. [3] For each mini-batch 16 random 96 x 96 High resolution sub images (the reason why the sub images are used instead of patches are mentioned above) of distinct training images are taken. For the SRResNet the learning rate is set to 10-4 and 106 update iterations, while the SRGANs are trained with 105 update iterations with the learning rate of 10-4.



Fig 9: The comparision of SRResNet, SRGAN results as portrayed in the work of Christian Ledig et al. [3]

III. Comparison of SISR Techniques

In the work of [3], the Mean Opinion Score(MOS) has been used as the test to check the ability of various techniques to upscale the images. [3] has used 26 raters and 100 image samples making 2600 samples for each method and the results are shown in Figure 10.

Set5	nearest	bicubic	SRCNN	SelfExSR	DRCN	ESPCN	SRResNet	SRGAN	HR
PSNR	26.26	28.43	30.07	30.33	31.52	30.76	32.05	29.40	∞
SSIM	0.7552	0.8211	0.8627	0.872	0.8958	0.8784	0.9019	0.8472	1
MOS	1.28	1.97	2.57	2.65	3.26	2.89	3.37	3.58	4.32
Set14									
PSNR	24.64	25.99	27.18	27.45	28.02	27.66	28.49	26.02	∞
SSIM	0.7100	0.7486	0.7861	0.7972	0.8074	0.8004	0.8184	0.7397	1
MOS	1.20	1.80	2.26	2.34	2.84	2.52	2.98	3.72	4.32
BSD100									
PSNR	25.02	25.94	26.68	26.83	27.21	27.02	27.58	25.16	∞
SSIM	0.6606	0.6935	0.7291	0.7387	0.7493	0.7442	0.7620	0.6688	1
MOS	1.11	1.47	1.87	1.89	2.12	2.01	2.29	3.56	4.46

Fig 10: Colour-coded distributions of MOS scores on BSD100 as shown in the work of Christian Ledig et al. [3]

The performance of various techniques mentioned above are tabulated which are devised in the work of [3]. It is to be noted that all of the data has been recorded using benchmark datasets and considering upscaling factor as 5

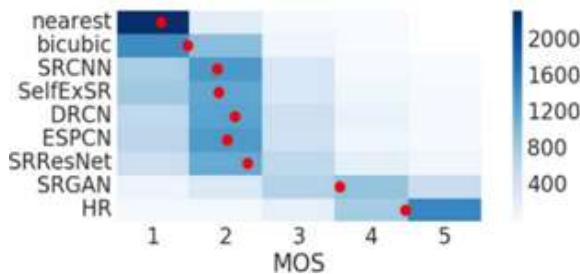


Fig 11: Comparison of various techniques on the benchmark datasets as deduced int the work of Christian et al.[3] .

All the results and outputs of above discussed techniques are tabulated in the figure 11 with respect to various performance metrics, and we can easily say which technique is more efficient one. This helps in the technique selection for super resolution of a particular image.

IV. Conclusion

In this paper the single image resolution techniques such as Nearest Neighbors interpolation, Bicubic interpolation, super resolution Convolutional Neural Network, super resolution residual networks and super resolution generative adversarial networks are reviewed, along with their working principles, advantages and limitations. From the discussion it is found that nearest neighbor interpolation approach is simple and easiest method among them. While the interpolation techniques bi-cubic interpolation is one of the efficient and effective method, and due to this it is the most famous interpolation method. And then the predictive models such as SRCNN, SRResNet and SRGAN has taken the spotlight due to their remarkable results as mentioned above.

References

- [1] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *nature*, vol. 521, no. 7553, p. 436, 2015.
- [2] Dong, C. C. Loy, K. He and X. Tang, "Image Super-Resolution Using Deep Convolutional Networks," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 38, no. 2, pp. 295-307, 1 Feb. 2016, doi: 10.1109/TPAMI.2015.2439281.
- [3] Ledig et al., "Photo-Realistic Single Image Super-Resolution Using a Generative Adversarial Network," 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Honolulu, HI, USA, 2017, pp. 105-114, doi: 10.1109/CVPR.2017.19.
- [4] Gavade, Anil & Sane, Prasana. (2013). SUPER RESOLUTION IMAGE RECONSTRUCTION BY USING BICUBIC INTERPOLATION. 10.13140/RG.2.1.4909.0401.
- [5] C.-Y. Yang, C. Ma, and M.-H. Yang. Single-image super-resolution: A benchmark. In European Conference on Computer Vision (ECCV), pages 372–386. Springer, 2014.
- [6] He, K., Sun, J.: Convolutional neural networks at constrained time cost. arXiv preprint arXiv:1412.1710 (2014).
- [7] Rukundo, Olivier & Cao, Hanqiang. (2012). Nearest Neighbor Value Interpolation. International Journal of Advanced Computer Science and Applications. 3. 25:30. 10.14569/IJACSA.2012.030405.
- [8] J. Johnson, A. Alahi, and F. Li. Perceptual losses for real-time style transfer and super- resolution. In European Conference on Computer Vision (ECCV), pages 694–711. Springer, 2016.
- [9] Goodfellow, Ian J., et al. "Generative Adversarial Networks." ArXiv:1406.2661 [Cs, Stat], June 2014. arXiv.org, <http://arxiv.org/abs/1406.2661>.
- [10] Radford, L. Metz, and S. Chintala. Unsupervised representation learning with deep convolutional generative adversarial networks. In International Conference on Learning Representations (ICLR), 2016.
- [11] J. Bruna, P. Sprechmann, and Y. LeCun. Super-resolution with deep convolutional sufficient statistics. In International Conference on Learning Representations (ICLR), 2016

A Review: Image Synthesis from Textual Descriptions using GANs

Srinivas Pavan

Department of Computer Science,
Chaitanya Bharathi Institute of Technology,
Hyderabad-500075, India.
srinivaspavan05@gmail.com

Varun Sundaram

Department of Computer Science,
Chaitanya Bharathi Institute of Technology,
Hyderabad-500075, India.
vaasha99@gmail.com

Dr. K. Sagar

Department of Computer Science,
Chaitanya Bharathi Institute of Technology,
Hyderabad-500075, India.
ksagar_cse@cbit.ac.in

Abstract: One of the evolving areas of interest in the field of generator networks is generating images from text using generative adversarial networks(GAN's). Generating realistic images from textual description have been advancing over the past few years and the images are getting more realistic with progressing generative models. Images generated by GAN's range from images of flowers to images of human faces that are generated from fusing the features described in the text. A lot of research has gone into this task and a lot of progress can be seen. In this paper, we will look at the improvement from the very first text to image synthesis with GAN-INT-CLS to the surreal images produced by TediGAN.

I. Introduction

The advancement in generative networks over the past 5 years has been immense. This can be mostly accredited to different approaches used by different models. From a simple generative adversarial network to the same network with different modules, the improvement is transparent and can be seen as a huge leap towards success. Generating images from mere textual description shows the advancement of technology and opens up more possibilities. The thought of creating images by fusing the desired features opens doors for many possibilities and shows how powerful GAN's [1] could be. In this process, user gives a textual description of the image he wants to generate. Important features are extracted from this textual description and an image is generated containing the features described. This image is then enhanced to become a bit more realistic. This enhancing involves softening the edges, adjusting the colours to make the image colours look more uniform. The final image generated is now an image that looks realistic and also satisfies the given description. This is achieved through Generative Adversarial Networks or GANs are unsupervised learning algorithms that produce complex outputs from simple inputs such as text and producing an image as an output. GANs are generative models that consists of two deep learning components that compete with each other. One of the

components is a generator that tries to produce realistic outputs based on fine-tuned constraints and conditions, the other component is a discriminator which tries to classify these outputs as real or fake. The main goal of a generator can be viewed as to trick the discriminator into believing that the output generated is real and the goal of a discriminator would be to not get deceived. This approach is used in generating images where the discriminator is fed with real images and the generator generates synthesized images. The synthesized images are sent to the discriminator which then asks the generator to improve the image quality if the image does not look realistic. In this process, the final synthesized images generated look a bit more realistic and is indistinguishable to the human eye.

II. Literature Survey

A. GAN-INT-CLS

This was one of the first attempts to translate human given textual descriptions to actual images which is synthesizing images which are indistinguishable to human eye from the features given in the text.

Text:	Generated Images
A blood colored pistil collects together with a group of long yellow stamens around the outside.	
The petals of the flower are narrow and extremely pointy, and consist of shades of yellow, blue	
This pale peach flower has a double row of long thin petals with a large brown center and coarse lob.	
The flower is pink with petals that are soft, and separately arranged around the stamens that has pi.	
A one petal flower that is white with a cluster of yellow anther filaments in the center	

Fig 1: Images produced by GAN-INT-CLS

Generative Adversarial Network(GAN) [1,18] with a layer of CNN were used for Image Synthesis conditioned to image features embedded in the textual descriptions. The model is trained with a

deep convolutional generative adversarial network (DC-GAN) [8] where the descriptive features of the images from the text are supplied through an encoded feature vector given by a well-trained convolutional-recurrent neural network. The entire model pushes both the sub models to perform feed-forward inference constrained by the text features.

Model	Inception Score (IS)	
GAN-INT-CLS	CUB	$2.88 \pm .04$
	COCO	$7.88 \pm .07$

Table 1: Inception score (IS) obtained for GAN-INT-CLS [10] on COCO [2] and CUB [3] datasets

The images synthesized can easily be distinguished by human eye from a real image. Although this model was able to generate images depicting the textual description to an extent, the images produced were seldom noisy and fuzzy. This made the model perform poor in terms of inception score and human rank.

B. STACK-GAN:

Stack-GAN [11] also known as Stacked GAN, as the name suggests stacks two stages of image synthesis and refinement to generate photo realistic images compared to its predecessor vanilla GAN [10] or GAN-INT-CLS. Stack GAN consists of two stages

Stage-I GAN: In this step, a low-resolution image is obtained by creating a basic layout containing the shape and base colours of the image.

Stage-II GAN: In this step, the generated low-resolution image is enhanced by correcting the incorrect features. The final generated image would be a realistic image depicting the desired features in the textual description.



Fig 2: Images generated using StackGAN for a description of "This flower has overlapping pink pointed petals surrounding a ring of short yellow filaments"

Though the model is about to perform well by synthesizing photo-realistic images compared to its predecessor there are few drawbacks with this model that include noise in the background layout of the object in the image. We can observe a decrease in the inception score when the size of the synthesizing image is reduced.

Model	Inception Score (IS)	
GAN-INT-CLS	CUB	$2.88 \pm .04$
	COCO	$7.88 \pm .07$
StackGAN	CUB	$3.70 \pm .04$
	COCO	$8.45 \pm .03$

Table 2: Comparison of Inception Scores (IS) [7] of GAN-INT-CLS and Stack- GAN

C. AttnGAN:

AttnGAN [13] proposed a novel method of using a two component system where an attentional generative network and a deep attentional multi-modal similarity model are used. Attentional Generative network tries to focus on sub regions in the image taking the textual description portraying particular areas of the image into account, instead of taking the entire sentence as a whole. This ultimately gives significance to certain words that actually contribute to the features in the final output. AttnGAN tries to identify different features in the text and synthesize the image based on the identified features.



Fig 3: Images generated by AttnGAN

Though the AttnGAN is able to generate photo realistic images focused on a particular category of subject/object, it showed poor performance in generating images depicting real-life situations.

Model	Inception Score (IS)		FID	
	CUB	COCO	CUB	COCO
GAN-INT-CLS	2.88 ± .04	7.88 ± .07	CUB	COCO
	7.88 ± .07	8.45 ± .03	-	-
StackGAN	3.70 ± .04	4.36 ± .03	CUB	COCO
	4.36 ± .03	23.98	-	-
AttnGAN	4.36 ± .03	25.89 ± .47	CUB	COCO
	25.89 ± .47	35.49	-	-

Table 3: Comparison of IS and FID [7,9] for GAN-INT-CLS, StackGAN and AttnGAN

D. DM-GAN:

DM-GAN [15] tried to solve the two of the main issues that the previous models could not solve. The first problem was that most of the previous methods depended mostly on the initial image quality. If the initial image quality is low, the later image refinement will hardly get refined and sometimes even end up giving a fuzzy image. The second problem is that unique words possess unique level of importance when depicting different image components, however, the same text representation is used in current image refinement process.

This model contains two stages namely initial image generation and dynamic memory based image refinement [15].

In the first stage which is initial image generation face, the text encoder is used to transform the textual description into sentence features and word features. Using these features, a rough image is generated containing the important features of the textual description. This is the initial image produced by the primary stage.

In the next stage, the image refinement stage uses a dynamic memory approach where more granular visual features are added to the previously generated fuzzy images to generate a photo realistic image and this refinement process can be repeated as many times as needed.

This bird has wings that are grey and has a white belly. This bird has wings that are black and has a white belly. This is a grey bird with a brown wing and a small orange beak. This bird has a short brown bill, a white eyering, and a medium brown crown. This bird has a white throat and a dark yellow bill and grey wings. This particular bird has a belly that is yellow and brown. This bird is a lime green with greyish wings and long legs. This yellow bird has a thin beak and jet black eyes and thin feet.



Fig 4: Images generated by DM-GAN

Though DM-GAN outperforms all of the previous models the final results still rely heavily on the layout of multi-subjects in initial images [10,11,15].

Model	Inception Score (IS)		FID	
	CUB	COCO	CUB	COCO
GAN-INT-CLS	2.88 ± .04	7.88 ± .07	CUB	COCO
	7.88 ± .07	8.45 ± .03	-	-
StackGAN	3.70 ± .04	4.36 ± .03	CUB	COCO
	4.36 ± .03	23.98	-	-
AttnGAN	4.36 ± .03	25.89 ± .47	CUB	COCO
	25.89 ± .47	35.49	-	-
DM-GAN	4.75 ± 0.07	30.49 ± 0.57	CUB	COCO
	30.49 ± 0.57	32.64	-	-

Table 4: Comparison of IS and FID of DM-GAN with other models

E. DF-GAN:

DF-GAN [16] tries to tackle 3 main problems which are persistent in its predecessor. The first problem is that for the backbone, there are multiple generators and discriminators stacked for generating different scales of images making the training process slow and inefficient. Secondly, for semantic consistency, the existing models employ extra networks to ensure the semantic consistency increasing the training complexity and bringing an additional computational cost. Finally, for the text-image feature fusion method, cross-modal attention is only applied a few times during the generation

Process due to its computational cost impeding fusing the text and image features deeply [16]. DF-GAN has solved these problems by using a single set of generator and discriminator to synthesize high quality images directly by implementing a simplified text-to-image model. DF-GAN uses an innovative regularization method called Matching-Aware zero-centered Gradient Penalty [16] which encourages the generator to synthesize more realistic images that consistently comply to the given descriptions in the text, without introducing extra networks. The fusion module called Deep Text-Image Fusion Block exploits the semantics of text descriptions effectively and fuse text and image features deeply during the generation process.

F. Tedi-GAN:

Tedi-GAN [17] is the most recent model and has the best resolution of 10242. This model has generated the most photo-realistic images when compared to all of the previous models, especially when compared to DM-GAN. This model is very efficient and fast as it lacks gated memory module [15,17]. Moreover, Tedi-GAN can take not only text but labels and even sketches as inputs and create an image that resembles that sketch or depicts that label. This model comprises three modules which are StyleGAN inversion module [14], visual-linguistic similarity learning, and instance-level optimization. These modules carry



Fig 5: Images generated by DF-GAN trained on CUB dataset

Model	Inception Score (IS)		FID	
	CUB	COCO	CUB	COCO
GAN-INT-CLS	2.88 ± .04	7.88 ± .07	CUB	-
	-	-	COCO	-
StackGAN	3.70 ± .04	8.45 ± .03	CUB	-
	-	-	COCO	-
AttnGAN	4.36 ± .03	25.89 ± .47	CUB	23.98
	-	-	COCO	35.49
DM-GAN	4.75 ± 0.07	30.49 ± 0.57	CUB	16.09
	-	-	COCO	32.64
DF-GAN	4.86 ± 0.04	-	CUB	19.24
	-	COCO	-	28.92

Table 5: Comparison of IS and FID of DF-GAN with its predecessors

their own responsibilities. The StyleGAN inversion module learns the inversion where an image encoder maps a real image to the latent space. The second visual-linguistic similarity module learns linguistic representations that are persistent with the visual representations by projecting them into the same latent space that has the image encoder from the first module. The task of the third instance-level optimization module is to change only the required features and maintain the identity of the image as a whole.



Fig 6: Comparison of images generated by different models trained on CelebA-HQ dataset [4]

Table 6: FID for TediGAN

Model	FID	
	CelebA	Non-CelebA
TediGAN	107.25	135.47

III. Result Analysis

A. Performance Metrics

To assess the visual quality of images generated by the generator of a generative adversarial network, evaluation metrics such as Inception Score (IS) and Fréchet inception distance (FID) [7,9] are used. These metrics give a reliable perception of the quality of images and tell how close they are to being photo-realistic.

- 1. Inception Score (IS):** Inception Score was the first attempt to remove the subjective human evaluation of images synthesized by GANs [7]. Inception score involves using a pre-trained deep learning neural network model for image classification to classify the generated images. The lowest value of IS is 1.0 and the highest value depends on the number of classes the model classifies the images into, which again depends on the dataset chosen. In case of the Inception v3 model, the model supports 1000 classes of the ILSVRC 2012 dataset [19] and as a result the highest possible IS for this dataset is 1000.
- 2. Fréchet inception distance (FID):** Unlike Inception Score(IS), which evaluates only the distribution of generated images, the FID compares the distribution of generated images [9] with the distribution of real images that were used to train the generator. The lower the FID score the better the synthesized image.

B. Discussion

Text to image synthesis models have come a long way from producing fuzzy images to generating almost perfect images. These images have almost all the features described in the textual data and the clarity of these images have also improved a lot. The very first model for text to image synthesis that is the GAN-INT-CLS which was published in 2016 generated images that have very low clarity and can be easily identified by human eye as a synthesized image. These images did not produce great results but managed to do the job partly by generating an image with few of the features described in the textual description. This model was implemented on the CUB, COCO datasets and had inception scores of 2.88 on the CUB dataset and 7.88 on the COCO dataset. It's successor, StackGAN had significant improvement in terms of inception score showing an increase to 3.70 from 2.88 on the CUB dataset and an increase to 8.45 from 7.88 on the COCO dataset. Although these results seem to be a drastic improvement, the images produced were not that pleasing to the human eye. While the images produced by StackGAN were better than images generated by the previous GAN-INT-CLS model, the

images seemed to be fused and not so natural. After further improvements, AttnGAN model was proposed for text to image synthesis. This model produced some pleasing results with an inception score of 4.36 on the CUB dataset and 25.89 on the COCO dataset. This model drastically outperformed the previous StackGAN model on the COCO dataset showing a huge increase by almost 175%. Images produced were good but not perfect. They looked a bit more natural but when taken a closer look, the edges of the features seemed to be a bit fuzzy and looked non-uniform. The following model DM-GAN used a different approach by adding memory gates and using those gates to store and retrieve valuable information in the process. This method proved useful and produced good and eye pleasing images. This showed an increase in the inception score from 25.89 to 30.49 on the COCO dataset and increase to 4.75 from 4.36 on the CUB dataset. This model produced more natural and uniform images and was difficult to distinguish the synthesized image from real images by a human eye. DM-GAN's successor DF-GAN was an improvement to the DM-GAN in terms of inception score showing an increment to 4.86 from 4.75 on the CUB dataset. The images produced by DF-GAN were more realistic and more natural. This uses a deep fusion approach so that the image generated is not completely dependent on the initial image. The novel TediGAN model shows surreal results and produces photo-realistic images. This was implemented on the CelebA and Non-CelebA datasets [4,5] and had FID's of 107.25 and 135.47 respectively. This model is the best model produced so far for text to image synthesis and outperforms all the other models creating almost perfect and natural images.

IV. Conclusion

Generating synthesized images from textual description using GAN's has seen a great improvement in terms of images generated and the features of the image depicting the text. Images produced by the novel TediGAN model seem to be the most realistic when compared to the previous models. However, there is room for improvement. When given a complex textual description, TediGAN does not produce accurate results which means that the image generated does not have all the features described in the text. TediGAN uses StyleGAN inversion techniques, however a latest model of StyleGAN2 has come out which can create even more photo-realistic images compared to its predecessor, StyleGAN2 even offers image enhancement techniques. Moreover, when given complex descriptions, the iterations taken to generate the final image increase thereby increasing the time taken to produce the result.

One of the problems that persist in almost every model is that the age of the person in the image is not precise. When asked to generate an image of a 50 year old man, the image generated is that of a middle aged man. This can be integrated with other models that contain the age adjustment feature and make this model a bit more accurate. This process can be further simplified to the user by taking user's speech and generating image from speech instead of prompting the user to enter the textual description.

References

- [1] [Ian J. Goodfellow et al., Generative Adversarial Networks (2014).]
- [2] Tsung-Yi Lin et al., Microsoft COCO: Common Objects in Context (2015).
- [3] Wah C., Branson S., Welinder P., Perona P., Belongie S. "The Caltech-UCSD Birds-200-2011 Dataset." Computation & Neural Systems Technical Report, CNS-TR-2011-001.
- [4] Liu, Z., Luo, P., Wang, X., & Tang, X. Deep Learning Face Attributes in the Wild (2015). In Proceedings of International Conference on Computer Vision (ICCV).
- [5] Gary B. Huang, Manu Ramesh, Tamara Berg, and Erik Learned-Miller. Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments. University of Massachusetts, Amherst, Technical Report 07-49, October, 2007.
- [6] Tero Karras, Timo Aila, Samuli Laine, and Jaakko Lehtinen. Progressive growing of GANs for improved quality, stability, and variation. In ICLR, 2018.
- [7] Barratt, Shane & Sharma, Rishi. A Note on the Inception Score (2018).
- [8] Alec Radford, Luke Metz, & Soumith Chintala. Unsupervised Representation Learning with Deep Convolutional Generative Adversarial Networks (2016).
- [9] Martin Heusel, Hubert Ramsauer, Thomas Unterthiner, Bernhard Nessler, and Sepp Hochreiter. GANs trained by a two time-scale update rule converge to a local Nash equilibrium. In NeurIPS, 2017.
- [10] Scott Reed, Zeynep Akata, Xinchen Yan, Lajanugen Logeswaran, Bernt Schiele, & Honglak Lee. Generative Adversarial Text to Image Synthesis (2016).
- [11] H. Zhang et al., "StackGAN: Text to Photo-Realistic Image Synthesis with Stacked Generative Adversarial Networks," 2017 IEEE International Conference on Computer Vision (ICCV), Venice, Italy, 2017, pp. 5908-5916, doi: 10.1109/ICCV.2017.629.
- [12] Zhang, Han & Xu, Tao & Li, Hongsheng & Zhang, Shaoting & Wang, Xiaogang & Huang, Xiaolei & Metaxas, Dimitris. StackGAN++: Realistic Image Synthesis with Stacked Generative Adversarial Networks (2017). IEEE Transactions on Pattern Analysis and Machine Intelligence. PP. 10.1109/TPAMI.2018.2856256.
- [13] T. Xu et al., "AttnGAN: Fine-Grained Text to Image Generation with Attentional Generative Adversarial Networks," 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, USA, 2018, pp. 1316-1324, doi: 10.1109/CVPR.2018.00143.
- [14] Tero Karras, Samuli Laine, & Timo Aila. A Style-Based Generator Architecture for Generative Adversarial Networks (2019).
- [15] Zhu, Minfeng & Pan, Pingbo & Chen, Wei & Yang, Yi. DM-GAN: Dynamic Memory Generative Adversarial Networks for Text-To-Image Synthesis (2019). 5795-5803. 10.1109/CVPR.2019.00595.
- [16] Ming Tao, Hao Tang, Songsong Wu, Nicu Sebe, Fei Wu, & Xiao-Yuan Jing. DF-GAN: Deep Fusion Generative Adversarial Networks for Text-to-Image Synthesis (2020).
- [17] Xia, W., Yang, Y., Xue, J.H., & Wu, B.. TediGAN: Text-Guided Diverse Face Image Generation and Manipulation (2020). In IEEE Conference on Computer Vision and Pattern Recognition (CVPR).
- [18] Jie Gui, Zhenan Sun, Yonggang Wen, Dacheng Tao, & Jieping Ye. A Review on Generative Adversarial Networks: Algorithms, Theory, and Applications (2020).
- [19] Olga Russakovsky, Jia Deng, Hao Su, Jonathan Krause, Sanjeev Satheesh, Sean Ma, Zhiheng Huang, Andrej Karpathy, Aditya Khosla, Michael Bernstein, Alexander C. Berg, & Li Fei-Fei (2015). ImageNet Large Scale Visual Recognition Challenge. International Journal of Computer Vision (IJCV), 115(3), 211-252.

A Survey on Speaker Diarization Techniques

Saad Ahmed

Department of Computer Science and Engineering
Chaitanya Bharathi Institute of Technology
Hyderabad-500075, India
saadahmed05999@gmail.com

M. Kalidas

Department of MCA
Chaitanya Bharathi Institute of Technology
Hyderabad-500075, India
mkalidas_mca@cbit.ac.in

Abstract: Making a report or maintaining activity in a diary is what the term “Diarize” implies, likewise keeping a list of “who spoke when” is known as Speaker diarization. To facilitate adaptive speaker computation, speaker diarization was used for speech recognition on audio recordings with multiple speakers. Now, it is more of a pre-processing step for many speech applications. With the rise of technology and development in Artificial Intelligence, deep learning, speaker diarization has gained popularity and is becoming a more popular area of interest. Remarkable progress in speaker diarization has taken place over the last decade due to groundbreaking developments and practices in speech application domains. In this paper, we examine different speaker diarization methods implemented using various technologies and compare the performance of each respectively. Also, the paper will discuss various methods that were combined in each implementation, leading to complement each other. This survey hopes to emphasize the technological trend and provide the community with valuable information, thus facilitating progress and versatility of speaker diarization.

Keywords: Speaker Diarization, DER, CALLHOME, UIS-RNN, LSTM

I. Introduction

The division of an audio recording into segments based on individual's speaker's identity is known as speaker diarization. Speaker Diarization is a necessary step in audio applications consisting of multiple speakers.

In the diarization process, the input is audio which is processed in a specific way. Generally, audio is separated and clustered into groups of speech segments. These results in labeling of the non-speech/speech shifts, speaker classification, speaker turn transitions. The approach may vary based upon the idea that is used to obtain results. Usually, no other data is required except the audio file. The input

Shaik Abdul Muqtadeer

Department of Computer Science and Engineering
Chaitanya Bharathi Institute of Technology
Hyderabad-500075, India
afraz99@gmail.com

Mohammed Zubair Ahmed

Department of Computer Science and Engineering
Chaitanya Bharathi Institute of Technology
Hyderabad-500075, India
zewbare@gmail.com

could be audio or visual transmissions from radio stations, interpersonal interactions, videos from social media sites or smartphones, corporate events, seminars, economic data.

Generally, speaker diarization systems are made up of separate modules, which can be broadly classified into four components; however, they may vary depending on the method employed. The first step is dividing the audio recording into segments and neglecting the parts which have no speech or audio signal in them. This is known as speech segmentation. The second step is the extraction of audio embeddings, in which unique features from the segmented sections are extracted, followed by cluster, where it is decided how many speakers are present. Finally, re-segmentation or refinement takes place, which is optional. Usually, each one of these sub-modules is designed separately.

This paper discusses diverse speaker diarization technologies like regional proposal network, LSTM, and various Artificial intelligence and Deep Learning methods. This paper reviewed some of the best survey papers in speaker diarization and discusses the evolution of speaker diarization with different approaches. The main criteria we used are based on how versatile each method is from another. However, we do not judge or bias any paper that we have taken into consideration. Nevertheless, if we consider Diarization Error Rate (DER), some have a slight benefactor over the other.

We briefly try to describe the approaches in each paper and make it easier for the readers to understand the elements used in the papers hence benefiting them by providing mature yet, could open up unprecedented opportunities to explore in the field of speaker diarization, it is evident how each paper came up with a novel method of its own and made recognizable efforts in creating more and efficient methods. Even though some methods might have comparatively lower score but, their definite aim was solving an existing problem. We have considered such papers to alleviating their contribution in the fields, which will help in future innovations. Yusuke

Fujita, Shinji Watanabe, Shota Horiguchi, Yawen Xue, Jing Shi, Kenji Nagamatsu [1] were mainly focused on solving the problem of limited speakers, and so they came up with a speaker diarization system using speaker-wise chain rules and achieved quality results.

We also give details about the Diarization Error Rate (DER) metric to evaluate the speaker diarization mechanism and the respective datasets used in each paper, and the results obtained after training. We hope that this overview work is a meaningful addition to the research community to unite the new improvements with neural techniques and subsequently encourage further advancement towards a more effective speaker diarization.

II. Diarization Error Rate

DER is the most important criterion for measuring diarization efficiency. NIST first used it in 2000 for their speaker segmentation mission. The metric is calculated by using a two-step approach:

1. Make a link between the speaker tags in the framework and the reference's speaker identities
2. Error rate is calculated using the mapping produced in the first step

The formula of DER is:

$$\text{DER} = \frac{\text{Miss} + \text{False Alarm} + \text{Confusion} + \text{Overlap}}{\text{Reference}} \quad (1)$$

III. Speaker Diarization Techniques

There are various speaker diarization approaches. Here, we have mentioned few research studies that have been conducted on speaker diarization by different researchers:

Huang et al. [2] tried to decrease the diarization error rate by coming up with a region proposal network for speaker diarization. The authors suggested the generation of speech proposals that overlap and simultaneously calculate embeddings through a neural network. The authors came up with a two-step approach. The first step is the joint speech segment proposal, where segmentation, re-segmentation, embedding extraction is combined. In this step, the prediction of audio segments takes place by the region proposal network. Then, for each audio segment, in-depth features are found by combining the regions of the feature maps. To aggregate the features into a specified size due to the difference in audio segment proposals' dimensions, RoIAlign[3] is used. In the second step, the segments are clustered, and non-maximum suppression is applied to get the

diarization result. The authors used Mixer6+SRE+SWBD and Simulated Train datasets to train the model and used CALLHOME, Simulated DEV, and Switchboard as their testing dataset. On the SWBD dataset, the proposed method produced a DER of 9.09%. Furthermore, on the CALLHOME dataset, the produced DER is 25.46%. Compared to standard diarization system, this technique has a shorter pipeline and is capable of handling overlapped speech.

Quan Wang, Philip Andrew Mansfield, Ignacio Lopez Moreno, Carlton Downey, Li Wan [4] came up with a speaker diarization system based on LSTM and compared their approach with i-vector-based embedding [5,6,7] and concluded that their approach had a considerably lower Diarization Error Rate compared to traditional approach of diarization systems based on i-vectors. It consists of sequence of steps. Firstly, the audio frames are converted into small sized frames with a 25ms of width and 10ms of step, after which log-Mel-filterbank energies of size 40 are retrieved as an input to the network. Next, they ran the LSTM network on sliding windows each of which had a fixed length on the frames. They considered the outcome from the LSTM's last frame as the d-vector. Next, the authors used spectral clustering, which consisted of four steps-First; they created an affinity matrix, where each entry comprised the cosine similarity between the segment embedding. Then they applied a sequence of refinement operations to smooth and denoise the data. Following this, on the refined matrix they executed Eigen decomposition. The amount of clusters was determined by making use of the maximum Eigen gap heuristics. In the last step, they used K means to cluster the speaker embedding and generate the labels of the speaker. The authors evaluated their proposed approach on two datasets-NIST SRE 2000, CALLHOME, and NIST RT-03 English CTS. They achieved a DER of 12.48% on the CALLHOME dataset, a DER of 12.30% on the NIST RT-03 English CTS dataset, and a DER of 18.8% on the NIST SRE 2000.

Yusuke Fujita, Shinji Watanabe, Shota Horiguchi, Yawen Xue, Jing Shi, Kenji Nagamatsu [1] proposed a chain rule for the speaker diarization and solved the problem of limited speakers as in the EEND approach [8]. In this paper, by making use of a probabilistic chain rule, they proposed a speaker-by-speaker conditional inference approach. A single random variable is considered as the speech activity of a particular speaker, and it is calculated in a linear fashion based on the speech activities of other speakers that have already been estimated. Using this approach, speech activity of each speaker is calculated in order using initially estimated speech activities acting like constraints. Since the previous speaker's speech activity is taken into account by the

neural network, the previous iteration's estimation error at times can have a negative impact on the output of the next iteration, so the authors made use of the teacher-forcing [9] method to reduce the error and improve the efficiency. They evaluated their proposed model on the CALLHOME dataset and achieved a DER of 18.07%. According to the results, this method has a good performance in predicting the speaker diarization result with varying speakers. It performs better than other diarization methods which are end-to-end, as per the DER.

V. Subba Ramaiah, R. Rajeswara Rao [10] proposed the use of Tangent weighted Mel frequency cepstral coefficient (TMFCC) and Lion optimization [11] for speaker diarization. They made use of the Lion algorithm to cluster the audio streams with respect to speaker groups. First, the audio stream that is given as input to this speaker diarization system will be segmented according to the speaker's identity. Then pre-processing of the audio stream takes place, which consists of the formation of an acoustic beam. The acoustic beam assists in making the audio stream diarization friendly. Subsequently, feature extraction takes place. The Mel filterbank is built using the power spectrum of input signals. TMFCC is obtained by calculating the energy band after the filter bank has been developed, and applying the tangent function. After the feature extraction stage, the process of detecting shift in speech activity takes place. The authors made use of the Bayesian Inference criterion (BIC) [12] to detect the change of speakers. Following this, i-vector extraction takes place using the universal background model [13]. Finally, using the Lion algorithm audio signals are clustered. The authors used the ELSDR corpus dataset consisting of more than two speakers to test their proposed model. The results showed that the proposed approach had 95% accuracy.

Aonan Zhang, Zhenyao Zhu, Quan Wang, John Paisley, Chong Wang [14] proposed a supervised approach for the speaker diarization problem. The authors made use of a process that includes labeled data for training and replaced the clustering module with a recurrent network known as unbounded interleaved-state recurrent neural network (UIS-RNN). The approach is as follows; first, the embedding extraction takes place, let $X = (x_1, x_2, \dots, x_T)$, be a sequence of embedding, and the ground truth labels for each speaker is represented by another sequence $Y = (y_1, y_2, \dots, y_T)$. Then UIS-RNN is a generative process where

$$p(X, Y) = p(x_1, y_1) \cdot \prod_{t=2}^T p(x_t | y_t, x_{t-1}, y_{t-1}) \quad (2)$$

To simulate the speaker's turn, the authors used a distance-dependent Chinese restaurant process, memorized long-term dependencies, and

used a gated recurrent unit. For training purposes, they used two datasets- ICSI Meeting Corpus and 2000 NIST Speaker Recognition Evaluation, Disk6. For testing, they made use of the 2000 NIST Speaker Recognition Evaluation (LDC2001S97) and achieved a DER of 7.6% on it.

Monisankha Pal et al. [15] proposed speaker diarization in generative adversarial networks (GAN) by making use of latent space clustering. The advantages of using GAN are the interpolation and interpretability in the latent space. A clustering-specific loss, GAN loss, and latent variable recovery loss are used to train the speaker diarization system. Using the initial speaker labels, the hypothetical variables are extracted from a blend of two variables which are continuous variables and one-hot encoded. The encoder network is used to perform inverse mapping, which is the backward projection of data into latent space. The approach is as follows: First, the input to the GAN discriminator is the x-vector embeddings of audio streams, followed by the latent space clustering. Then segmentation phase takes place in which segmented speech is embedded in a fixed 512-dimensional x-vector. Finally, ClusterGAN training takes place. They evaluated their approach on AMI meeting corpus, ADOS, and BOSCC dataset and achieved a DER of 7.82% on AMI, a DER of 9.22% on ADOS, and a DER of 11.17% on BOSCC. Paweł Cyrtą, Tomasz Trzcinski, Wojciech Stokowiec [16] suggested the extraction of speaker embeddings using a Deep Recurrent Convolutional Neural Networks. The authors suggested that learning the embeddings during training the network leads to a suitable generalization of the embeddings and speakers who were absent in the dataset used during training. The approach is as follows-First they used supervised training to train the recurrent neural network with the aim of speaker classification. Speaker embeddings are then extracted using the pre-trained neural network. For each case, the entire amount of activation can be achieved by taking the aggregate of the sigmoid outputs by summing all outputs with respect to classes over the entire audio segment and to make the values normalized, the values are divided with the highest value between classes by contrasting the collected and modified embedding with those already seen, by using these embeddings the device can identify speaker change and recognize the speakers which are new. The speaker is considered new if the embedding's cosine similarity is greater than 0.4. Otherwise, it is mapped to the embedding that is closest to it. The input to the network is a weighted spectrogram. The authors made use of log-Mel, Gammatone, and Constant Q transforms (CQT) as weighting filters. The network architecture consists of eleven learnable layers comprising of four blocks which are convolutional, two recurrent layers, and one layer which is fully connected. They evaluated their model on AMI

meeting corpus, ISCI meeting corpus, and Youtube speakers corpus. They achieved a DER of 15.3% on AMI, a DER of 13.8% on ISCI, a 17.8% DER on Youtube corpus.

Enrico Fini, Alessio Brutti [17] made use of a sample mean loss for the diarization problem having multi domain data. In this approach, the authors proposed qualitative modifications to the UIS-RNN model, which enhanced the performance of diarization and also increased the efficiency of learning. Using Sample Mean loss they trained the RNN in order to provide a better convergence rate which in turn enables the network to achieve deeper minima. Moreover, they invented an empirical concept to measure the likelihood of a new speaker to join the audio and found that their approach was more accurate in detecting the nature of speaker change. The training was done on speech segments of specific length and allowed the neural network to accumulate the embeddings, eliminating the speaker change constraint. The use of Sample Mean loss results in the definition of a predictor of the embedding distribution's mean. The authors evaluated their findings on the dataset employed in the DIHARD II challenge, achieved a DER of 27.3%, and observed that their proposed approach had a better performance than UIS-RNN.

Yangfan Zhang, Xiao Song, Jian Zhang [18] proposed speaker diarization system for conversations involving multiple speakers using x-vectors. The authors made use of a Deep neural network to generate x-vectors and Agglomerative hierarchical clustering [19] to aggregate the segments. The approach followed by the authors is as follows: First, parts of the recording which did not contain any speech were taken out using voice activity detection (VAD). Then they extracted MFCC features from the audio stream and then train a DNN for extraction of embeddings. The embeddings are then grouped into multiple clusters, each mapping to their respective speakers. Next, they used a probabilistic linear discriminant analysis (PLDA) to determine the pair's similarity and used AHC to measure the similarity between two random embeddings which are obtained from a deep neural network to check whether they are of the same speaker. They evaluated their approach on AMI meeting corpus and achieved a DER of 44%.

Yanni Chen, Yonghong Yan, Wei Hong, Songzan Guan [20] proposed a Full-Posterior probabilistic linear discriminant analysis based Speaker Diarization. The authors observed that the speaker diarization system's clustering segments are tiny, typically less than 1 minute, and their durations are random. The traditional PLDA model has a poor performance in this situation, so they made use of the posterior PLDA model to cluster the data, which

considers the uncertainty corresponding to the extraction of the i-vector into consideration. The FP-PLDA supposes that i-vector to be described as:

$$\mu = m + Uy + ei \quad (3)$$

FP-PLDA replaces the residual noise with ei; They made use of a clustering system consisting of two stages. In the first stage, the segments are clustered into respective speakers, and the top ten scores are selected for each cluster. KNN is used as the second stage clustering method. The authors made use of the SHIWANG database for training and testing purposes and observed a reduction of close to 31% from the standard PLDA system

IV. Conclusion

This paper defined the concept of Speaker Diarization and discussed some of the recent speaker diarization. The core objective of all the research works has been to minimize the diarization error rate. Perhaps, the most difficult task in the diarization process is the management of overlapped speech. However, with the increasing number of people recognizing the value of audio methods for many applications, this challenge can be easily solved in the near future..

References

- [1] Fujita, Yusuke & Watanabe, Shinji & Horiguchi, Shota & Xue, Yawen & Shi, Jing & Nagamatsu, Kenji. (2020). Neural Speaker Diarization with Speaker-Wise Chain Rule.
- [2] Z. Huang et al., "Speaker Diarization with Region Proposal Network," ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Barcelona, Spain, 2020, pp. 6514-6518, doi: 10.1109/ICASSP40776.2020.9053760.
- [3] Kaiming He, Georgia Gkioxari, Piotr Dollar, and Ross Girshick, "Mask r-cnn," in Proceedings of the IEEE international conference on computer vision, 2017, pp. 2961–2969.
- [4] Wang, C. Downey, L. Wan, P. A. Mansfield and I. L. Moreno, "Speaker Diarization with LSTM," 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Calgary, AB, Canada, 2018, pp. 5239-5243,doi:10.1109/ICASSP.2018.8462 628.
- [5] Mohammed Senoussaoui, Patrick Kenny, Themis Stafylakis, and Pierre Dumouchel, "A study of the cosine distance based mean shift for telephone speech diarization," IEEE/ACM Transactions on Audio, Speech and Language Processing (TASLP), vol. 22, no. 1, pp. 217–227, 2014.
- [6] Stephen H Shum, Najim Dehak, Reda Dehak, and James R' Glass, "Unsupervised methods for speaker diarization: An integrated and iterative approach," IEEE Transactions on Audio, Speech, and Language Processing, vol. 21, no. 10, pp. 2015–2028, 2013.

- [7] Gregory Sell and Daniel Garcia-Romero, "Speaker diarization with plda i-vector scoring and unsupervised calibration," in Spoken Language Technology Workshop (SLT), 2014 IEEE. IEEE, 2014, pp. 413–417.
- [8] Y. Fujita, N. Kanda, S. Horiguchi, K. Nagamatsu, and S. Watanabe, "End-to-end neural speaker diarization with permutation-free objectives," in Proc. Interspeech, 2019.
- [9] J. Williams and D. Zipser, "A learning algorithm for continually running fully recurrent neural networks," Neural Computation, vol. 1, no. 2, pp. 270–280, 1989.
- [10] Ramaiah, Subba & Rajeswara Rao, Ramisetty. (2017). A novel approach for speaker diarization system using TMFCC parameterization and Lion optimization. Journal of Central South University. 24. 2649-2663. 10.1007/s11771-017-3678-3.
- [11] K. Malik, K. Srivastava and K. Sharma, "Optimization of Neural Network Architecture using Lions Optimization Algorithm," 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2020, pp. 692-696, doi: 10.1109/ICICCS48265.2020.9121072.
- [12] PEELING P, CEMGIL A T, GODSILL S. Bayesian hierarchical models and inference for musical audio processing [C]// Proceedings of IEEE Wireless Pervasive Computing. Las Vegas, NV, USA: IEEE, 2008: 278–282.
- [13] Hasan and J. H. L. Hansen, "A Study on Universal Background Model Training in Speaker Verification," in IEEE Transactions on Audio, Speech, and Language Processing, vol. 19, no. 7, pp. 1890-1899, Sept. 2011, doi: 10.1109/TASL.2010.2102753.
- [14] Zhang, Q. Wang, Z. Zhu, J. Paisley and C. Wang, "Fully Supervised Speaker Diarization," ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brighton, UK, 2019, pp. 6301-6305, doi: 10.1109/ICASSP.2019.8683892.
- [15] M. Pal et al., "Speaker Diarization Using Latent Space Clustering in Generative Adversarial Network," ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Barcelona, Spain, 2020, pp. 6504-6508, doi: 10.1109/ICASSP40776.2020.9053952.
- [16] Cyrtà, Paweł & Trzcinski, Tomasz & Stokowiec, Wojciech. (2018). Speaker Diarization Using Deep Recurrent Convolutional Neural Networks for Speaker Embeddings. 107-117. 10.1007/978-3-319-67220-5_10.
- [17] Fini and A. Brutti, "Supervised Online Diarization with Sample Mean Loss for Multi-Domain Data," ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Barcelona, Spain, 2020, pp. 7134-7138, doi: 10.1109/ICASSP40776.2020.9053477.
- [18] Y. Zhang, X. Song and J. Zhang, "Speaker diarization for multi-speaker conversations via x-vectors," 2019 IEEE International Conference on Signal, Information and Data Processing (ICSIDP), Chongqing, China, 2019, pp. 1-4, doi: 10.1109/ICSIDP47821.2019.9173442.
- [19] Sell G, Snyder D, McCree A, et al. Diarization is hard: Some experiences and lessons learned for the JHU team in the inaugural DIHARD challenge[C]//Proc. Interspeech. 2018: 2808-2812.
- [20] Y. Chen, Y. Yan, W. Hong and S. Guan, "Full-posterior PLDA based speaker diarization of telephone conversations," 2017 First International Conference on Electronics Instrumentation & Information Systems (EIIS), Harbin, 2017, pp. 1-5, doi: 10.1109/EIIS.2017.8298729.

Opinion of Specific Tweets on Twitter

Sai Goutham Goli

Department of Computer Science and Engineering
Maturi Venkata Subba Rao (MVSRC)
Engineering College,
Hyderabad-501510, India.
saigouthamgoli111@gmail.com,

Sai Tarun Chinthalapati

Department of Computer Science and Engineering
Maturi Venkata Subba Rao (MVSRC)
Engineering College,
Hyderabad-501510, India.
saitarunchinthalapati@gmail.com,

Abstract: The issue of sentiment analysis on Twitter is addressed in this paper; that is, categorizing tweets in line with the feelings communicated in them: positive, neutral, or negative. Twitter is an online medium for micro-blogging and social networking, allowing users to post brief status updates 280 characters long. Twitter has 34 crore users all around the world producing 50 crore tweets per day. As per the survey, Twitter users are 38% more likely than other social media users to share views about brands and products. Twitter is used by most business users to provide customer support to their customers. As per the above survey report analysis, we try to achieve a reflection of public sentiment by scrutinizing the sentiments communicated in the tweets. Public sentiment analysis is useful in many applications, such as analyzing the stock exchange, political trends, product experience, etc.

Keywords: Twitter, Sentiment Analysis, Natural Language Processing.

I. Introduction

Twitter is an online medium for micro-blogging and social networking, allowing users to post brief status updates 280 characters long. Sorting tweets is one of the major applications to find out public opinion. Analyzing the tweets and categorizing them into positive, neutral, or negative based on the polarity of tweets is known as Twitter Sentiment Analysis.

The main objectives of our paper are to classify the tweets of a user based on Twitter username and the count of the number of tweets to be analyzed, to classify the tweets and plot a bar graph and pie chart based on hashtags and the count of the number of tweets to be analyzed, and to classify the text as positive, neutral, or negative.

Sanjeev Varkala

Department of Computer Science and Engineering
Maturi Venkata Subba Rao (MVSRC)
Engineering College,
Hyderabad-501510, India.
sanjeevsanju.varkala@gmail.com,

Venkataramana Battula

Department of Computer Science and Engineering
Maturi Venkata Subba Rao (MVSRC)
Engineering College,
Hyderabad-501510, India.
venkataramana_cse@mvsrec.edu.in

We have opted to work with Twitter data because, as opposed to traditional internet articles and web blogs, we believe it is a stronger approximation of public opinion. Also, the response on Twitter is more prompt and much more general. Sentiment analysis is one of the major applications in today's era. It is used to analyze the public sentiment towards a movie, product, etc., and gives the information to the companies to give the best service to its customers.

We extract the Tweets from Twitter based on usernames, hashtags, keywords by signing up into a Twitter Developer Account. Before classifying the tweets, we pre-process the tweets such as removing mentions, removing URLs, converting a number into a numeric text, tokenization, lemmatization, etc., We then classify the pre-processed tweet into positive, neutral, or negative with the use of TextBlob Library. We also built a GUI application using Tkinter, to get the analysis of a user based on the Twitter username and the analysis graphs based on keywords.

Internet is an open medium for all people to express their opinion in various languages. The concept of sentiment analysis has a lot of scope in the future. Sentiment analysis can be done in various languages using multi-linguistic sentiment analysis.

II. Literature Survey

Aliza Sarlan, Shuib Basri, Chayanit Nadam designed a sentiment analysis model, by collecting a huge amount of Twitter data. Prototyping was used in their work. Their results classified customer's opinions into negative and positive and depicted them on a web page and pie diagram.[1]

Apoorv Agarwal, Ilia Vovsha, Boyi Xie, Rebecca Passonneau, Owen Rambow, used state-of-the-art unigram model as their baseline and they achieved an overall gain of over 4% for 2 categorizing tasks: 3-way neutral versus positive versus negative and a binary, negative versus

positive. They explored the feature-based model and tree kernel model; both the above-mentioned models performed better than the unigram model. For the feature-based method, they merged prior polarity of words and parts of speech tags for more accurate analysis.[2]

Mrs. Monika Malhotra, Onam Bharti, proposed sentiment analysis on Twitter data on mobile reviews. They applied various machine learning(ML) algorithms like KNN, modified k means clustering, and Naïve Bayes and found that k means clustering is more accurate than other algorithms. They also found that modified k means algorithm has less time complexity than other algorithms.[3]

Abhilash Mittal, Sanjay Patidar, have made analyses on various datasets of Twitter to get the user opinion or sentiment. They performed various techniques on a single dataset and analyzed the results and came to the conclusion that Naïve Bayes works faster than other techniques.[4]

Gulden Uchyigit and James Spencer created a platform for analysis of sentiment of Twitter Data. They used the Naïve Bayes algorithm to categorize the tweets into negative, positive. They have analyzed that bigrams is preferable when conducting the classification process.[5]

Hamid Bagheri, Md Johirul Islam, examined the significance of social network analysis and its applications in various areas. They have created a python program for sentiment analysis. They showcased the results on various daily topics. They observed that number of neutral phrases are statistically higher.[6]

Teeja Mary Sebastian and Akshi Kumar extracted the opinion words from the tweets and proposed a hybrid approach using both dictionary-based methods and corpus-based methods for the sentiment analysis on Twitter data.[7]

Bholane Savita Dattu, Prof.Deipali V. Gore, have applied different machine learning(ML) algorithms like Naïve Bayes, SVM, etc. for sentiment analysis. They observed that the Naive Bayes classifier is insensitive to unbalanced data, resulting in more precise performance.[8]

Varsha Sahayak, Apashabi Pathan, Vijaya Shete, used three machine learning models, the tree kernel model, feature-based model, and unigram model. As a result, the sentiments of tweets obtained from Twitter are summarised by the proposed methods.[9]

Thirupathi Rao Komati, Sai Balakrishna Allamsetty, Chaitanya Varma Pinnamaraju, analyzed the Twitter data and generated output in the form of visual representation of the total sentiment score of the tweet.[10]

Neethu M S, Rajasree R, created an efficient feature vector by doing feature extraction after text pre-processing. Classification is done using various classifiers like SVM, Nava Bayes, Maximum Entropy and observed that all the classifiers have near accuracy for the new feature vector.[11]

Sahar A. El_Rahman, Wejdan Abdullah AlShehri, Feddah Alhumaidi AlOtaibi, collected data from Twitter, and data was given to numerous machine learning models and the results from the numerous machine learning models were tested using several metrics like f-score and cross-validation.[12]

Wilson, T., Kouloumpis, E., & Moore, J, as per their analysis, in the microblogging domain, part-of-speech(POS) features are not appropriate for sentiment analysis. They collected training data using hashtags, which proven to be helpful, as did data collected based on positive and negative emotions. The benefit of emotion training data is reduced when microblogging functions are used, according to their findings. They concluded by stating more study is required to determine whether the Parts of Speech(POS) features are appropriate for sentiment analysis in the microblogging domain.[13]

François Bar, Dogan Can, Hao Wang, Abe Kazemzadeh, and Shrikant Narayanan, demonstrated a method for real-time Twitter sentiment analysis of the 2012 U.S. presidential election, which was also underway at the time. To get a comprehensive and precise picture of the online political situation, they used the expert-curated rules, Twitter "firehose", and keywords. they developed a predictive opinion model and real-time data processing infrastructure that evaluates public sentiment shifts in relation to breaking political news and events as they occur. Since the architecture and process are generic, they can quickly be implemented and applied to other domains.[14]

Z. Jianqiang and G. Xiaolin studied the effect of six separate pre-processing approaches on sentiment polarity categorization in Twitter. They used four classifiers in a sequence of tests on five Twitter datasets to check the effectiveness of various pre-processing approaches. According to their studies, numbers, eliminating stop words, and URLs(Uniform Resource Locator) is a good process to minimize noise while having little effect on results. For sentiment analysis, replacing negation is effective.[15]

R. I. Yaghi, S. E. Shukri, H. Alsawalqah, and I. Aljarrah, used sentiment analysis models to derive the polarity and sentiments (opinions) of consumers regarding three of the most well-known car brands, which aids marketing. It would serve people who are looking to buy a car in contrasting the three companies based on the experiences of former buyers.[16]

Gohil S, Vuik S, Darzi A, used a variety of methods, for sentiment analysis of Twitter data in the healthcare environment. The commercial and open-source methods are developed on generic social media messages and product reviews. The above methods have not been checked thoroughly on a corpus of healthcare texts to ensure accuracy. Their research indicates that a reliable and well-tested method for sentiment analysis of tweets should be built first, using a corpus of manually annotated tweets from a healthcare environment.[17]

K. N. Reddy, V. S. Pagolu, G. Panda, and B. Majhi, in their analysis, have analyzed that there is a strong interrelationship between a company's stock price rise/fall and public expectations or feelings towards that company shared on Twitter by tweets. Negative, positive, and neutral tweets are grouped into three categories. They claimed that positive market opinion about a business on Twitter would reflect in its share price. They speculate this has a promising future.[18]

Ke Wang and Xiaojun Wan proposed a neural network model with a novel abstract-based attention mechanism to resolve the difficult challenge of sentiment analysis in the domain of scholarly paper peer review. They generated 2 evaluation datasets from the ICLR open feedback and had a lengthy discussion about the evaluation results. Their model can extract the opinions of multiple reviewers at the same time, making it much easier for authors to better their papers.[19]

S. E. Saad and J. Yang, J. Yang and S. E. Saad, analyzed sentiment analysis of Twitter data based on ordinal regression using various machine learning algorithms. They extracted Twitter sentiment analysis by building a scoring and balancing model, then they classified tweets into various classes using various machine learning (ML) classifiers.[20]

III. Implementation

We applied for Twitter Developer Account and created a project through the Developer Account portal. We generated access_token_secret, access_token, consumer_secret, and consumer_key from the created project as shown in below Fig 1.

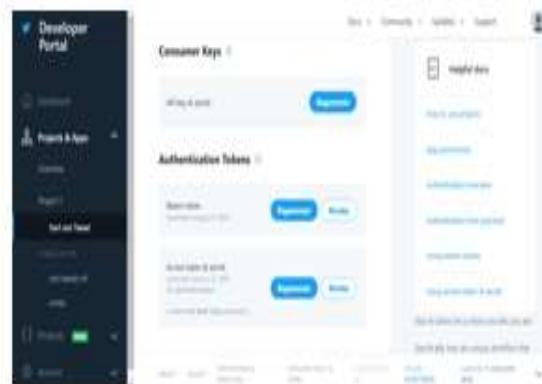


Fig 1: Twitter Developer Account –Project DashBoard

Tweepy is a Python package that gives us an easy way to access the Twitter API. We authenticated our API keys and authentication tokens by using Tweepy Library in Python. We then, extracted tweets using the tweepy and then stored them in the data frame, which is created using pandas.

We preprocess the extracted tweets using Natural Language Processing (NLP) Techniques.

First, we preprocess the tweets by

- Removing mentions,
- Removing hashtags,
- Removing punctuations,
- Removing URLs,
- Removing emojis,
- Removing white spaces,
- Converting the text into lower case,
- Converting number into a numeric text,
- Tokenization,
- Lemmatization.

With the help of regular expressions in python, we removed mentions, hashtags, punctuations, URLs, emojis of a tweet. By using inflect library in python, we converted the number into numeric text.

Tokenization is the way of converting large sentences into smaller units. These tokens help us in understanding the context.

Lemmatization is the way of generating the root form of the given word based on the parts of speech given.

We used the word_tokenize() method in the NLTK module to split a sentence into tokens or words.

We used lemmatize() method in the lemmatizer for the lemmatization of tweets.

We then use TextBlob in python to get the polarity of the Tweets. We first create an object for the TextBlob and then pass the preprocessed tweet to it as an argument. We get the polarity of a tweet as an output.

Polarity ranges from +1 to -1. +1 indicates the most positive sentence and -1 indicates the most negative sentence.

We then, classify the tweets according to the polarity, If the polarity of a tweet is greater than(>) zero, it is classified as a positive tweet, if the polarity of a tweet is less than(<) zero, it is classified as negative tweet and if the polarity is equal(=) to zero, it is classified as a neutral tweet.

We then plot pie charts and bar graphs according to the classification done earlier.

We also built a GUI application using the Tkinter module, to get the sentiment of tweets according to the username, to predict the sentiment of input text, and get the analysis graphs based on keywords or hashtags.

IV. Testing and Results

GUI application consists of four tabs, namely, Text Sentiment Analysis, Twitter Sentiment Analysis, Twitter Analysis Graph, About, using frames in the Tkinter module.



Fig 2: Opinion of Specific Tweets on Twitter GUI - Tabs

In the Text Sentiment Analysis tab, we have one input field, one output field, and four buttons namely, Tokenize, Analyze, Reset and Clear Result. In this tab, if we give a sentence or string as an input, we get the results as per the buttons clicked such as tokenize (after lemmatization), analyze, etc.



Fig 3.1: Opinion of Specific Tweets on Twitter GUI – Sentiment Analysis Tab

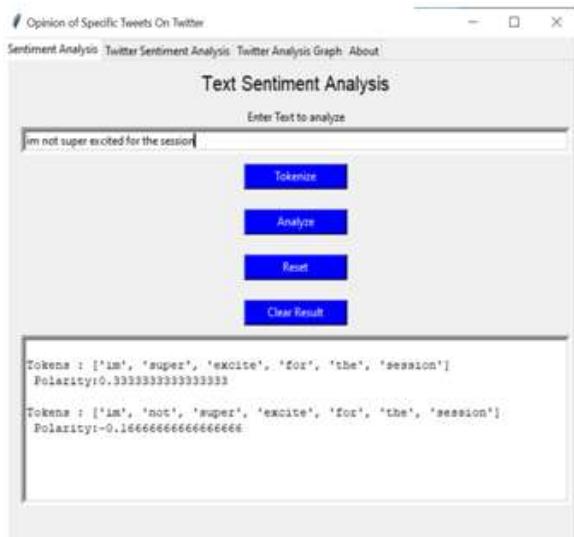


Fig 3.2: Opinion of Specific Tweets on Twitter GUI – Sentiment Analysis Tab

In the Twitter Sentiment Analysis tab, we have two input fields, one output field, and three buttons namely, Analyze, Reset and Clear Result.

In this tab, we need to enter the Twitter username and the count of the number of tweets to be analyzed as an input, here all the tweets are analyzed and we get the mean of the polarity of all the tweets of that particular username as an output. This tab helps us to analyze the tweets of a user and classify whether the user has positive intent or negative intent based on the polarity which we get as a result.



Fig 4: Opinion of Specific Tweets on Twitter GUI – Twitter Sentiment Analysis Tab

In the Twitter Analysis Graph tab, we have two input fields, one output field, and three buttons namely, Get Analysis Graph, Reset and Clear Result.

In this tab, we need to enter keywords or hashtags and the count of the number of tweets to be analyzed as an input, we get the count of classification of tweets and pie chart and bar graph as an output according to the buttons clicked. This tab analyses the latest tweets as per the count given and classifies them as positive, neutral or negative which helps us to understand the trends on that particular keyword.

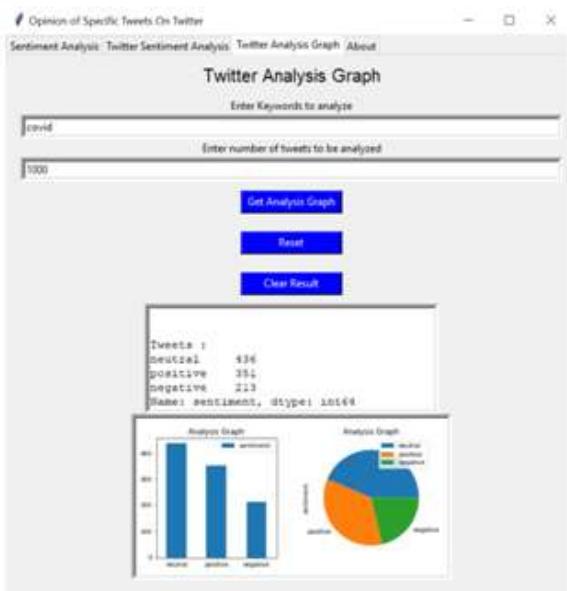


Fig 5: Opinion of Specific Tweets on Twitter GUI – Twitter Analysis Graph Tab

V. Conclusion

Sentiment Analysis is one of the major applications to analyze user's opinions. Twitter is one of the largest social networking platforms to express user's opinions, we extracted tweets from Twitter, pre-processed the extracted data using NLP techniques such as tokenization, lemmatization, etc., and then we obtain the polarity of the pre-processed data using TextBlob. Here we classify the tweets based on the polarity of Tweets obtained above (+1 polarity indicating most positive tweet, -1 polarity indicating most negative tweet). We also built a GUI, which has features such as, Text Sentiment Analysis, Twitter Sentiment Analysis, and Twitter Analysis Graphs. Twitter Sentiment analysis helps to understand the latest trends around the world, to get the user opinion about the products, helps companies to get the feedback from the users, etc.

Twitter Sentiment analysis has a lot of future scopes. Tweets are done by users in many languages. Sentiment analysis can be done in various languages using multilingual sentiment analysis. The concept of multilingual sentiment analysis is a lesser-explored domain and has a lot of scope for future work

References

- [1] Sarlan, Aliza & Nadam, Chayanit & Basri, Shuib. (2014). Twitter sentiment analysis. 212-216. 10.1109/ICIMU.2014.7066632.
- [2] Apoorv Agarwal, Boyi Xie, Ilia Vovsha, Owen Rambow, and Rebecca Passonneau. 2011. Sentiment analysis of Twitter data. In Proceedings of the Workshop on Languages in Social Media. Association for Computational Linguistics, USA, 30–38.
- [3] Bharti, Onam and Mrs. Monika Malhotra. "SENTIMENT ANALYSIS." (2016).
- [4] Abhilash Mittal and Sanjay Patidar. 2019. Sentiment Analysis on Twitter Data: A Survey. In Proceedings of the 2019 7th International Conference on Computer and Communications Management ICCC 2019). Association for Computing Machinery, New York, NY, USA, 91–95.
- [5] Spencer, J. and Gulden Uchyigit. "Sentimentor: Sentiment Analysis of Twitter Data." SDAD@ECML/PKDD (2012).
- [6] Bagheri, H. and M. J. Islam. "Sentiment analysis of twitter data." ArXiv abs/1711.10377 (2017): n. pag.
- [7] Kumar, Akshi & Sebastian, Teeja. (2012). Sentiment Analysis on Twitter. International Journal of Computer Science Issues. 9. 372-378.
- [8] Bholane Savita Dattu, Prof.Deipali V. Gore / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (6) , 2015, 5358-5362
- [9] Sahayak, Varsha, V. Shete and A. Pathan. "Sentiment Analysis on Twitter Data." (2015).
- [10] Thirupathi Rao Komati, Sai Balakrishna Allamsetty, Chaitanya Varma Pinnamaraju. "Implementation Of Sentiment Analysis On Twitter Data"

- [11] M. S. Neethu and R. Rajasree, "Sentiment analysis in twitter using machine learning techniques," 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, India, 2013, pp. 1-5, doi: 10.1109/ICCCNT.2013.6726818.
- [12] Rahman, Sahar A. El, Feddah Alhumaidi AlOtaibi and Wejdan Abdullah AlShehri. "Sentiment Analysis of Twitter Data." 2019 International Conference on Computer and Information Sciences (ICCIS) (2019): 1-4.
- [13] Kouloumpis, E., Wilson, T., & Moore, J. (2011). Twitter Sentiment Analysis: The Good the Bad and the OMG!. Proceedings of the International AAAI Conference on Web and Social Media, 5(1). Retrieved from <https://ojs.aaai.org/index.php/ICWSM/article/view/14185>
- [14] Hao Wang, Dogan Can, Abe Kazemzadeh, François Bar and Shrikanth Narayanan Annenberg Innovation Laboratory (AIL) Signal Analysis and Interpretation Laboratory (SAIL) University of Southern California, Los Angeles, CA.
- [15] Z. Jianqiang and G. Xiaolin, "Comparison Research on Text Pre-processing Methods on Twitter Sentiment Analysis," in IEEE Access, vol. 5, pp. 2870-2879, 2017, doi: 10.1109/ACCESS.2017.2672677.
- [16] S. E. Shukri, R. I. Yaghi, I. Aljarah and H. Alsawalqah, "Twitter sentiment analysis: A case study in the automotive industry," 2015 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT), Amman, Jordan, 2015, pp. 1-5, doi: 10.1109/AEECT.2015.7360594.
- [17] Gohil S, Vuik S, Darzi A, Sentiment Analysis of Health Care Tweets: Review of the Methods Used, JMIR Public Health Surveill 2018;4 (2):e43.
- [18] V. S. Pagolu, K. N. Reddy, G. Panda and B. Majhi, "Sentiment analysis of Twitter data for predicting stock market movements," 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Paralakhemundi, India, 2016, pp. 1345-1350, doi: 10.1109/SCOPES.2016.7955 659.
- [19] Ke Wang and Xiaojun Wan. 2018. Sentiment Analysis of Peer Review Texts for Scholarly Papers. In The 41st International ACM SIGIR Conference on Research & Development in Information Retrieval (SIGIR 18). Association for Computing Machinery, New York, NY, USA, 175–184. DOI:<https://doi.org/10.1145/3209978.3210056>.
- [20] S. E. Saad and J. Yang, "Twitter Sentiment Analysis Based on Ordinal Regression," in IEEE Access, vol. 7, pp. 163677-163685, 2019, doi: 10.1109/ACCESS.2019.2952127.

Types of Cyber-attacks and Defense Strategies

Mandru Suma Sri

Department of Computer networks and
Information Security
Chaitanya Bharathi Institute of Technology
Gandipet, Hyderabad-500075, India
mandrusumasri98@gmail.com

Rayapati Goutham

Department of Cyber Forensic and Security
Illinois Institute of Technology
Illinois, US
grayapati@hawk.iit.edu

Abstract: Rapid use of computer in every field has given a scope for the attackers to perform the Cyber Attacks more effectively and efficiently, which is a very sensitive issue in this world of internet security. The attacks are becoming more sophisticated due to the extreme usage of internet in this digital world. Some attackers attack out of curiosity and to make fun while some other attack for monetary gain. The importance of cyber security is growing, along with the sophistication and potential significance of the results of the attacks. Some fundamental security practices help in mitigating the risk from these attacks. There should be basic awareness to employees of an organization about these security attacks. This paper discusses about the various types of security attacks used by the cybercriminals such as malware attacks, phishing attacks, Sql injections etc., along with the preventive measures for all the types of attacks.

Keywords: Malware, Phishing, Attacker, Vulnerabilities, Cyber-attacks, Preventive measures, Threat.

I. Introduction

Cyber-attack is where the attacker tries to get the unauthorized access of the system. There are chances of an attack by the remote attacker only when the computer is connected to the internet. Hackers are rapidly developing their hacking techniques and the objectives of the attacker is to gain unauthorized access to the system, denial of service attacks and running malicious code on victim's system. These cyber-attacks pose threat to both an individual and larger organizations like IT companies, banks, health departments etc. nowadays computer attacks are conducted by individuals who are more organized. A cyber-attack against The New York Times originating from china lasted four months, in which they breached the network and used the data to access the employee's accounts. This attack may be linked to Chinese APT which Mandiant recently discovered. The case of Man Honan is also one of the major cyber-attack where a culprit was able to telephonically extract some sensitive data from Apple and Amazon customer support ("Cybersecurity 101: Intro", 2019). Using that sensitive data, he wiped out all of Honan's apple devices, causing a data breach but the damage is very

low. These are some of the examples of major cyber-attacks which caused data breach of users. Attackers do these malicious acts for the intent of financial gain, disruption of service or the sensitive data. There are many types of cyber-attacks where an attacker tries to get unauthorized access of the data such as Phishing mails, malware attacks, web attacks etc., There are some countermeasures which helps us to prevent from these attacks to only some extent, because the attackers are using more sophisticated attacks day by day.

What is a Cyber Attack?

Cyber-attacks are nothing but exploitation of vulnerabilities. They are taking place all the time and the security of organizations are compromised (Taylor, 2020). It is a malicious attempt by an individual or team to breach the system of other organization. Some does this for fun and some for money or sensitive data. A successful attack can disrupt the service or steal data or create a launch point for other attacks. Attackers use variety of methods to launch attack and some of them are malware attack, phishing attacks, denial of service. A cyber-attack can be launched from one or more than one computer against an individual or organization.

What is the goal of the attacker?

The goal of the attacker is to get the victim's system data and admin privileges on it or disrupt the service of the target system.

How often do cyber-attacks take place?

Cyber-attacks usually take place every day. Jhon Chambers, former CEO of Cisco once said that there are two types of companies: those that have been hacked and those that do not know yet that they have been hacked ("What Are the Most Common", n.d.).

What is a computer bot?

A bot is an automated program and sometimes works according to the instructions over the internet. Attacker sometimes use these bots to launch the attack. They are also used to perform repetitive tasks.

What is botnet?

A botnet is a network of infected computer which is used by a attacker to launch the attacks like distributed denial of service. Attackers can control the bots without the knowledge of the user.

II. Common Types of Cyber Attacks

To gain unauthorized access of a victim's computer or disrupt the service of target computer, cyber criminals use different methods. Here are the most common types of cyber-attacks used by attackers:

A. Malware Attack

The term malware is nothing but a malicious software which controls the victim's system and bring the system's performance to knees by destroying the entire network. If you have ever seen an anti-virus alert like pop-up on your computer or clicked mistakenly on a suspicious email attachment then you had a close call with this malicious software ("Common Types of Cybersecurity Attacks", n.d.). Attacker uses different methods to get malware into victim's system but at some stage it often requires user to take an action to click and install the malware which includes clicking the malware or clicking a suspicious email attachment where the malware is hidden. The malware includes virus, ransomware, spyware. (Dobran, 2019).

Malware attacks are becoming more sophisticated year by year and is often difficult to detect the malware without the anti-virus. A malware is a major threat to the sensitive and personal data on your computer. There are various forms of malware and we will discuss some of them:

- 1. Viruses:** Viruses infect applications attaching themselves to the initialization sequence ("Cybersecurity 101: Intro to top", 2019) by attaching themselves to an executable file, thus saving it with the same name and .exe extension. These viruses start infecting all the data in the hard disk by replicating itself and makes the system performance very low.
- 2. Worms:** Worms are like viruses but there is a slight difference between the worms and viruses. Worms do not attack the host, but they propagate across devices in the network. These are often installed through email attachments. Worms are generally used in denial-of-service attack by overloading an email server. The slight difference between worms and virus is virus replicates itself without any action of the user whereas worms replicate only with the action of user.

- 3. Trojan horse:** A trojan is a form of malware which hides inside a useful program with malicious intent and misrepresents itself to appear as useful software. They look like a useful and common software and persuade user to install ("Cybersecurity 101: Intro", 2019). A trojan is commonly used to set as a backdoor which can be exploited by attackers and they do not replicate themselves like virus (Dobran, 2019). Trojan are usually designed to steal financial and sensitive information and so they are considered as dangerous among all types of malwares.
- 4. Drive-by Attack:** In this a cyber-criminal looks for a vulnerable website where he can plant malicious script in PHP or http of the webpage. When the user clicks on such webpage, the malware gets installed on the computer or will be redirected to the malware download page. In some cases, upon clicking on the malicious script page the attacker gets control over the victim's system and it makes the code more complicated to be analyzed by security researchers and hence these attacks are termed as drive-by attacks as they do not require any action from the user except visiting the webpage.
- 5. Ransomware:** It is a malicious software, when executed in victim's system it encrypts all the files and demands ransom for the decryption key. These are usually done for the ransom. WannaCry, Crypto Wall, Petya are some of the examples of the ransomware. There is no guarantee of data even if the ransom is paid. So, it is advised not to pay the ransom once infected and this was endorsed by FBI (Fruhliger, 2020).
- 6. Spyware:** Spyware is nothing but a spying software. It is used to connect the user's data and monitor their activities on system. This malware when installed collects all the data of user and sends to attacker. Attacker uses this data to blackmail and get money from victim. Sometimes this malware is also used to install other malicious software's on the system (Taylor, 2020).
- 7. Malvertising:** This is one of the famous malware attack where cyber criminals buy some legitimate advertisement space on websites. When posting the advertisements, they will embed some malicious code in that ad. So, when the user browses that web page, they will be infected with the malware. Malvertising is different from adware. Whereas adware just shows some unwanted advertisements or content to the user.

B. Phishing Attacks

Phishing attacks are most common type of cyber-attacks where an attacker sends a fraud email to unsuspected users tending to come from reliable source using some social engineering. These are usually done to steal credit card numbers and login credentials of an organization. The attacker tricks the individual by posing as a trusted individual and makes him to open the email or message which can cause installing ransomware into his system which results in stealing credit cards, unauthorized purchases from the cards, stealing of funds, identity theft (“Cybersecurity 101: Intro”, 2019).

When an attacker wants to install malware, they often use phishing attack tactics like pretending to be someone you trust like your boss or your organization replicating some urgency Since they try to deal with social engineering and human emotions, these phishing attacks are difficult to stop. The phishing mails are very neatly crafted so that it looks like coming from the genuine source. The following are the various types of phishing attacks.

1. **Spear Phishing Attack:** Spear phishing attacks are email attacks which are targeted at specific organization or individual which are done by particular individuals to get trade secrets or financial information. The aim of this attack is to get the login credentials, crucial information of the company. These phishing mails looks like coming from the recipient's own organization or who knows the target personally. Each attacker has their own social engineering method to effectively customize websites (Dobran, 2019).
2. **Whale Phishing Attack:** This is a type of phishing attack that only targets high profile individuals like CEO or CFO of an organization as they have unlimited access to the organizations data. These attacks are more difficult to notice as they are highly targeted (Dobran, 2019). These types of attacks can be reduced by conducting security awareness programs.
3. **Pharming Attack:** Here, the attacker hijacks the website's DNS without involving the email unlike Spear and Whale attacks. As it hijacks the DNS the fake websites seem to be legit sites and authenticate links are also redirected. Pharming attack is very dangerous because it cannot be noticed or detected (Segal, n.d.).

C. Web Attacks

1. **SQL Injection:** SQL is nothing but Structured Query Language which is used to communicate with the databases that contains employer

details, customer details, and some sensitive data of the company. SQL injection is a type of web attack that is used by the attackers to manipulate the websites using malicious code and access the backend databases which is unauthorized for attacker, through which they can delete the entire tables in the database, view the sensitive data in the database (Dobran, 2019), causing huge impact on business organization such as loss of customer trust as the customers personal details, credit card numbers are exposed. (“Cybersecurity 101: Intro”, 2019).

2. **Cross-site Scripting:** In this the attacker injects malicious code into a website which doesn't harm the website but sets the user's browser information like username and passwords at risk. This code is usually sent through comment box or search box in JavaScript, which is done to damage the reputation of the website by placing user's information at risk (Dobran, 2019).
3. **Denial of Service:** Denial of Service is an attack which makes the server shut down by flooding it with traffic which exhausts the resources and bandwidth or by sending the information that crashes the system. When huge traffic is sent to server which it cannot handle then server stops responding to all the requests. This is known as denial-of-service attack. These DoS attacks are performed by many computers at the same time.
4. **Distributed Denial of Service:** The difference between DDoS and DoS is DoS uses one computer and one internet to flood the traffic whereas DDoS uses multiple computers with internet connections to flood the target as shown in Fig 1. It can even shutdown the server and make it offline. DDoS is more powerful than DoS. Here, there is no theft or loss of sensitive information in this attack but it costs victim a lot of money and time to mitigate. They are usually done to distract from other network attacks and also on major organization, government agencies, banks etc., (Dobran, 2019). Detecting DDoS is difficult as traffic comes from different IP address.

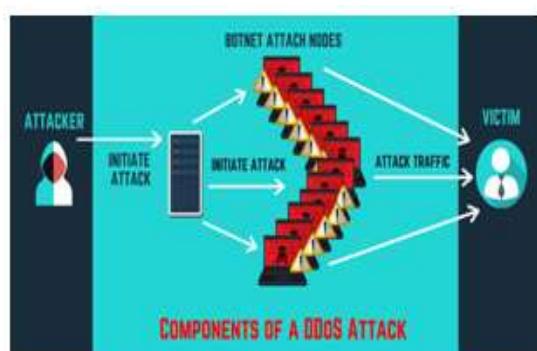


Fig 1: Components of DDoS Attack

5. Man-in-the-Middle Attacks: These attacks occur when an attacker intercepts a transaction and manipulates the data between two persons which is usually due to the vulnerabilities in the network or it is a public Wi-Fi. (“Cybersecurity 101: Intro”, 2019). It is not easy to notice this kind of attacks because sender and the receiver are unaware and presume it is sent to legitimate user (Dobran, 2019). Fig 2 shows how the attacker intrudes a transaction in a network.

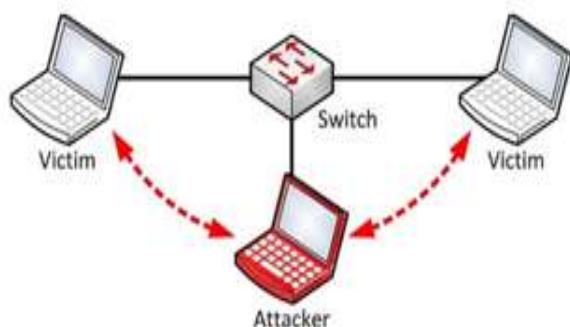


Fig 2: Man-in-the-Middle Attack

D. Password Attacks

Password attacks are nothing but getting login credentials of the victim with illegal intentions using social engineering or phishing attacks. The password attack includes cracking, brute force attacks, dictionary attacks and password sniffers. The only remedy for defending against the password attacks is following the password policy like using minimum length of the password, including symbols, alphanumeric character etc. Using these password policies, we can defend against the password attacks. Because it takes some years to brute force the password. These attacks are usually carried out by recovering password or by continuously guessing the password. The attackers try several combinations of password until they get the correct password (Sobers, 2020).

Eavesdropping is a type of password attack where attacker steals password when user is typing or by intercepting the network traffic. These attacks targets when the transmission is weak between the server and client which makes receiving transmission easy for attacker. Dictionary attack is a password attack where there are some possible passwords in a file. The attacker tries each password of that file until password matches. Brute force is also a password attack where it tries all the possible variants, combinations and ultimately it gets the password, but password cracking time depends on the length of the password. Two-factor authentication adds another layer of password security.

E. Other Attacks

1. Zero-day Exploit: A zero-day exploit is a vulnerability which is new and announced before it is patched. Zero-day attackers exploit the vulnerability when no solution or preventive measure exist (“Cybersecurity 101: Intro”, 2019). So, preventing zero-day exploit attacks requires constant monitoring. Methods for exploiting zero-day vulnerabilities are usually sold in dark web. Sometimes if government finds a zero-day exploit then they use it for their benefit rather than patching it (Fruhlinger, 2020).

2. Internet-of-Things Attacks: IoT attacks are rapidly increasing because of the growth of IoT devices. As all the IoT devices are connected to the internet there is high possibility of finding a vulnerability and then exploit. One more reason behind IoT attacks is low priority is given to the embedded security of the devices. There are unlimited access points for attackers to attack the IoT device. The only way to prevent the IoT attacks is to keep the strong password for the device and always keep the software up-to-date.

3. Sources of Cyber Attacks: The sources of cyber-attacks are nothing but the attackers or cyber criminals. So, the attackers of the cyber-attack might be crime groups, unhappy insiders, terrorists, business competitors, company spies and cyber organizations with large number of employees creating and executing exploits (Taylor, 2020).

III. Defense Strategies of Cyber Attack

- Build cyber threat awareness among the employees of the organization by conducting some awareness programs on cyber-attacks.
- Every organization should develop their own security policy which includes security practices that must be followed, acceptable and unacceptable use of company resources.
- Conduct the internal research and develop internal cyber security strategy for your organizations which includes identifying unpatched vulnerabilities in the company's systems.
- To minimize the password attacks on your organization, tighten the password policies like minimum password strength and also account access.
- Constantly monitor the server logs to check whether anyone is attacking on company website or server.
- Make sure the encryption is enabled at all levels of data in use.

- Regularly backup all the data and store it. If any case, you are infected with the ransomware, the data can be recovered.
- Always use multifactor identification because a small mistake done by the employer may cause compromise of the system.
- Install anti-malware software because it can detect the malware in your computer and prevent from various malware attacks like ransomware, spyware, adware.
- It is better to use the firewall as a first line of defense, which helps to reduce the attacks. Firewall acts as a barrier between your storage and attackers.
- Document the cybersecurity policies of your organization and it is very essential to document protocols.
- Always keep your software's you are using and operating system up-to-date. Because software's with older version may have vulnerabilities and gives the chance for the attackers.
- Never download software from unknown resources. Always download from legitimate websites.

IV. Conclusion

Taking the preventive measures can reduce the risk of attacks and 100% security is never possible. The attacks are becoming more sophisticated everyday with different type of vulnerabilities and exploits. But following basic security measures can prevent these attacks to some level. Along with good defense strategies, an organization should install anti malware software and keep the software up-to-date. The health industries and government agencies are most attractive targets for cyber criminals because they have sensitive information and are willing to pay ransom. So, following these defense strategies can mitigate the risks. The attacks are increasing day by day due to the increase in usage of internet. The recent cyber-attacks which caused heavy loss to the companies are ransomware attacks. These attacks can be mitigated by not clicking on unwanted pop-ups and visiting malicious sites. Creating awareness among the employees and people by conducting workshops helps in not falling for the pray. In future, we try to build a model to prevent the attacks from happening, which will be more efficient than detecting the attacks.

References

[1] Common Types of Cybersecurity Attacks and Hacking Techniques. (n.d.). Rapid7. Retrieved April 7, 2020, from

- <https://www.rapid7.com/fundamentals/types-of-attacks/>
- [2] Cyber Attack—What Are Common Cyberthreats? (n.d.). Cisco. Retrieved April 7, 2020, from <https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html>
- [3] Cybersecurity 101: Intro to the Top 10 Common Types of Cyber Security Attacks. (2019, May 1). Infocyte. <https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/>
- [4] Dobran, B. (2019, February 21). 17 Types of Cyber Attacks To Protect Against in 2020. PhoenixNAP Global IT Services. <https://phoenixnap.com/blog/?p=71548>
- [5] Fruhlinger, J. (2020, February 27). What is a cyber attack? Recent examples show disturbing trends | CSO Online. <https://www.csionline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html>
- [6] Graham, A. (2019, May 9). The 5 most common cyber attacks in 2019. IT Governance UK Blog. <https://www.itgovernance.co.uk/blog/different-types-of-cyber-attacks>
- [7] mimecast. (n.d.). Best Practices for Cyber Security Defenses | Mimecast. Retrieved April 11, 2020, from <https://www.mimecast.com/content/protecting-data-in-the-healthcare-industry/best-practices-for-cyber-security-defenses/>
- [8] Paul. (2018, June 20). What is Cybersecurity? | Introduction to Cybersecurity. Edureka. <https://www.edureka.co/blog/what-is-cybersecurity/>
- [9] Porter, K. (n.d.). Malware attacks: What you need to know. Retrieved April 10, 2020, from <https://us.norton.com/internetsecurity-malware-malware-101-how-do-i-get-malware-complex-attacks.html>
- [10] Segal, C. (n.d.). 8 Cyber Security Best Practices For Your Small To Medium-Size Business. Retrieved April 11, 2020, from <https://www.coxblue.com/8-cyber-security-best-practices-for-your-small-to-medium-size-business-smb/>
- [11] Sobers, R. (2019, November 20). 110 Must-Know Cybersecurity Statistics for 2020 | Varonis. Inside Out Security. <https://www.varonis.com/blog/cybersecurity-statistics/>
- [12] Taylor, H. (2020, January 22). What Are Cyber Threats and What to Do About Them. The Missing Report. <https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/>

Session-A4:
Cloud Computing and Cyber Security

DOALB: Nature inspired Meta heuristic -Dragonfly Optimization Algorithm based Improved Load balancing Technique for Cloud

Vijayakumar Polepally

Kakatiya Institute of Technology & Science, Warangal,
Telangana-506015, INDIA
vijayakumarpolepally@gmail.com

Abstract: Load balancing is an important activity in cloud computing since cloud servers have to accumulate an enormous data that raises the server load. The intention of the Load balancing method is that it sustains a trade-off by allocating equivalent load on servers with minimum power. Consequently, this chapter offers the load balancing method depending on Dragonfly optimization algorithm based load balancing (DOALB). Primarily, the load and capacity of every Virtual Machine (VM) are computed. If balanced threshold value is lesser than the load of VM then, the load balancing scheme is applied for assigning the tasks. The load balancing methodology computes the determining factor of every VM and verifies the VM load. Subsequently, it evaluates selection parameter of every task. Consequently, the task that has improved selection parameter is assigned to the VM. The performance of suggested load balancing technique is assessed in terms of set up 1 and set up 2 depending on the tasks. The investigational results demonstrate that the implemented scheme migrate 4 tasks whereas the conventional technique, HDLB migrates 7 tasks.

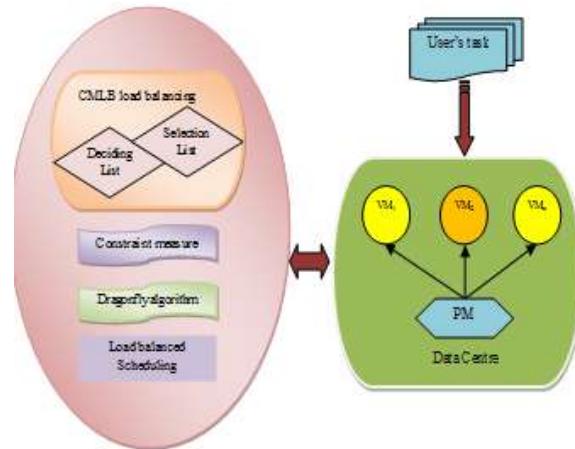
Keywords: Load balancing, Cloud computing, Dragonfly optimization.

I. Introduction

This the conventional research works on load balancing problem do not take into consideration of the capacities of resources to carry out a specific task and to fulfill the user's demands. As a result, the resource consumption was reduced in the given methodologies, and it generates the limitations to cloud computing [1]. Even though numerous algorithms were proposed for load balancing problem in the cloud, they did not offer the improved response time and scalability [2]. System congestion and the increased hardware cost are the significant crisis which persists in the load balancing schemes.

This proposed work illustrates the implemented DOALB scheme for assigning tasks to VM's and reassigning them while disparity happens. Fig.1. demonstrates the block representation of implemented DOALB methodology. The data center comprises of Physical Machines (PM), and every PM has a certain number of VM's. The task requirements

from a variety of users are given to the datacenter where the user submitted tasks are implemented by the VM's [3]. Accordingly, the tasks from a variety of users are assigned to VM's by the DOALB methodology. At first, the DOALB scheme discovers the determining factor of the entire VM's offered in the data center and then it generates the deciding list. Subsequently, it discovers the selection parameter of the entire user's tasks and produces the complete selection list. In the suggested scheme, the Dragonfly Algorithm (DA) is applied to produce desired optimal threshold value [4]. The load balancing approach verifies the VM's load in the deciding list. If the balanced is lesser than the load of the VM and if the VM has the enhanced deciding factor subsequently, the certain VM can be obtained from the decision list, and the user task holding the enhanced selection parameter is allocated to that VM. The allocated task is discarded from the selected list. Likewise, the entire tasks are allocated to VM's in a stable approach [5].



II. Load Balancing Depending on Task Reallocation

1. Task allocation based load balancing

A significant procedure in cloud is the allotment of task to the VM's. The allotment of resources to a requested task is essential in cloud computing owing to the constrained quantity of VM's. The user tasks are required to assign to the VM's in a stable approach [6]. In certain circumstances, the VM is much loaded, i.e., amount of tasks is assigned to it and the system's response

time is increased. Therefore the load balancing scheme is established to assign the tasks to the VM's. A load balancing approach obtains the user tasks from the overloaded VM, and then they are reassigned to the underloaded VM. As a result, the tasks are implemented with reduced time and hence, response time of the system is lessened. In load balancing scheme [7], the load and capacity of every VM are evaluated. In addition, the capacity of the VM is based on a variety of constraints, such as amount of processors, bandwidth, and the amount of instructions of processor [8]. The capacity of the VM, is evaluated as given in Eq. (1).

$$C(V_i) = \left[N_p^i \times N_m^i + B^i \right] \times \frac{1}{100} \quad (1)$$

where, indicates the capacity of the VM, V_i , N_m^i denotes the amount of processor in the VM, , signifies the amount of million instructions available in the virtual machine , V_i , and B^i denotes the bandwidth.

The load of the VM is computed by Eq. (2)

$$L(V_i) = \frac{\frac{1}{|E_j|} \sum_{\text{assigned task on } V_i} E_j}{C(V_i)} \quad (2)$$

where, $L(V_i)$ represents the load of the VM, V_i , E_j denotes the time for executing task T_j , and $C(V_i)$ signifies the capacity of the VM, V_i .

Subsequently, the load on the PM is evaluated by the complete load of all VM's offered in that PM, which is indicated by Eq. (3).

$$L(PM_k) = \frac{1}{|V_M^k|} \sum_{i=1}^m L(V_i) \quad (3)$$

In Eq. (3), $L(PM_k)$ indicates the load of the PM, PM_K , $L(V_i)$ denotes the load of the VM V_i .

Algorithm 1 demonstrates the process for assigning the tasks to VM in load balancing method. Initially, the entire tasks of users are red, and the tasks were allocated to the VM's based on Round Robin scheduling scheme (RRS). The jobs are allocated to the processor by RRS, by offering time quantum to every task. If task implementation is not concluded within time limit and at once the time limit runs out, subsequently the task will get terminated,

and the job can continue implementation after the erstwhile jobs are consuming their time quantum. Accordingly, the algorithm ensures the physical machine's load. If the PM's load is bigger than one, subsequently the course of action will stop. If the balanced is lesser than physical machine's load, then the load balancing scheme is carried out task reallocation. The abovementioned process is carried out until the entire jobs are performed.

Algorithm 1: Task allocation in load balancing

1. **Input:** Tasks T , VM's V
2. **Output:** The entire tasks are assigned to VM's
3. **for each** task in T
4. Allocate tasks to the VM depending on RRS
5. Using DOA find the unbiased threshold B_t .
6. **if** $L < (L(PM_k))$ **then**
7. Reassignment of tasks is not required.
8. **else if** ($B_t < (L(PM_k))$) **then**
9. Invoke load balancing scheme
10. **Else**
11. Go to step 3
12. End **if**
13. End **for**

2. Proposed DOALB algorithm

Here, the implemented DOALB approach for task reassignment is illustrated. The implemented technique evaluates the selection parameter for every task and deciding constraint for each VM. The deciding parameter of the VM is designed as given by Eq. (4), where, V_i indicates the i^{th} VM, $L(V_i)$ denotes the load of the VM V_i , $C(V_i)$ signifies the capacity of the VM V_i , and c^i corresponds to the task reallocation cost.

$$\text{deciding factor}(V_i) = 1 - \frac{1}{3} \left[c^i + L(V_i) + \frac{L(V_i)}{C(V_i)} \right] \quad (4)$$

The deciding parameter of the VM has to be highest. The selection parameter describes the task's priority level. The selection parameter of the task is evaluated as given by Eq. (5)

$$\text{selection factor}(T_j) = \left[\frac{P_j}{3} \right] \quad (5)$$

where, T_j denotes the j^{th} task and P_j indicates the priority level.

The tasks available in the VM are offered with 3 phases of priority, namely, priority level 1, 2 and 3. Here, the 3rd priority level denotes the highest task priority. Therefore Eq. (5) elucidates the selection factor that denotes the mean of 3 priority levels. The selection constraint of the task has to be high. At last, the job with highest selection parameter is assigned to VM with the greatest deciding factor, reduced load and least task reallocation cost.

Algorithm 2 demonstrates the suggested load balancing approach for assigning the tasks to VM's in cloud surroundings. Initially, this technique regards the entire VM's and discovers the deciding parameter of every VM by means of Eq. (4), and generates the deciding list. Followed by that, the algorithm discovers the selection constraint of the entire tasks and produces the selection list. Subsequently, it verifies the value of load to the VM. In addition, the balance threshold for the suggested DOALB approach is established with DA scheme. If the balanced TV is lesser than the load of the VM then, it assigns the task that has improved selection parameter to the VM that has an enhanced deciding factor. Further, the assigned task is obtained from the deciding list of the specific VM. If the deciding list does not encompass any VM's then, the deciding parameter of the VM's is evaluated another time. Further, it verifies the physical machine's load. If the balanced TV is lesser than the load of the PM then, the scheme will follow step 7, and the process is sustained till the entire jobs are implemented.

3. Obtaining optimal threshold value by DA approach

In this chapter, the optimal threshold value, TV is evaluated by DA approach [4]. The DA approach is carried out depending on the dragonflies swarming behavior. They form dense swarm for moving and hunting. Static swarm hunting stage, and dynamic swarm indicates the moving stage. Likewise, the DA approach includes two phases, that is, exploitation phase and exploration phase. The static swarm is identical to the exploration phase, and the dynamic swarm is identical to the exploitation phase. DA scheme includes three measures namely, separation, cohesion, and alignment. Separation is exploited to evade the conflict among dragonflies. The matching velocity of the dragonflies is denoted by alignment and the nature of dragonflies to the center of the neighborhood group is addressed by cohesion.

Solution Encoding: The TV in a set lies among zero to one, therefore the solution of the DA approach alters among zero to one.

Fitness Calculation: It is evaluated for each solution by placing the threshold stated in the solution to

cloud system and calculate the time necessary for the system to exceed the load balancing stipulation. This signifies that the PM's load exceeds one. For instance, the fitness refers to the time necessary for the PM's to exceed one.

Algorithm:

Step 1: Initialization: Here, the dragonflies' population and the step vectors are assigned. The dragonflies' population is indicated as, $P_d (d = 1, 2, \dots, n)$ and the step vectors are signified as, $\Delta P_d (d = 1, 2, \dots, n)$.

Step 2: Computation of objective value: For the entire iteration, $s = 1, 2, \dots, n$ the objective values of the entire dragonflies are computed.

Step 3: Food source and enemy update: Here, the positions (food source and the enemies) of entire dragonflies will be updated.

Step 4: Weight values update: The weight values, like alignment, cohesion, and separation are updated in this pace.

Step 5: Position update: Here, the dragonflies' positions are updated by subsequent formulations. The separation is determined from Eq. (6), in which, P indicates the current individual's position, P_r signifies r^{th} individual's position from the present individual, M denotes entire amount of neighboring individuals, L_d addresses d^{th} individual's separation.

$$L_d = - \sum_{r=1}^M P - P_r \quad (6)$$

III. Experimental Analysis

In this section, the investigational outcomes of the suggested DOALB technique with experimental description of the implemented technique for 1st setup and 2nd setup are portrayed.

Experimental Setup

The implemented load balancing technique is simulated in Cloudsim, and the computation is calculated with a variety of cloud set up for capacity and load. Here, the investigational outcome of implemented DOALB technique is portrayed for 1st setup and 2nd setup. The 1st set up includes five PM's and the 2nd set up contains ten PM's that are operating with 12 VM's.

Evaluation Measures

The implemented load balancing technique is computed for the loading and capacity measures.

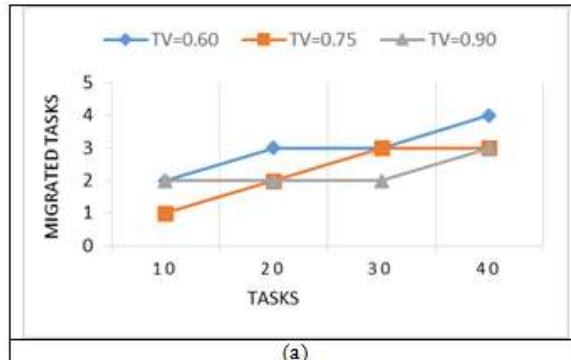
Load: It is described as the entire count of tasks allocated to the VM's [4].

Capacity: Capacity of the VM [4] is computed by Eq. (7), in which, U symbolizes the amount of processors, I addresses the amount of instructions, and B denotes the bandwidth.

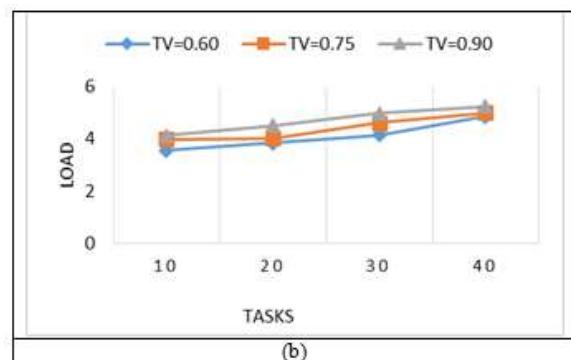
$$\text{Capacity(VM)} = U \times I + \text{Band} \quad (7)$$

Analyzing the maximum task size of 40

Fig.2 demonstrates the amount of load and migrated tasks of the VM's when the number of tasks are ten, twenty, thirty and forty while deploying of 0.6, 0.75, and 0.9 for 1st setup. Fig. 2(a) portrays the amount of migrated tasks while the amount of tasks are ten, twenty, thirty and forty for a of 0.6, 0.75 and 0.9. Fig. 2(b) demonstrates the load of the VM's while the amounts of tasks are ten, twenty, thirty and forty.



(a)



(b)

Fig 2: 1st setup when the numbers of tasks are 10, 20, 30 and 40 for (a) amount of migrated tasks (b) amount of load.

Fig. 3 demonstrates the design of amount of load and migrated tasks of VM's when amount of tasks are ten, twenty, thirty and forty while offering the of 0.6, 0.75 and 0.9 for 2nd setup. Fig. 3 (a) illustrates the amount of tasks migrated when the

amount of tasks are ten, twenty, thirty and forty for the of 0.6, 0.75 and 0.9. Fig. 3 (b) illustrates the load of the VM's while the amount of tasks is ten, twenty, thirty and forty while deploying the 0.6, 0.75, and 0.9.

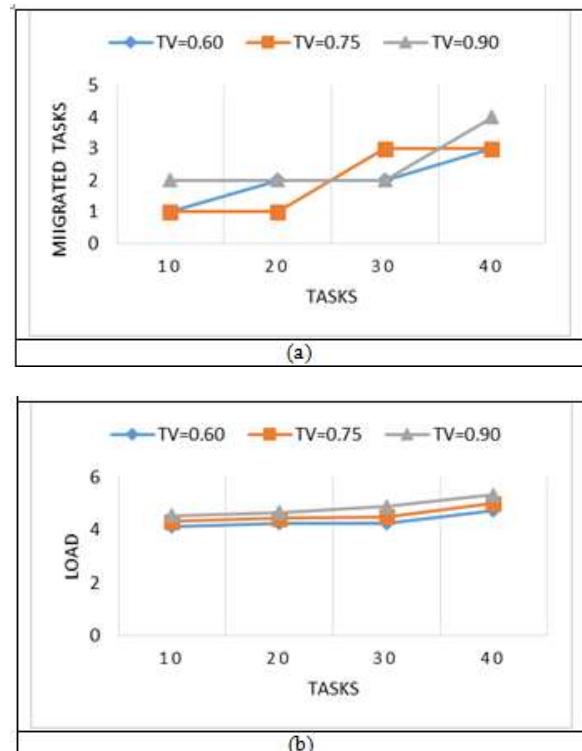


Fig 3: 2nd setup when the amounts of jobs are 10, 20, 30, and 40 for (a) amount of migrated tasks (b) amount of load.

IV. Conclusion

This chapter presents the load balancing approach based on the DOALB. Initially, the tasks are allocated to the VM's depending on the RRS scheme and the capacity and load of each VM was evaluated. If the balanced threshold value is lesser than the load of the VM, then the load balancing approach was exploited for tasks scheduling to the VM's. The load balancing scheme evaluates the deciding factor of the entire VM's and fills the deciding list. Subsequently, it evaluates the selection parameter of every task and fills the selection list and verifies the load of the VM. If the balanced threshold value is lesser than the load of the VM then, the load balancing scheme allocates the task that has enhanced selection parameter to the VM that has an enhanced deciding parameter. Followed by this, the assigned task was discarded from the selection list, and the VM was discarded from the deciding list. Likewise, the entire tasks were allocated to the VM's by the suggested load balancing technique. The number of migrations are increasing with the increase in the number of tasks.

References

- [1] Zhao, J., Yang, K., Wei, X., Ding, Y., Hu, L., Xu, G.: A heuristic clustering-based task deployment approach for load balancing using bayes theorem in cloud environment. *IEEE Trans. Parallel Distrib. Syst.* 27(2), pp.305–316 (2016).
- [2] Polepally, V., Shahu Chatrapati, K. Dragonfly optimization and constraint measure-based load balancing in cloud computing. *Cluster Comput* 22, 1099–1111 (2019).
- [3] Tong, Wuning, Song Xiao, and Hongbin Li. "Fault-tolerant scheduling algorithm with re-allocation for divisible loads on homogeneous distributed system." *IAENG Int. J. Comput. Sci* 45, no. 3 (2018).
- [4] Polepally Vijayakumar, and K. Shahu Chatrapati. "Exponential gravitational search algorithm-based VM migration strategy for load balancing in cloud computing." *International Journal of Modeling, Simulation, and Scientific Computing* 9, no. 01 (2018).
- [5] Mafarja, Majdi, Ibrahim Aljarah, Ali Asghar Heidari, Hossam Faris, Philippe Fournier-Viger, Xiaodong Li, and Seyedali Mirjalili. "Binary dragonfly optimization for feature selection using time-varying transfer functions." *Knowledge-Based Systems* 161 (2018).
- [6] Polepally, Vijayakumar, and Kaila Shahu Chatrapati. "Multiple objective-based modified exponential gravitational search algorithm to VMM strategy for load balancing in cloud." *migration* 68 (2017).
- [7] Li, Cuihong, and Katia Sycara. "A stable and efficient scheme for task allocation via agent coalition formation." In *Theory And Algorithms For Cooperative Systems*, pp. 193-212. (2004).
- [8] Dasgupta, K., Mandal, B., Dutta, P., Mondal, J.K., Dam, S.: A genetic algorithm (GA) based load balancing strategy for cloud computing. In: *Proceedings of the International Conference on Computational Intelligence: Modeling Techniques and Applications* 10, pp. 340–347 (2013).
- [9] Mirjalili, S.: Dragonfly algorithm: a new meta-heuristic optimization technique for solving single-objective, discrete, and multi-objective problems. *Neural Comput.Appl.* 27(4), pp. 1053–1073 (2016)

Exploiting the vulnerabilities of Traditional Captcha System and Exemplifying Smart Captcha System

Mrs. S. Sandhya

Assistant professor

Computer science engineering

G. Narayananamma Institute of Technology and
Science Hyderabad-500104, India

Ms. Satvika Eda

Computer science engineering

G. Narayananamma Institute of Technology and
Science Hyderabad-500104, India

Ms. Srishti Mathur

Computer science engineering

G. Narayananamma Institute of Technology and
Science Hyderabad-500104,
India

Ms. Prathyusha Kundavaram

Computer science engineering

G. Narayananamma Institute of Technology and
Science Hyderabad-500104, India

Abstract: CAPTCHA is a security mechanism designed to differentiate humans from malicious bot programs and are used for security checks which prevent hackers from getting the web data. But what if CAPTCHA could be broken? It means bots could decode CAPTCHA and access to web data. To demonstrate the importance of security of CAPTCHAs, we build an application that can be used to decode the text-based CAPTCHA system to prove that the data on the web can be exploited. We use CNN to build a model which can detect the characters of a CAPTCHA image. On manifestation, we know that the web data is vulnerable and partially exposed. Then, in order to have a reliable system, we build a CAPTCHA system to provide a safer and resilient approach. We now propose a system with a text-based CAPTCHA image and an object image as a combined CAPTCHA system with radio buttons. The result is a combination string of characters of text-based CAPTCHA image and name of the object image in the displayed order. Here, the radio buttons are generated based on the images extracted from the database. If the user doesn't clearly understand the images displayed, the user can refresh the page which displays new images. Therefore, this system makes it difficult for bots to attack and also helps humans to solve it faster and with ease in comparison to the conventional text-based CAPTCHA system.

Keywords: BOTS, CAPTCHA, Image Captcha, Security, Text-based Captcha

I. Introduction

In the present era of artificial intelligence, we need to make sure that bots will not over power the human world. Artificial intelligence was initially introduced to make life easier for humans but it is now working as a counter attack to dominate humans. CAPTCHA system is a way to achieve the same by protecting web data from malicious unknown activities by bots. CAPTCHA's security over the

years has reduced as they can be broken easily using machine learning algorithms.

This paper has two phases. In the first phase it shows the vulnerability of text-based CAPTCHA. In the second phase, this paper proposes a smart CAPTCHA system that is easy for humans and difficult for bots to solve.

II.Existing Systems

The current CAPTCHA methods can be divided into five groups: Text-based CAPTCHAs, Image-based CAPTCHAs, Audio-based CAPTCHAs, Motion-based CAPTCHAs and Hybrid CAPTCHAs [5]. A text-based CAPTCHA has a distorted version of characters of a word rendered as an image and are presented to the user. An Image-based CAPTCHA usually use the superiority of humans over computer vision systems in identifying the type of an object in an image. An audio-based CAPTCHA picks a string, renders it to a sound clip and presents it to the users who are asked to recognize the contents of the audio clip. Another category is motion-based CAPTCHAs in which a movie or animation is presented to the users and they are asked to recognize an action, animated word or image in the movie. Hybrid CAPTCHA is a combination of different types of CAPTCHAs or CAPTCHA's designed for special purposes.

There are various CAPTCHA breaking systems which can work as an extension on the web browser, so user can enable them whenever required. For example, auto CAPTCHA solver, ReCAPTCHA solver [3], CAPTCHA less. These extensions will automatically detect CAPTCHAs with in the page but user will have to select the correct CAPTCHA IMAGE and the correct CAPTCHA FIELD then REFRESH the browser for the service to solve the CAPTCHA automatically. There are other CAPTCHA solving services such as 2CAPTCHA, DeathByCAPTCHA, ImageTyperz, Anti-CAPTCHA, BestCAPTCHASolver and EndCAPTCHA provided to solve and bypass CAPTCHA [4].

III. Proposed System

The system proposed two phases, one for proving the vulnerable CAPTCHA system and the other to propose a safer system. The workflow is mentioned in the fig 1.

The phase-1 breaks CAPTCHAs present on a webpage. We automate the entire process of CAPTCHA filling and submitting without human involvement. CAPTCHA is detected, solved, auto-filled and submitted with no human intervention.

In the phase-2[8], to improve the overall security of CAPTCHAs, a new CAPTCHA system proposed is being implemented which has a combination of a text-based CAPTCHA and an object image. There are radio button options to choose the result from. This needs human interaction to go forward.

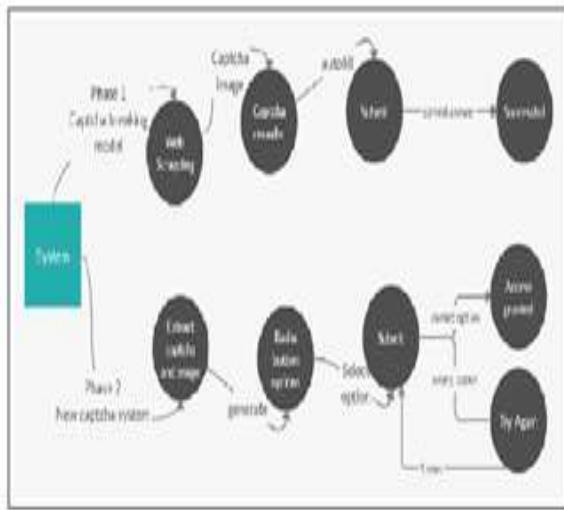


Fig 1: Workflow of the paper

IV. Methodology

The process flow of phase-1 is as follows: Once the CAPTCHA is detected by the application on the webpage, the CAPTCHA is scraped from the webpage, passed to the CAPTCHA breaking model where the image is broken down and result is identified. Then the system will itself find the text field in which the result needs to be filled and is automatically filled. It proves that the text-based CAPTCHA system is not safe enough for protecting the web data.

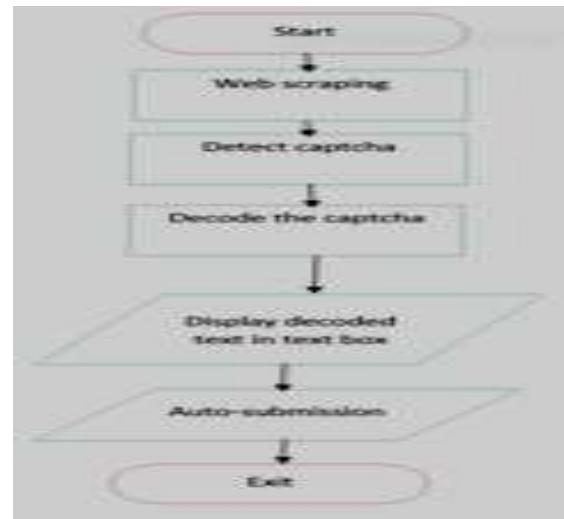


Fig 2: Flowchart of CAPTCHA breaking

Web page used in this phase has a CAPTCHA image, text field and a submit button. The web page is loaded by the command prompt in an automated mode using selenium library. Then, the CAPTCHA image is being detected in the web page and scraping is done using beautifulsoup library. The scraped CAPTCHA image is then passed to the CAPTCHA breaking CNN (Convolutional neural network) model. The image is then threshold and contoured where the boundaries of each character are identified to find out the characters of the CAPTCHA image.

Finally, the blobs are sent to the model and it is decoded. Then the decoded text i.e., the CAPTCHA result is filled in the text field in web pages using the selenium library and then it is submitted automatically with a sleep time of two seconds.

In the phase-2, we propose a smarter system which uses a combination of a text-based CAPTCHA and an object image. This needs human interaction to go forward.

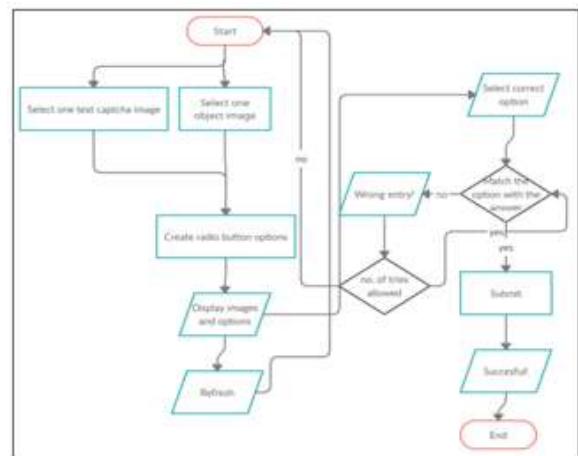


Fig 3: Flowchart of SMART CAPTCHA System

The images needed for our paper are collected and stored in a database. The images needed for the paper are two types of images where one is text-based CAPTCHA image and the other type is real-time object image [8].



Fig 4: Text-based CAPTCHA image



Fig 5: Real-time object image, in this case “MIRROR”

These images of each type are stored in different dataset i.e., the text-based images are stored in one dataset and the real-time object images are stored in other dataset. Each of the images has its name as its label and used to access the images from the database. Each data table has two columns, with one column being the image and the other column being the label of the image. We are using SQLite3 module to connect the GUI to the database. After connecting the database to the GUI, each image from each dataset is selected randomly and displayed on the GUI.



Fig 6: Images displayed by the CAPTCHA system

Once the images are selected randomly from each dataset and being displayed respectively. The labels of the images will be concatenated and saved in a list. To produce the other options other than the correct option, a random image is selected from text-based image database and another random image is selected from general object image database. The labels of the randomly selected images are concatenated and are stored in the list. Then, the contents of the list are generated as radio button options randomly on the GUI along with correct option. The user should select the correct option which has text CAPTCHA and object image.

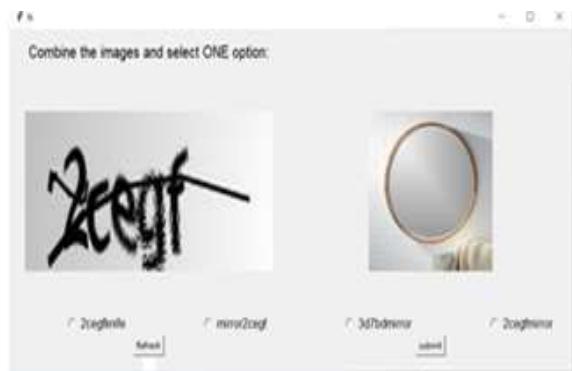


Fig 7: New Smart CAPTCHA generator

V. Results and Discussion

In phase-1, we understand how the CAPTCHA system is entirely automated. So, as a result we proposed a smarter way to do the CAPTCHA verification. In phase-2, the user should select the correct option which has text CAPTCHA and object image. If the user fails to do so, a wrong entry message will show up and will ask the user to try again. The user is given only two tries for a single combination of images.



Fig 8: Wrong Option is selected

If he fails to select the correct option in those two tries, the images will be automatically refreshed.

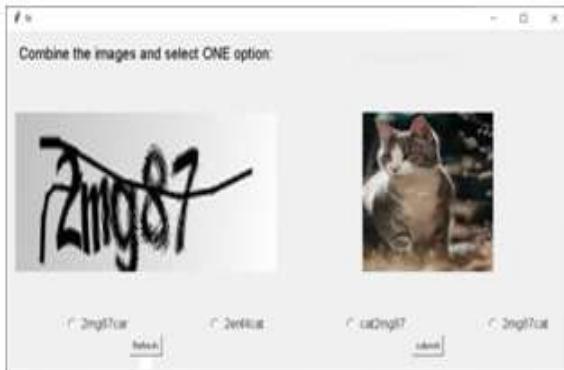


Fig 9: Automatically refresh if two wrong options are selected.

If the user selects the correct option and submits then the access granted message will pop up and the user can continue with his work.

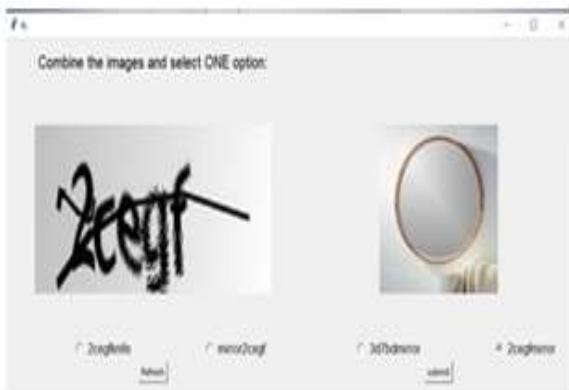


Fig 10: Correct Option is selected

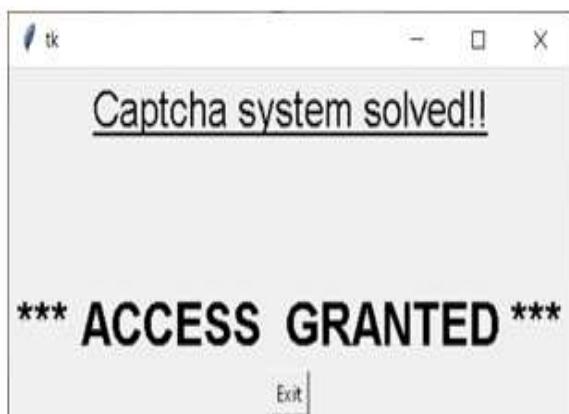


Fig 11: Access granted message pops after submitting correct option

The user can also refresh the page to generate another CAPTCHA and image.

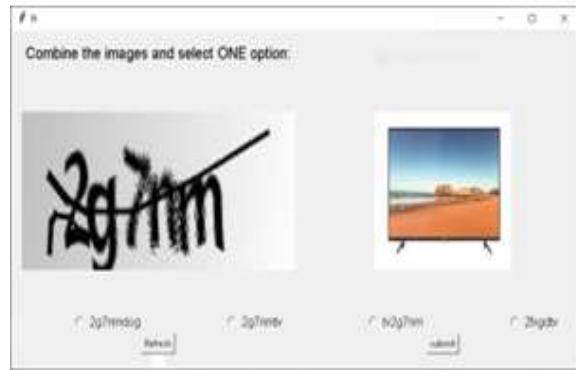


Fig 12: Different pictures will appear when 'Refresh' is clicked

VI. Conclusion

Initially, the main reason why CAPTCHA system was being introduced is to protect the web data from bots. This is a way to make sure that artificial intelligence will not over power the human world. Artificial intelligence was initially introduced to make life easier for humans but it is now used as a counter attack to dominate humans. The paper here demonstrates the flaw in the present CAPTCHA system by showing how CAPTCHA filling can be automated by using deep learning models and automation libraries. In order to overcome the same and make it safer, a solution is proposed by providing a smarter CAPTCHA system. Text based CAPTCHA system is vulnerable and prone to exploitation and thus, risking the web data. The main goal of smart CAPTCHA system is that it should make humans and computers apart and block the bots from maliciously taking over the web data. This new system decreases the difficulty for humans to solve the CAPTCHA and at the same time it makes it difficult to bots. It ensures better security when compared to the other systems.

VII. Future Work

The text-based CAPTCHA can be made more complicated using distortion, rotation and split algorithm which is still easy for human to recognize in a few seconds but difficult for bots to solve in a specified time. The images stored in the database has to be changed periodically because it should be difficult for the machine learning algorithm to learn about the image and map the correct text in the specified time. The images also can be displayed in a distorted form which can be recognized by humans but difficult for bots to solve. The paper can be made compatible with Mobile devices.

References

- [1] Adam Geitgey, "How to break a CAPTCHA system in 15 minutes with Machine Learning", Article on medium.com, Dec 13, 2017
- [2] BanduMadar, G.Kiran, C. Rama Krishna, "CAPTCHA Breaking using Segmentation and Morphological Operations", International Journal of computer Applications , May 2017
- [3] Fatih Merkez, "ReCAPTCHA Solver", Offered by Nowon48, Chrome web store
- [4] Garenne Bigby, "CAPTCHA Solving Services and Available CAPTCHA Types", Blog on DYNOMapper, October 12, 2018
- [5] Imperva, "CAPTCHA", Learning platform
- [6] Jun Chen, Xiangyang Luo, Yanqing Guo, Yi Zhang, Daofu Gong, "A Survey on Breaking Technique of Text-Based CAPTCHA", Security and Communication Networks, vol. 2017, Article ID 6898617, 15 pages, 2017.
- [7] Roberto Iriondo., "Breaking CAPTCHA using Machine Learning in 0.05 Seconds" , Article on medium.com, December 19, 2018
- [8] Uma P, Member, IAEENG, Siddivinayak K, Ramachandra P., "Smart CAPTCHA to Provide High Security against Bots" , Proceedings of the World Congress on Engineering 2019 WCE 2019, July 3-5, 2019, London, UK

A Trust Based Method for Providing Secure Data Transmissions in Mobile Ad hoc Networks

Venkata Krishna Reddy M

Asst. Professor,

CSE Department

Chaitanya Bharathi Institute of Technology

Hyderabad-500075,Telangana India

krishnareddy_cse@cbit.ac.in

Dr. Ravinder Reddy R

Assoc. Professor,

CSE Department

Chaitanya Bharathi Institute of Technology

Hyderabad-500075,Telangana India

ravinderreddy_cse@cbit.ac.in

Abstract: Now a days Mobile Ad hoc Networks (MANET) are being part of many other heterogeneous networks including “Internet of Things (IoT)”. Because of lack of Infrastructure, dynamic topology, Constraints on resources, sharing of bandwidth, security is always a great challenge and critical concern in Mobile Ad hoc Networks. A number of security solutions are proposed but they are not sufficient to provide security to Mobile Ad hoc Networks effectively. In this paper, a trust based approach is proposed which takes into consideration the direct observations of the node and neighbor recommendations about the node under consideration for evolving the final trust. This approach calculates trust based on the behavior of the node by considering network parameters. Simulation results under various performance metrics show that the proposed model performs efficiently.

Keywords: MANET, Dynamic Topology, Security, Direct Trust, Neighbor Trust, Resultant Trust, Routing

I. Introduction

Mobile Ad hoc Networks are infrastructure less, self organizing and consists of dynamic topology. These networks will not have any centralized control. They usually forms with set of mobile nodes and exchange data dynamically with one another in the range of one hop directly [1]. In recent years, the widespread usage of cheaper and powerful wireless nodes for communication, mobile ad hoc networks have gained much more attention and emerged as most promising area [2]. Due to their growing importance because of their wireless medium, mobile ad hoc networks are used in many heterogeneous networks like Internet of things (IoT) that also includes other networks like wireless sensor networks, ad hoc networks and ZigBee. In present days, the usage of IoT devices has been increased significantly. The areas include homes, organizations, offices, industries etc.

In MANETs, all the nodes involved within the range of one hop can communicate directly and those nodes that do not fall within the range should

depend on intermediate nodes for communication. Each node in the network can work as a intermediate node as well as terminal node, that means each node may generate the traffic while forwarding the packets of data received from source nodes to its neighboring nodes. The intermediate nodes has to dissipate their energy for forwarding others data packets. Due to the infrastructure less and dynamic topology, links between the nodes can change at faster mode and suddenly. Therefore, the nodes in a MANET have to help each other for transmission of data in multi hops.

Security is critical concern in MANET due to frequent connection interruptions, bandwidth and resource constraints, and high mobility of the wireless nodes. The nodes may behave selfishly and maliciously due to the energy constraints in forwarding other nodes packets as they have to use their own energy[3]. Another significant problem in MANETs is malicious nodes can wontedly drop or alter the packets contents. Due to this nature, packet transfer to the destinations can be interrupted, which in turn decreases packet delivery ratio, throughput and reliability [4]. Trust is augmented with Security. Trust can be used as important factor in providing secure transmission in Mobile ad hoc networks. Trust worthiness of all neighboring nodes should be evaluated well before involving them in any routing decision. Finding trustworthiness of a node is always a good measure to make sure the availability of the trusted and dependent nodes for secure path and to ensure secure communication between source and destination. Conventional procedures may not help in order to find such misbehaviors that occur randomly which causes threats to the network security. Trust-based Methods that involves in detecting and isolating untrusted and selfish nodes in MANETs, has been always treated as efficient measure to encounter the security threats caused by pernicious nodes [5].

In this paper, a novel and efficient security model based on trust that combines Direct trust values and Neighbor trust values is proposed. The direct trust value is evaluated through a quantifiable model by considering network parameters. Neighbor trust is calculated by taking into consideration the weights assigned to the neighbors depending on the

distance. The proposed scheme combines direct observations of the node and recommendations from various neighbors collected for calculating final resultant trust. In order to provide good performance and trustable links for secure transmission of data, the proposed solution depends on the trust factor.

The remaining part of the paper is arranged as follows. Review of related literature work is presented in Section II. A trust model is proposed in Section III and Section IV shows results obtained through the simulation and shows the effectiveness of the proposed method in terms of performance metrics. Finally, Section V concludes the paper.

II. Related Work

Trust is used in various applications of computing. It includes E-Commerce, distributed and social networks. The trust inclusion in Mobile ad hoc networks creates a positive impact. This perspective is supported by number of studies.

A security solution based on trust evaluation in Mobile ad hoc networks is given in [6] in which trust depends on statistical theory, owner's preference policy, intrusion detection results, reference by other nodes, and experience. In Adaptive trust dependent on Demand Ad hoc Routing approach [7], a nodes trust is its belief on its neighboring node. Various trust levels are defined in order to apply security accordingly. This approach saves power of the node, highly secured and also takes less time for communication. A trusted secured routing solution [8] presents a method for calculating, propagating and updating trust that has proven very effective against the presence of malicious nodes working together. A mechanism is proposed by Wang et al. [9] to differentiate cooperative peers from selfish ones purely based on "ad hoc on-demand distance vector (AODV)" routing protocol. A state machine model based on locally noticed AODV occurrences is used to generate numerical representation of each nodes character. Various patterns pertaining to node mobility can be considered as interesting feature to extend this work which can give additional insights. Jiang and Baras [10] used random theory of graphs and dynamic cooperative games theory to address distributed trust computation and propagation. In this scheme, opinion trust of intermediate nodes' is computed. Depending on that trust value, particular route for communication can be decided. Velloso et al. [11] projected a method based on trust management for a human centric model by projecting trust relations among the nodes where trust is calculated using local trust ratings. In [12], Zhang et al. applied routing driven algebra along with cluster centric trust computation in a conventional analysis of a trust oriented routing system. Dynamic Adaptive Fuzzy Petri Net (DAFPN) algorithm is used in

proposed method with concurrent reasoning. In [13], Xu et al. analyzed the routing protocols and presented a mathematical outline to derive the efficiency of the algorithms. Rath et al. [14], discussed security issues of MANET associated with "Internet of Things (IoT)". The method concentrated on security challenges and vulnerabilities for pervasive computing including IoT in connection with Mobile ad hoc networks. Sethuraman et al. [15] given a trust management strategy that allows data packets transmission securely along the network with low energy consumption. In this solution a unique trust value is assigned to each node randomly. The integration of energy consumption and trust of every node is essential due to high node mobility. A public key application method that includes the trust graph model is proposed in Kambourakis et al. work [16]. An algorithm is presented by Ahmed et al. where trust is calculated to isolate misbehaving nodes[17]. It was observed that the projected method was helpful in order to perform data transmission securely in Mobile Ad hoc Networks. A compound trust model which involves communal and QoS trust components is proposed by Jhaveri et al.[18] to calculate the degree of trust for the nodes in which social trust component called as the ditch ratio was used. This "ditch ratio" is useful for estimating the nodes performance while identifying misbehaving nodes.

Koul et al.[19] proposed a scheme which ensures security in Mobile ad hoc networks by considering QOS issues. It consists of five modules, i.e., packet forwarder, packet receiver, security information module (SSM), data security module (DSM) and QoS routing module (RM). In this multilayered approach, all the modules are used to find malicious and selfish nodes using QoS parameters.

III. Proposed Model

The implementation of the proposed model is discussed elaborately in this section. This model evaluates the trustworthiness of the nodes in the network in order to improve the security in collaborative routing and also the performance of Mobile ad hoc networks.

A. Trust Model

Figure 1 explains the Trust Model which illustrates the generation of trust, its propagation, Node Categorization and Routing Decision.

Routing Decision is made depending on the Node Categorization whereas Node categorization depends on Trust calculation.

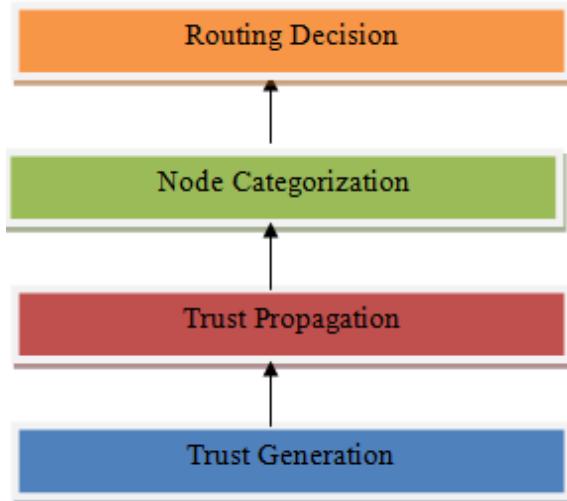


Fig 1: Framework for Trust Calculation and Routing Decision

The phases involved in the trust model are as follows

B. Trust Generation

Node A wants to calculate trustworthiness of Node B which it wants to include as intermediary node for routing data packets to the destination. Node A initiates trust calculation on Node B. This phase is performed in three step process.

C. Direct Trust Calculation

A node should listen to its neighbor nodes to estimate the trust. Because of the distributed nature of Mobile ad hoc Networks, a node can monitor neighbor node to evaluate its behavior during their direct communications in a passive mode. The proposed scheme uses the direct observations to calculate Direct trust related values DTrust of neighbor nodes by applying the below network parameters.

- a. number of data packets forwarded (considered as Good)
- b. number of data packets dropped (considered as Bad)

Node A collects the information regarding above network parameters for calculating trust by observing traffic that goes through the each neighbor of Node B. Then ‘Node A’ uses the above information to calculate direct trust value in a time period τ_{Time} . After running out of each time period τ_{Time} , the trust parameters are gathered again and direct observation “DTrust” is evaluated. Trust is calculated periodically due to the dynamic nature of MANETs. Nodes are classified based on their good and bad characterisations.

After gathering the information about good and bad behaviors of the node, the Direct Trust can be calculated by Node A on Node B using Equation 1.

$$D_{Trust} = \alpha / (\alpha + \beta) \quad (1)$$

where α represents Good behavior and β represents Bad behavior and $0 \leq D_{Trust} \leq 1$, $\alpha, \beta > 0$

D. Neighbor Node Trust Calculation

In the process of trust evolution on Node B, Node A also takes into consideration the recommendations of neighboring nodes on Node B in 1-Hop distance. The Neighbor Node Trust ‘ND_{Trust}’ can be calculated by Equation 2.

$$ND_{Trust} = \sum_{i=1}^n (w_i * D_{Trust}) \quad (2)$$

Where w_i is weights assigned to the nodes depending upon their distance in 1-Hop, $0 \leq w_i \leq 1$ and D_{Trust} is the Direct Trust Observations of the Neighboring Nodes on Node B.

E. Resultant Trust Calculation

Final trust calculation of a node is done based on Direct Trust component evaluated and consolidated Neighbor Trust component using Equation 3

$$\text{Resultant Trust } R_{Trust} = D_{Trust} + ND_{Trust} \quad (3)$$

F. Trust Propagation

Once the ‘Resultant Trust’ R_{Trust} is determined for the Node, it is broadcasted across the network so that the other nodes can update.

G. Node Categorization

In this method, A node is said to be bad one if it randomly drops packets intentionally but not for intrinsic network issues. The nodes are clustered into two groups depending on their good and bad behavior setting a threshold limits TH_{Max} and TH_{Min}. These threshold limits are fixed depending on network configuration.

Good: if $R_{Trust} \geq TH_{Max}$

Bad: if $R_{Trust} \leq TH_{Min}$

H. Routing Decision

Source finds trusted nodes using the proposed scheme to establish the secure route to destination. Each node consists the list of dependable(trusted) neighbor nodes as well as their latest trust values calculated. At this point, the

source-to-destination path is formed by considering only good nodes.

IV. Simulation and Results

The efficiency of the proposed trust-based solution is shown by comparing it to the scheme proposed by Chatterjee et al. [20]. In [20], a wide distributed trust solution for Mobile ad hoc networks security has been proposed. The proposed scheme of this paper calculates the direct trust value of a node by observing its data transmission nature. Various transmission parameters like number of data packets forwarded or dropped are considered for the direct trust calculation. In this proposed solution, the resultant trust is evaluated using a computable approach by considering the direct trust observations of the Node itself and the Neighbor observations on the Node under consideration. Simulation is carried out in a $500 \times 500 \text{ m}^2$ network area and IEEE 802.11 MAC for 600s with 20-nodes is used. In the simulation part, it is observed that good nodes drop the data packets because of the environmental anomalies of the network which likely to be nodes mobilization, packet collisions etc. whereas the malicious/selfish nodes drop the data packets deliberately. Table 1 summarizes the simulation parameters.

Table 1: Simulation Parameters

Simulation Parameter	Value
Simulator	NS2.34
No of Nodes	20
Network area	500×500
Packet Size	512 bytes
No. of malicious nodes	06
Traffic Type	CBR/UDP
Mobility	4–25 m/s
Pause Time	5s
Simulation Time	480s

A. Performance Evolution

It is detected that almost 22% of the data packets (non intentional-malicious drops) are found lost because of the environmental glitches in the network. For performance evolution of the proposed scheme, metrics like Packet Delivery Ratio (PDR), Detection of False Positives are taken into consideration.

B. False Positives Detection Ratio

The ratio defined as the count of good nodes wrongly identified as malicious to the total available count of nodes in the network is used to calculate ‘False positive’. In Figure 2, the percentage of

packets collided vs percentage of false positives detected of the proposed scheme is shown. The below graph shows that only 4.8% nodes are wrongly detected as. false positives i.e. malicious when 25% packet collisions occur.

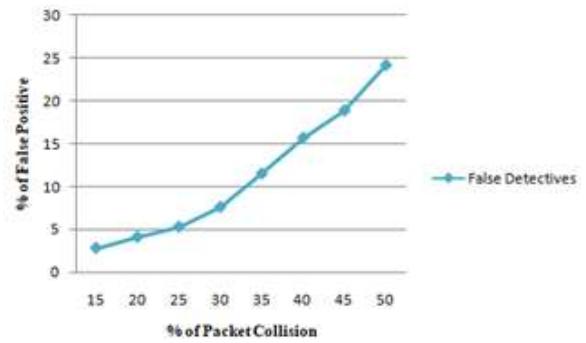


Fig 2: False Positive Detection Ratio

C. Packet Delivery Ratio

Figure 3 shows how packet delivery is effected with the presence of malicious nodes. The graph depicts the comparison between the existing distributed trust model and the proposed method. It clearly shows that Packet Delivery Ratio is high even when the malicious nodes are high.

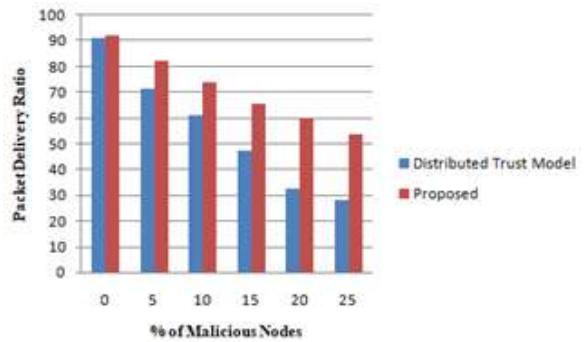


Fig 3: Packet delivery ratio mapped with number of malicious nodes.

V. Conclusion

This paper presents a quantitative trust model by the integration of direct observations and neighbors recommendations. The proposed trust method calculates resultant trust using the combination of Direct and Neighbor trusts by collecting information of a node through network parameters. Simulation results shows that the model performs with good efficacy in terms of performance metrics like false positive detection and packet delivery ratio. Trusted Nodes can be easily identified using this method efficiently. So the path between source and destination is formed only using the trusted nodes identified.

In the future, this method can be used in making efficient routing decisions. The proposed trust scheme can be applied to provide security in mobile ad hoc networks. Source finds trusted nodes using the proposed scheme to establish the secure route to destination.

Acknowledgment

We would like to thank and acknowledge Dr. P.V.S. Srinivas, Professor of CSE Dept, Sri Nidhi Institute of Technology and Dr Y Rama Devi, Head of CSE, Chaitanya Bharathi Institute of Technology for providing their continuous support.

References

- [1] Sumathi, K.; Priyadarshini, A. Energy Optimization in MANETs Using On-demand Routing Protocol. *Procedia Comput. Sci.* 2015, 47, 460–470.
- [2] Hinge, R.; Dubey, J. Opinion based trusted AODV routing protocol for MANET. In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies (ICTCS), Udaipur, India, 4–5 March 2016; ACM: New York, NY, USA, 2016.
- [3] Gite P.; Kanellopoulos, D.; Choukse, D. An Extended AODV Routing protocol for secure MANETs based on node trust values. *Int. J. Int. Tech. Secure. Trans.* in press.
- [4] Zafar, S.; M.K. Trust based QOS protocol (TBQP) using meta-heuristic genetic algorithm for optimizing and securing MANET. In Proceedings of the International Conference on Reliability Optimization and Information Technology, Faridabad, India, 6–8 February 2014.
- [5] Sirisala, N.; Bindu, C.S. A Novel QoS Trust Computation in MANETs Using Fuzzy Petri Nets. *Int. J. Intell. Eng. Syst.* 2016, 10, 116–125.
- [6] Z.Yan, P. Zhang and T. Virtanen, Trust Evaluation Based Security Solution in Ad hoc Network, Technical Report, Nokia Research Center, 2003.
- [7] Nekkanti Rajiv K. and Lee Chung-wei, Trust Based Adaptive on Demand Ad Hoc Routing Protocol, in Proc. of the ACM Southeast Regional Conference, pp. 88-93, 2004.
- [8] Tirthankar Ghosh, Niki Pissinou and Kami Sam Makki, Towards Designing a Trusted Routing Solution in Mobile Ad Hoc Networks, *International Journal of Mobile Networks and Applications*, pp. 985-995, 2005
- [9] Wang, X.; Liu, L.; Su, J. Rlm: A general model for trust representation and aggregation. *IEEE Trans. Serv. Comput.* 2012, 5, 131–143.
- [10] Jiang T.: Baras J.S. Cooperative Games, Phase Transition on Graphs and Distributed Trust in MANETs. In Proceedings of the 43th IEEE Conference on Decision and Control, Nassau, Bahamas, 14–17 December 2004; pp. 93–98.
- [11] Velloso, P.; Laufer R.; de O Cunha, D.; Duarte, O.; Pujolle G. Trust management n mobile adhoc networks using a scalable maturity-based model. *IEEE Trans. Serv. Manag.* 2010, 7, 172–185.
- [12] Zhang C.; Zhu, X.; Aong, Y.; Fang, Y. A Formal Study of Trust-Based Routing Wireless Ad hoc . In Proceedings of the 2010 IEEE INFOCOM, San Diego, CA, USA, 14–19 March 2010; pp. 1–9.
- [13] Xu, H.; Wu, X.; Sadjadpour, H.R.; Garcia-Luna-Aceves, J.J. A unified analysis of routing protocols in MANETs. *IEEE Trans. Commun.* 2010, 58, 911–922.
- [14] Rath, M.; Panigrahi, C.R. Prioritization of Security Measures at the Junction of MANET and IoT. In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, Udaipur, India, 4–5 March 2016; pp. 1–5.
- [15] Sethuraman, P.; Kannan, N. Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET. *Wirel. Netw.* 2017, 23, 2227–2237.
- [16] Kambourakis, G.; Konstantinou, E.; Douma, A.; Anagnostopoulos, M.; Fotiadis, G. Efficient Certification Path Discovery for MANET. *EURASIP J. Wirel. Commun. Netw.* 2010, 243985.
- [17] Ahmed, M.N.; Abdullah, A.H.; Chizari, H.; Kaiwartya, O. Flooding Factor based Trust Management Framework for secure data transmission in MANETs. *J. King Saud Univ. Comput. Inf. Sci.* 2017, 29, 269–280.
- [18] Jhaveri, R.H.; Patel, N.M.; Jinwala, D.C. A Composite Trust Model for Secure Routing in Mobile Ad-Hoc Networks. In *Ad Hoc Netw.*; Ortiz, J.H., de la Cruz, A.P., Eds.; InTech: London, UK, 2017; ISBN 978-953-51-3109-0.
- [19] Koul, A.; Kaur, H. Quality of Service Oriented Secure Routing Model for Mobile Ad hoc Networks. In Proceedings of the International Conference on Intelligent Systems, Metaheuristics & Swarm Intelligence, Hong Kong, China, 25–27 March 2017.
- [20] Chatterjee, P.; Ghosh, U.; Sengupta, I.; Ghosh, S.K. A trust enhanced secure clustering framework for wireless ad hoc networks. *Springer Wireless Networks* 2014.

Load Balancing Policy to Improve the Data Center Processing Time in Cloud Environment

Ramana Reddy B

Research scholar , VTU , Belgavi

Asst. Professor, Department of CSE

Chaitanya Bharathi Institute of Technology

Hyderabad, Telangana-500075

ramanareddy1984@gmail.com

Dr.Indiramma M

Professor,

Department of CSE

B.M.S. College of Engineering

Bangalore-560019, India

indira.cse@bmsce.ac.in

Abstract: In Today's world, cloud computing is an emerging services and has been proved a profit business model. We can observe cloud computing growth was good in the last decade because of its easy to access services. The number of users is increasing dynamically, to handle the load, load balancing is required. Load balancing algorithms minimize the data centre processing time and increases the throughput. In this paper, we have implemented the Round robin algorithm, Eq. spread algorithm and Throttled algorithm. Experiment results are observed on overall response time, Datacenter processing time and Virtual machine's(VM's)cost.

Index Terms: Cloud Computing, Cloud Analyst, Virtual Machines, Data Center, Load Balancing

I. Introduction

These days Cloud Computing is one of the latest trending technologies; it has a property easy to use and cost optimization services. It has so many characteristics out of which reliability, virtualization, multi-tasking, infrastructure cost optimization etc., with the help of mentioned features, Cloud Computing is the trending technology. Today Cloud Computing is used by so many startup entrepreneurs are saving their cost, time and working space. They use personal computers to connect the cloud services instead of purchasing the Infrastructure. Cloud computing, in short, the services are available pay as you go model. Due to this now days so many short-time requirement users use Cloud Computing services.

There are many MNC's providing the cloud services such as Amazon web services, Microsoft etc [1]. The Cloud services are Infrastructure as a service(Iaas), Platform as a service(Paas), Software as a service(Saas). Here, AWS EC2 instances are an example of Infrastructure as a service. Microsoft Azure is an example of a Platform as a service; Google apps are examples of Software as a service.

Because user-friendly, quickly to up the services and ease of doing business model, cloud services are used by many users. So Dynamic demand is there in cloud computing. Due to this,

Load balancing came into the picture in Data centre. Before to apply any algorithm in Data centre, we need to know about the performance of the algorithm. For this reason, we are working on the analysis of algorithms. In this paper, we analyze the performance of the algorithm in the Data Center using Cloud Analyst Simulator.

II. Load Balancing Algorithms

A. Round Robin Load Balancing Algorithm

Round Robin is the most straight forward algorithm that uses the concept of quantum time. In Round Robin, each virtual machine will get quantum time. Once quantum time completes, the turn will get another virtual machine. If the quantum time is very large, then the round-robin algorithm acts as an First come First serve.

The drawback of this algorithm is to determine the quantum time additional load on the scheduler, and it has higher context switches between the machines. so that it leads to increase the turnaround time.

B. Eq. Spread Current Execution load Balancing Algorithm

In this approach, the load balancer noted the list of all virtual machines and their availability. When a client requests the load balancer, it scans the entire virtual machine list and if any virtual machine found it will be allocated [1]. For equal load distribution, we suppose to calculate the current allocation of load on each virtual machine. It maintains a updated allocation table for handling equal load towards all virtual machines. It increases the throughput, and it has also it's own drawbacks.

C. Throttled Load Balancing Algorithm

A throttled algorithm is based on virtual machines data bases. That is, load Balancer will maintain a table databases of virtual machine id and also maintain their VM services like services are available (or) services are busy [3].

1. At the start, all VM's are available in the Data bases.
2. Data centre controller receives a new VM service re-request.
3. Data centre controller requests the Throttled VmLoad Algorithm for the allocation.
4. Algorithm checks the database from the start to the end of the data base.

If found:

- a. Load Balancer returns the VM id from data base to the controller.
- b. The controller notifies the new allocation of VM.
- c. Load Balancer updates the VM's status in the databases.

If not found:

- a. The Algorithm returns -1 (un sucessfull allocation).
- b. The controller place the new request in the queue.
5. If the virtual machine completes the task, the controller receives the response of task, it generate the a signal to load Balancer to de-allocation of virtual machine [3].
6. The Data Center controller checks if any waiting re-requests in the VMqueue. If any, continue from the step 3.
7. Continue from the step2.

III. Cloud Analyst Simulator

Many tool kits can be used to model a simulated Data centre environment. Cloud Analyst simulation enables the results to analysed easily and more efficiently. Let's brief the technical terms used in Cloud Analyst Simulator.

Zone: In the Cloud Simulator, the world map is split into six zones. User Bases and Data centres belong to any one of the six zones.

Internet: Real-world internet is the abstraction in Cloud Analyst Simulation. Due to internet traffic, it has transmission latency and transfer delays.

User Base: A userBase is a group of Cloud users considered a single unit in the Cloud Simulator. Sometimes, the single user base may consist of hundreds of users. The user base is the instrument to generate the load.

Internet Cloud-let: An Internet Cloud-let is a group of requests from the user. The Internet Cloud-let carries information such as input file, output file and execution command. In this paper Cloud-let and tasks are same as per the convenient we can use the terms.

Controller: Controller is the heart of Cloud Analyst Simulator. It will manage the activities like virtual machine creation and destruction in the Data Center environment.

VmLoad Balancer: The Controller uses a VmLoadBalancer to find which VM should be assigned the cloudtask for execution.

IV. Experimental Simulation Results

Simulation is the zero cost to test the load balancing algorithms in the Data centre. The world map was divided into six zones like Zone 0, Zone 1, zone 2, zone 3, zone 4 and, zone 5. Let us consider the Social Network Facebook users, which has more than two hundred million users worldwide.

Table 1: Facebook Users

Zonal Name	Zonal Id	No. of registered users
America (North zone)	0	80 million
America (south zone)	1	20 million
Europe zone	2	60 million
Asia zone	3	27 million
Africa zone	4	5 million
Oceania zone	5	8 million

To practice the simulator implementation, but on a measurement of 1/10 of the real time users considering. Let us define the six user databases representing the above mentioned six zones, with the mentioned parameters(Table II).

Table 2: User Database Configurations

User Base	Zonal Id	Time zone	peak hour (GMT)	online users peak hrs	online users non peak hrs
UB 1	0	GMT 6:00	- 13:00 - 15:00	4,00,000	40,000
UB 2	1	GMT 4:00	- 15:00 - 17:00	1,00,000	10,000
UB 3	2	GMT 1:00	+ 20:00 - 22:00	3,00,000	30,000
UB 4	3	GMT 6:00	+ 01:00 - 03:00	1,50,000	15,000
UB 5	4	GMT 2:00	+ 21:00 - 23:00	50,000	5,000
UB 6	5	GMT 10:00	+ 09:00 - 11:00	80,000	8,000

Each userbase is generating the user requests to the Data centre for processing the requests. The following are the Data Center configurations like the type of hardware, operating system, the cost for specific operations in the table (Table III).

Table 3: Data Center Configurations

Name	Data Center 1
Region ID Number	0
Architecture	X86
Operating System	Linux
Virtual Machine	Xen
Cost per Virtual Machine	0.1\$ / hr
Memory cost	0.05\$ / sec
storage cost	0.1\$ / sec
Data Transfer cost	0.1\$ / GB
Physical HardWare No's	2

A. Running a Simulation

Cloud Analyst Simulation will show the percentage of the simulation completed. The simulation screen will display an animation showing which user bases send messages to which data centres. It has a show region boundaries at the bottom right hand corner in the map to observe the map regions.

A Simulation can be cancelled at any time by using the cancel button at the bottom right-hand corner.



Fig 1: Simulation panel during a simulation

B. Overall response time

Response time can be measured as the total time taken to complete processing by the requested process. After Cloud Analyst Simulation, we observed three different algorithms results of overall response time, as reported in the given graph fig.2. The overall response time of Round robin is 300.9 ms, Equally spread current execution is 300.8ms, Throttled is 288.01ms. We conclude that Round Robin, Eq.spread current execution takes more response time which is not suitable for the load balancing algorithm. So throttled have less response time as compared to the other two algorithms.

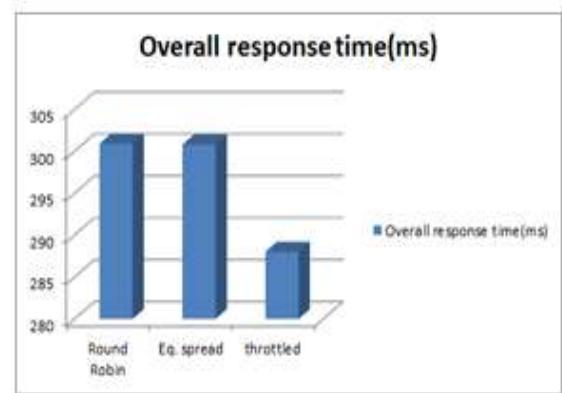


Fig 2: Overall response time

C. Data center processing time

Data centre processing time is the data centre's time for the load balancer to process the required requests. The Processing time for Round-robin is 25.98ms, Equal spread is 25.88ms, and Throttled is 13.22ms. Throttled is reasonable to compare to Round robin and Equal spread in Data center processing time from the graph.

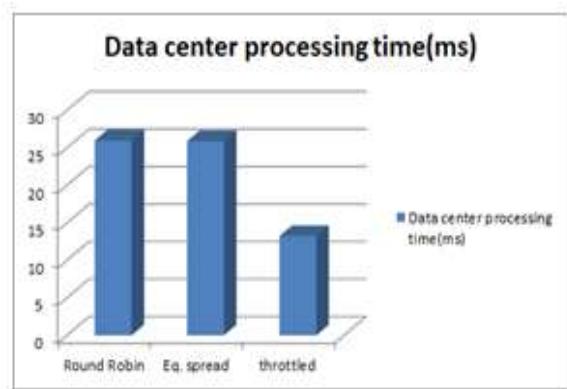


Fig 3: Data center processing time

D. Simulation Results Summary

After the Simulation, the result summary for the overall response time and Data centre processing time tabularized below.

Table 4: Performance Comparison

Algorithm	Overall response time(ms)	Data center processing time(ms)
Round Robin	300.9	25.98
Eq. spread	300.8	25.88
throttled	288.01	13.22

Cloud Analyst Simulation has rich potential in identifying and experimenting with mechanisms

and algorithms to improve performance in Cloud applications.

V. Conclusion

We can conclude which algorithm is best based on the total response time and data centre processing time from the above simulation result. As per Simulation results, load balancing algorithms performance depends on many factors such as which policy using and requests from the user base. Our research concludes that the Throttled load balancing algorithm is the best simulation results as compared to other two algorithms.

References

- [1] Singh, Archana, and Rakesh Kumar. "Performance Evaluation of Load Balancing Algorithms Using Cloud Analyst." 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence). IEEE, 2020.
- [2] Volkova, Violetta N., et al. "Load balancing in cloud computing." 2018 IEEE conference of russia young researchers in electrical and electronic engineering (EICoRus). IEEE, 2018.
- [3] Buyya, Rajkumar. "CloudAnalyst: A CloudSim-based tool for modelling and analysis of large scale cloud computing environments." Distrib. Comput. Proj. Csse Dept. Univ. Melb (2009): 433-659.
- [4] Narale, Snehal A., and P. K. Butey. "Throttled load balancing scheduling policy assist to reduce grand total cost and data center processing time in cloud environment using cloud analyst." 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT). IEEE, 2018.
- [5] Gao, Guanyu, et al. "Resource provisioning and profit maximization for transcoding in clouds: A two-timescale approach." IEEE Transactions on Multimedia 19.4 (2016): 836-848.
- [6] Chen, Zheyi, et al. "PSO-GA-Based Resource Allocation Strategy for Cloud-Based Software Services With Workload-Time Windows." IEEE Access 8 (2020): 151500-151510.
- [7] Yamini, R., and M. Germanus Alex. "Comparison of resource optimization algorithms in cloud computing." International Journal of Pure and Applied Mathematics 116.21 (2017): 847-855.
- [8] Seddigh, Milad, Hassan Taheri, and Saeed Sharifian. "Dynamic prediction scheduling for virtual machine placement via ant colony optimization." 2015 Signal Processing and Intelligent Systems Conference (SPiS). IEEE, 2015.
- [9] Liu, Meng, et al. "A decentralized cloud firewall framework with resources provisioning cost optimization." IEEE Transactions on Parallel and Distributed Systems 26.3 (2014): 621-631

Session-B4:
RF Communications and Applications

Performance Evaluation of GNSS system using Z-test for RAIM

D. Sony

Department of ECE

Chaitanya Bharathi Institute of Technology(A)
Hyderabad-500075, India

Dr. D. Krishna Reddy

Department of ECE

Chaitanya Bharathi Institute of Technology(A)
Hyderabad-500075, India

JB Farheen

Department of ECE

Chaitanya Bharathi Institute of Technology(A)
Hyderabad-500075, India

Dr. P. Naveen Kumar

Department of ECE

Osmania University College of Engineering
Hyderabad-500007, India

Abstract: Critical applications such as civil aviation sector are the one that requires integrity assurance information related to the signals received from the positioning systems. Receiver Autonomous Integrity Monitoring (RAIM) is a technique that is used to assess the integrity of the signals received from satellite systems. Global Navigation Satellite System (GNSS) systems provides signals, which used for various applications, aviation sector is one such application which uses the signals obtained from satellites for position estimation, but there is a possibility that GNSS systems provide incorrect information. Hence, it is required to evaluate the integrity of the signals received from satellite systems to be used for safety critical applications. In this paper, a new methodology is proposed using Z-test to indicate the level of accuracy of the signals obtained from satellites.

Keywords: integrity, RAIM, level of accuracy, Z-test

I. Introduction

Satellites broadcast information which is received by the user and it is used for position and timing information. Satellites are susceptible to faults and hence results in the errors when used in position estimation [2]. Therefore, it is necessary to give an indication related to the accuracy obtained and thus commenting on the integrity.

Integrity is termed as the level of trust that one can place on information transmitted by the satellite systems. Integrity performance can be evaluated if the accuracy is measured. For safety critical applications like aviation integrity is crucial and also the key parameter for receiver autonomous integrity monitoring (RAIM).

II. Methodology

In this paper the integrity monitoring of GNSS system is carried out, by performing statistics (proportions and Z-score used) on a sample of data

and then estimating the reliability of whole by using sample data.

The steps involved in the implementation are indicated below:

1. The pseudoranges from the observation file are extracted and stored (pseudoranges observed).
2. The satellite position is calculated from RINEX navigation file and pseudorange is calculated based on satellites position and receiver position (pseudorange calculated).
3. The difference between calculated values and observed values are estimated.
4. The critical values (Z-score) is taken for confidence levels like 90, 95%
5. Using the critical values corresponding to the specified confidence level, margin of error is computed and the final proportion of population is estimated.

The satellite coordinates have been calculated from ephemeris data [3] (taken from RINEX Navigation File), and also, they are validated by its corresponding sp3 file. The calculated range values are estimated from the satellite coordinates and the receiver coordinates, by computing the transit time of signal.

The threshold is estimated using z-test for different levels of errors. The formula used for calculation of Z-score is given below by equation (1).

$$Z = \text{norminv}(\text{prob}, \mu, \sigma) \quad (1)$$

Where $Z = Z\text{-score}$ (threshold)

$\text{prob} = \text{sample average}$

$\mu = \text{mean}$

$\sigma = \text{standard deviation}$

$$\text{MOE} = Z * \sqrt{\frac{\hat{q} * \hat{p}}{n}} \quad (2)$$

$Z = Z\text{-score}$

$\hat{p} = \text{proportion of success of event}$

$\hat{q} = \text{proportion of failure of event}$

$n = \text{sample size}$

Margin of Error (MOE), in statistics, shows the degree of error in the results received from random sampling survey. The higher the margin of error, it indicates that the likelihood of relying on results of a survey or poll is less, which says, the confidence on the results will be lower to represent a population.

$$\hat{p} - MOE < P < \hat{p} + MOE \quad (3)$$

The above equation (3) gives us the range in which the population proportion lies (Confidence Intervals) corresponding to the confidence levels (99% or 95%).

Using these confidence intervals one can predict if the data is reliable or not, if the statistic parameter (here proportion) obtained for the population is within the desired limits, it can be stated that the data is reliable.

The Receiver Position is also calculated with calculated pseudoranges using Bancroft algorithm [4].

If x_u , y_u and z_u represent the unknown coordinates of the user position and x_j , y_j , z_j , (where $j = 1, 2, 3, 4$) represent the known positions of Satellite Vehicles in the ECEF coordinate system, the user position (3-D) and the time offset t_u (between satellite clock and receiver clock) are obtained by solving the nonlinear equation (4).

$$\rho = \sqrt{(x_j - x_u)^2 + (y_j - y_u)^2 + (z_j - z_u)^2 + ct_u} \quad (4)$$

Where 'c' is velocity of electromagnetic signals in free space (m/s).

The range measured from satellites is called pseudorange as the bias in the receiver clock prevents the correct measurement of actual range (true range). To calculate the receiver position accurately, all the errors like ionospheric delay, tropospheric delay, Relativistic effects and the Satellite clock bias have to be estimated.

III. Results and Discussions

The RINEX navigation file and observation file are taken from the CDDIS website (<https://cddis.nasa.gov/archive/gnss/datadaily/2017/264/170/> from CKSV, located in Cheng Kung University). The observation data of 21st September 2017 from (0hrs. 0 min. 0 sec. to 22hrs. 0min. 0sec.) have been used. The satellites available at the epoch time have been considered. Satellite position is estimated at the epoch time. All calculations have been carried out by writing programs in MATLAB.

A sample of data is taken and the difference in the pseudoranges (i.e Corrected and Calculated) for the available epochs has been computed, the count of values based on hours of a day is shown in Fig. 1, then statistics has been performed on the taken sample to evaluate the integrity of whole data.

The test statistic used here is proportion parameter and Z-score value is used as critical value.

For the sample taken, the errors have been grouped like (<25m, <50m, <70m, >70m), the success proportion for each of these has been computed and the proportion of the same can be estimated for whole data with 95% and 99% confidence level.

It has been estimated that with 95% confidence level, the proportion of error in pseudoranges (>70m) lies between 2-11%

the proportion of error in pseudoranges (<50m) lies between 14-30%

the proportion of error in pseudoranges (<25m) lies between 25-45%

It can be observed that the proportion of error (>70m) is less and the proportion of error for (<25m) is around 25-50%, which says the data is likely to be reliable if error of 25m is considerable.

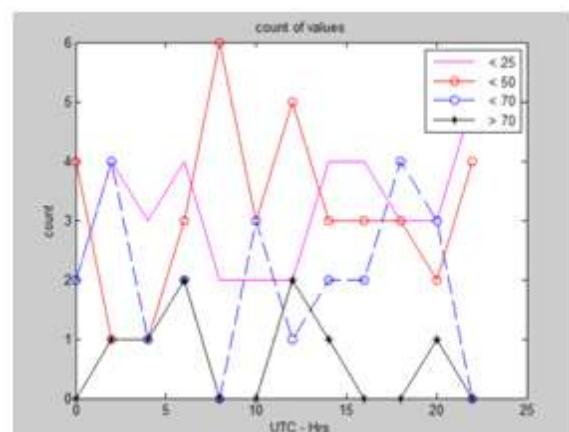


Fig 1: Hourly count of values for the specified levels.

These calculated pseudoranges, are then used in calculation for receiver position which is done using Bancroft algorithm.

The results shown in Fig. 2 are for the observed satellites available from 0 hours, 0 minutes and 0 seconds of 21st September 2017 to 22 hours, 0 minutes and 0 seconds of 21st September 2017.

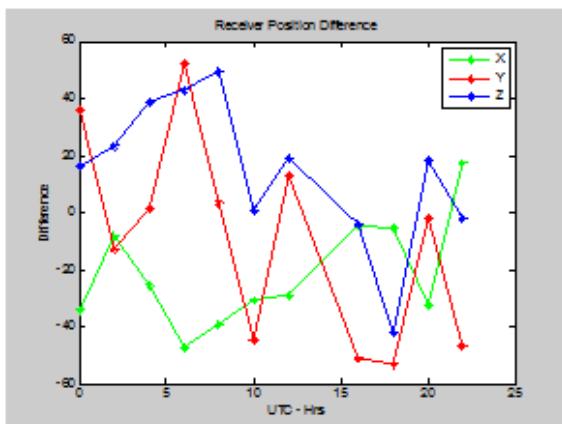


Fig 2: Error in Receiver position X, Y, Z in metres (m).

User Position as per the observation data:

$X_u = -2956619.139$ m, $Y_u = 5075902.277$ m and

$Z_u = 2476625.565$ m.

User position by Bancroft algorithm at 0hrs 0min 0sec is:

$X_u = -2956653.237$ m, $Y_u = 5075937.897$ m and $Z_u = 2476641.467$ m.

IV. Conclusion

In this paper the methodology for evaluating the integrity of GNSS signals using z-test has been outlined. It was observed that with 95% confidence level, the proportion of error (> 70 m) is found to lie between 2-11% and the proportion of error (< 25 m) is between 25-45% for the same level of confidence for that particular day's data.

References

- [1] Indian Regional Navigation Satellite System — Signal in Space ICD for Standard Positioning Service, version 1.0, June 2014 (Indian Space Research Organization, Bangalore 2014).
- [2] P.Misra and P.Eng, “Global Positioning System: Signals, Measurements and Performance”, Ganga-Jamuna Publishers, 2001.
- [3] Geoffrey Blewitt, “Basics of the GPS Technique: Observation Equations”, Department of Geomatics, University of Newcastle Newcastle upon Tyne, NE1 7RU, United Kingdom geoffrey.blewitt@ncl.ac.uk.
- [4] Bancroft. S, “An algebraic solution of the GPS equations”, IEEE Transactions on Aerospace and Electronic Systems 21 (1985) 56–59.
- [5] Sony; V. Satya Srinivas; P. Naveen; D. Krishna Reddy, “IRNSS User Range Accuracy Evaluation for Receiver Autonomous Integrity”, 2019 URSI Asia-Pacific Radio Science Conference (AP-RASC), 20 June 2019.
- [6] Mathieu Joerger; Stefan Stevanovic; Samer Khanafseh; Boris Pervan, “Differential RAIM and relative RAIM for orbit ephemeris fault detection”, Proceedings of 2012 IEEE/ION Position, Location and Navigation Symposium.
- [7] M. Udaya, D. Sony, Dr. D. Krishna Reddy, “Design of IRNSS Tracking System using 1.5 bit ADPLL and Correlator”, (IJITEE) ISSN: 2278-3075, Volume-9, Issue-10, August 2020.

Analytical Study of Global Solar Radiation Estimation and Forecasting methods: a Review

Deepa Rani Yadav

Department of Electronics and
Communication Engineering

Amity School of Engineering and Technology,
, Noida- 201303, India
deepayadav201092@gmail.com

Stuti Shukla Datta

Department of Electronics and
Communication Engineering

Amity School of Engineering and Technology
Noida- 201303, India
ssdatta@lko.amity.edu

Abstract: Solar radiation estimation is of utmost importance and the future of sun's energy has amazing potential. Estimation is based on various expressions and factors such as ambient temperature, relative humidity, sunshine duration etc. It is of utmost importance as it will provide the practical knowledge of radiation data received and distributed at particular geographical location which will lead to efficient utilization. The models for such estimation and prediction are Markov processes based model which is a random process and works with large data . Sunshine duration is the most important parameter here, recording of radiation data is done on day, monthly hour basis or minute basis, which will result in larger dataset availability. Prediction with large dataset leads to lesser errors and hence more accuracy. This paper deals with the analytical study and comparison of various models of solar radiation estimation both linear, non-linear and the performance of AI based ANN techniques for forecasting global solar radiation. The result shows that large data availability forms the basis of estimation, AI techniques based models have lesser justifications with respect to their outcomes and is more accurate as the result is based upon the learning experiences and the model that is efficient in consecutive time series analysis with easy and accurate prediction is presented.

Keywords: ANN, Global Solar Radiation, Markov process, Sunshine duration.

I. Introduction

Sun is an ultimate source of energy with its potential being beyond imagination. Sun is a richest energy source with giving huge amount of energy to the planet earth which will never run out[1]. It has various advantages and vast applications in almost every field. With rapidly increasing energy demands of various sectors including both industrial as well as economical world, usage of this utmost energy source will be very beneficial in both of its availability as well as its cost. So, sun's energy has vital role to play in the energy world.

II. Basic Considerations

The radiation from sun reaches to earth by experiencing long distance journey under which the radiation faces and interacts with various objects which greatly affects the radiation[2]. Hence, these objects need to be considered carefully for accurate examination and modeling of Global solar radiation. These radiations can be classified into 3 types –

1. Direct
2. Diffuse
3. Reflected

When all these 3 radiations are received by earth is called as Global Solar Radiation.

The various fundamental parameters that greatly affects Global Solar Radiation are-

1. **Atmospheric parameters-**
Water vapour, Aerosole optical depth
2. **Environmental variables-**
Altitude, Terrain shading, Air temperature
3. **Solar geometry-**
Azimuth angle, Zenith angle
4. **Various atmospheric conditions-**
Humidity, ambient temperature, cloud conditions, rainfall etc.

On the basis of these basic parameters the models can be also be categorized differently[4].

These various categories can be subdivided into clear sky and cloud based models along with some other type of transposition and terrain models.

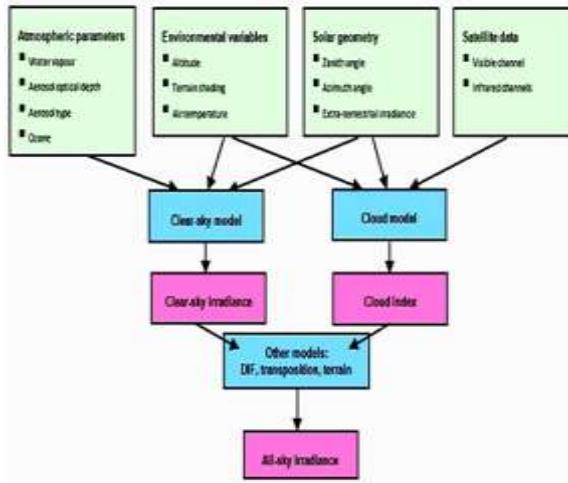


Fig 1: Fundamental parameters of Solar Radiation

The main factor that forms the basis of radiation estimation as well as prediction is sunshine duration. Estimation can be done by taking monthly mean, daily radiation or on hour basis. With hourly radiation, it will lead to more data, radiation changes can be recorded accurately which will ultimately lead to less errors thereby allowing more accurate estimation[3].

III. AI Based Methodology

The term AI stands for Artificial Intelligence which is a brain inspired intelligent machine. It is a emerging technology and has wide applications in various domains also it can perform complex task easily with less efforts and complexity. The performance is based on the structure of neurons in human brains[6]. AI based techniques are as follows-

1. Artificial Neural Network
2. Fuzzy logic
3. Expert system
4. Wavelet Neural Networks
5. Genetic Algorithm

ANNs

Artificial Neural Networks is a layered architecture with various units involved which forms the basis of processing. These units are connected with each other in different layers- input layer, hidden layer, output layer. The output is basically some of incoming data from hidden layer. The operation with ANN is based upon their training, they need training dataset to perform the task hence they have the capability to process with number of data[5]. There can be 1 input layer, 1 output layer but can be even more than hidden layers. In between input layer and hidden layer we basically use a function that signifies the relation between input and hidden layer, this function is multiplication function.

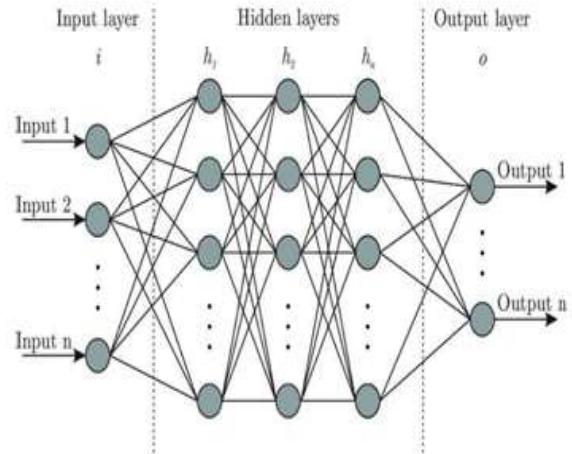


Fig 2: ANNs layered architecture

There can be no. of inputs, no. of outputs, single input layer, single output layer, single or multiple hidden layer, hence it is capable of dealing with multiple inputs which forms the basis of training and testing dataset. It is emerging technology, provides great accuracy, solves complex problems easily, it is speedy technique with the only requirements of imagination and data with the help of which it will create revolution in the future of energy world.

Fuzzy logic

Fuzzy as its name specifies, means vague logic which basically meant for cases of uncertainties which helps in dealing with inaccuracies and hence produces accurate results[8]. There is no exact true value or false value, it raises the chances of uncertainties i.e., the case of partially true or false. For clear description of fuzzy logic, let us consider a example in the figure given below

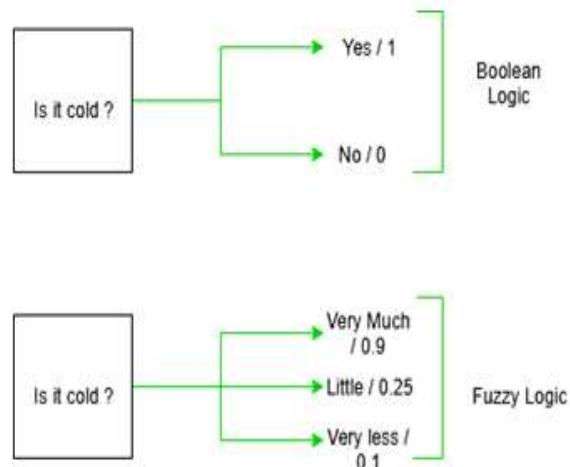


Fig 3: Fuzzy and Boolean logic comparative description

- under which let us make a comparison between Boolean logic and Fuzzy logic, for determining the true or false chances of the cold or not cold atmosphere, taking 1 as true value and 0 as false value. This technique can greatly coordinate in radiation estimation as it can process with any type of data value with any kind of corrupted information, it has simplified way of problem solving technique, and efficient technique resembling simple calculations that we humans tend to do[7].

Expert System

The expert system of AI technique is based upon static and dynamic knowledge base. These knowledge base comprises of various informations regarding recorded data, radiation affecting parameters, various rules and procedures to follow. Hence, these knowledge base for basis for radiation estimation considering various informations and rules related to parameters affecting[12]

Genetic Algorithm

Genetic algorithms helps in finding optimized solutions. As its name specifies, this algorithm is based upon the genetic concepts and ideas. Genetic algorithms are applicable to the areas or objects that are adaptable to environmental changes and still processing and surviving efficiently. In this hostile world, nothing is permanent, everything is changing wth time continuously and the living beings need to be adptive to these changes, GA is inspired by this survival features and strategies of living organisms[12]

GA is based upon three basic operations-

1. Selection-

Selecting the living being which is surviving their best. Fitness score of the living being leads to his/her selection/rejection

2. Crossover-

Crossover is a randomly chosen point fpr creating the offspring

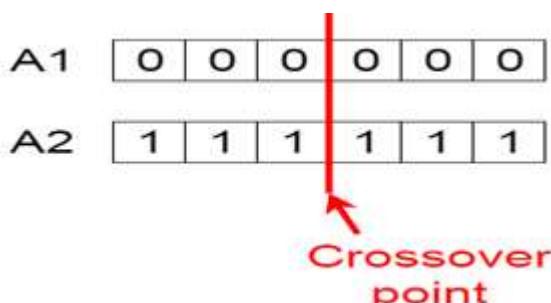


Fig 4: considering randomly a crossover point

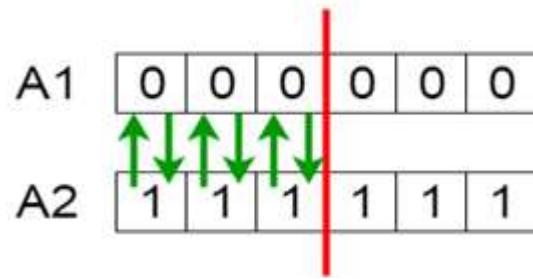


Fig 5: Exchange of genes

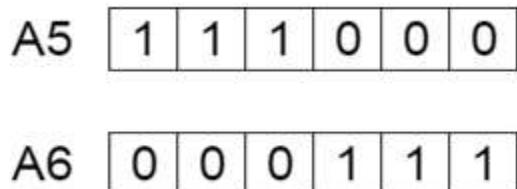


Fig 6: result of crossover exchange

3. Mutation-

Mutation refers to flipping . for clear understanding of the concept mutation , lets have a look at figure 4

Before Mutation

A5	1	1	1	0	0	0
----	---	---	---	---	---	---

After Mutation

A5	1	1	0	1	1	0
----	---	---	---	---	---	---

Fig 7: Process of Mutation

Since GA has special feature of adaptability with the changes, it allows efficient Global Solar Radiation estimation as the radiation is greatly affected by various atmospheric parameters such as temperature, humidity, sunshine hour, cloud conditions, rainfall etc.[9]. By making use of Genetic Algorithm, it follows survival of the fittest and hence recorded data remains undisturbed which leads to efficient prediction as well as utilization.

IV. Machine Learning Based Methodology

Machine learning is another efficient AI technique which is applicable to the cases which are impossible to have explicit algo. And exact representation. Hence machine learning methods finds solution to the complex cases such as pattern recognition, in making predictions etc.

Ensemble Methods

Ensemble methods combines number of machine learning algorithm into a single valued output which is utilized in estimation and forecasting. Since it combines multiple machine learning algos. Hence, it results in mature outcomes with less errors and hence more accuracy. Decision trees forms the basis of these ensemble methods, these decision trees comprise of various branches which is reflecting the values that may be used for prediction hence because of number of branches involved in making decisions, the process is time taking[9].

Bagging: It ensures accurate and stable output. It is also called as Bootstrap Aggregating under which, bagging is applied to the various branches of decision tree and result is aggregated at the final output hence it also avoids overfit outputs and results in accurate result. To understand the concept of bagging, let us consider fig.8 showing the decision tree diagram with bagging operation under which the final result is obtained by aggregating the possible estimated values. Bagging also has its application in regression analysis and can be applicable to not only machine learning algorithms but to various other learning methodologies to have aggregate result. It can also be considered as a kind of averaging technique.

Random Forest: It is similar to bagging concept with the difference that here the result of various branches of decision trees are not aggregated, they are compared instead to have better predictions. It is based upon proposed way of problem solving which is again comprised of decision trees. In this kind of ensemble methodology the output of decision trees may result into single or multiple branch[10]. These single or multiple branches are then made into comparative examination to have better estimation and hence prediction which can provide efficient Global Solar Radiation estimation.

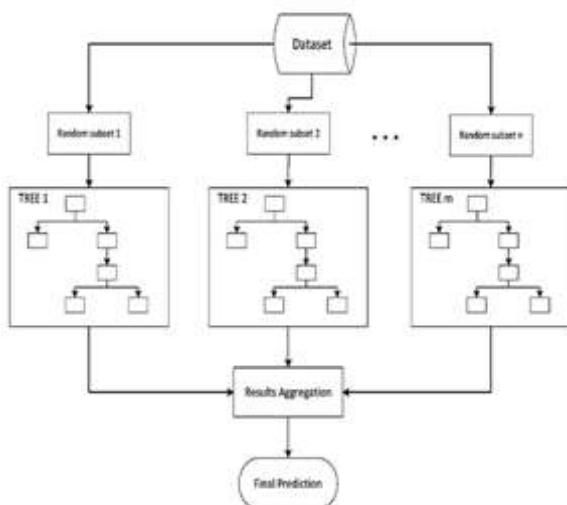
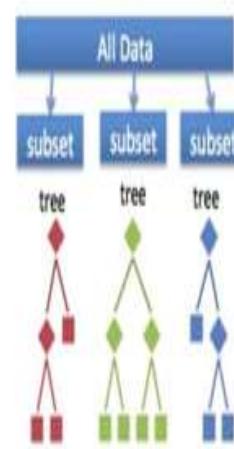


Fig 8: Bootstrap Aggregation



A random forest takes a random subset of features from the data, and creates n random trees from each subset. Trees are aggregated together at end.

Fig 9: Random Forest Ensemble method

V. Different Models for Global Solar Radiation Estimation

Many researchers have emphasized various modeling techniques for Global Solar Radiation Estimation. For radiation estimation there is a great need of radiation data to be made available and details about the related location such as azimuth angle, latitude, longitude, altitude[12]. By making use of modeling techniques all the mentioned requirement for efficient estimation and prediction of GSR is fulfilled. The models can be of various types based on various parameters, categorizing the models as-

1. Sunshine duration based
2. Monthly/daily/hourly average estimation based
3. Temperature, cloud. and various atmospheric condition based

The modeling can be categorised on the basis of linearity of the recorded data, number of input parameters and type of meteorological parameters such as sunshine duration, temperature, humidity, cloud conditions geographical location etc. for detailed description of modeling referring to figure 10 below.

Non- Linear modeling

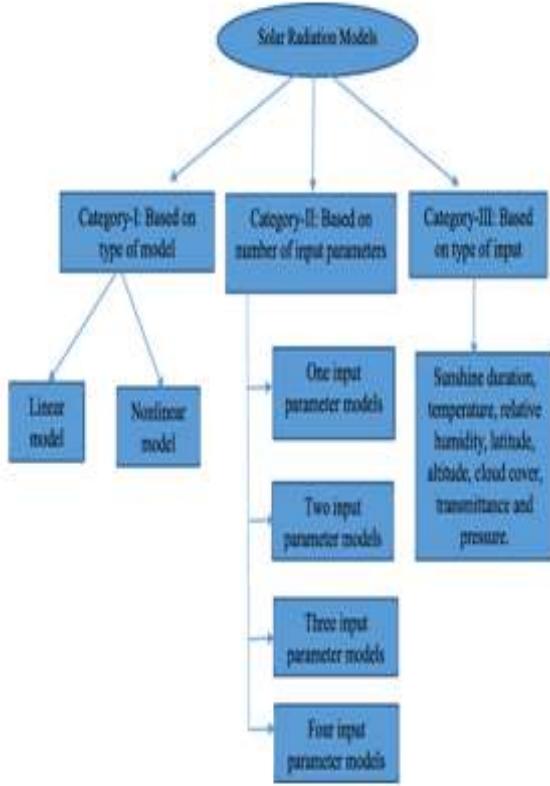


Fig 10: GSR model categorization

Table 1: AI based GSR applications

AI technique	Area	Number of applications
Artificial neural networks	Prediction of solar radiation	11
	Modelling of solar steam-generator	1
	Prediction of the energy consumption of a passive solar building	1
	Characterization of Si-crystalline PV modules	1
	Efficiency of flat-plate solar collectors	1
	Heating controller for solar buildings	1
Fuzzy logic	Modelling of a solar air heater	1
	Photovoltaic solar energy systems	2
	Sun tracking system	1
	Prediction of solar radiation	5
	Control of solar buildings	1
Adaptive Network based Fuzzy Inference System	Controller of solar air-conditioning system	2
	Prediction of solar radiation and temperature	3
Genetic algorithms	Photovoltaic solar energy systems	2
	Determination of Angstrom equation coefficients	1
	Solar water heating systems	2
	Hybrid solar-wind system	2
	PV-diesel hybrid system	2
	Solar cell	1
	Flat plate solar air heater	1
Data Mining	Solar cell	1

Non linear modelling are based on AI techniques. Non – linear modeling forms the intelligent model for efficient forecasting. Since these are the intelligent machines with human brain mimicking which is based on large data set with which it learns and experiences. Hence results in less errors and more accurate outcomes[13]. AI based techniques are discussed in detailed form in section 3 of this paper. Various AI based models for GSR prediction and its application in solar energy world are listed in the table below.

VI. Conclusions

Solar energy has amazing future. With growing demands in energy sector, there is great need of energy source, sun is an ultimate energy source which has countless advantages and applications . There will never be scarce of this renewable and sustainable energy source as it is available in huge amount. So to make best possible use of it, its accurate estimation and prediction is an attractive issue. As per this study there are various methodologies , techniques and models available to estimated and forecast GSR. These various methods have different parameter dependencies, different features, different processings and differ in advantages and applications. Various Linear models involves equations and coffecients with related characteristics whose accuracy is a major concern[14]. Among various categories of linear and

non linear models available for radiation data estimation, AutoRegressive Moving Average model proves to be easier, efficient and accurate model for radiation estimation, it is suitable for time series analysis and gives accurate radiation prediction.

As per this study, among various available methodologies discussed for radiation estimation which is a critical issue, ANN based techniques are emerging technologies. It is capable of handling and solving complex and even impossible tasks with great ease and flexibility. So we have variability in estimation techniques among which ANN based techniques are unique, interesting and amazing with good accuracy. With the availability of radiation data ANN techniques can be helpful in upgrading the present and forecasting the future which will ultimately bring tremendous benefits in energy world in the near future.

References

- [1] Amit Kumar Yadav , S. S. Chandel .Solar radiation prediction using ANN techniques : A review . Renewable and sustainable energy review . Volume 5 , issue 4 , December 2001 . Elsevier science Ltd.
- [2] Deepa Rani Yadav, Dr. Deependra Pandey. Analytical study of ANN modeling based estimation of solar radiation, IOSR journal of engineering (IOSR JEN) .National seminar cum workshop on “Data science and information security 2019”
- [3] Junliang Fan, Haiyang Zou. Empirical and machine learning models for predicting daily global solar radiation from sunshine duration: A review and case study in China. Renewable and sustainable energy reviews. Science Direct Volume 100, Feb 2019
- [4] N. Kumar, S.P.Sharma, U.K.Sinha, Y. Nayak. Prediction of solar energy based on intelligent ANN modeling, International journal of renewable energy research, S.P.Sharma et al, Vol. 6, No.1, 2016.
- [5] Ahmet Teke, H. Basak Yildirim, Ozgur celik. Evaluation and performance comparison of different models for the estimation of solar radiation. Renewable and sustainable energy reviews. 1364-0321/ 2015 Elsevier ltd.
- [6] Atsu SS Dorvlo, Joseph A Jervase, Ali Al Lawati. Solar Radiation estimation using Artificial Neural Networks. Applied Energy 71 (4). 307-319, 2002
- [7] M Mohandes, S Rehman, T O Halawani. Estimation of Global Solar radiation using Artificial Neural Networks. Renewable Energy 4 91-40, 179-184, 1998
- [8] Koray Ulgen, Arif Hepbasli. Diffuse Solar Radiation estimation models For Turkey's big cities. Energy Conservation and management 50(1), 149-156, 2009
- [9] M Chegaar, A Chibani. Global Solar Radiation in Algeria. Energy Conservation and Management 42 (8), 973, 2001
- [10] Mossad El-Metwally. Sunshine and Global Solar Radiation Estimation at different sites in Egypt. Journal of Atmospheric and Solar-Terrestrial Physics 67 9140, 1331-1342, 2005
- [11] Soteris A. Kalogirou. Artificial Neural Networks in renewable energy systems applications : a review . Renewable and sustainable energy reviews. 2001 Elsevier Science Ltd.
- [12] Cyril Voyant, Gilles Notton, Soteris Kalogirou, Marie Laure Nivet, Christophe Pouli, Fabrice Motte, Alexis Fouilloy. Machine Learning methods for Solar Radiation Forecasting : A Review. Renewable Energy. 0960-1481/2017 Elsevier ltd.
- [13] Abasheer M. H. Ajmeer . Artificial neural networks : fundamentals , design , computing and applications , journal of microbiological methods , vol 43 , issue 1 , 1 Dec 2001 , Elsevier Science Ltd.
- [14] Jianyuan Zhang Li Zhao , Shuai Deng , Weicong Xu , Ying Zhang . A critical review of models used to estimate solar radiation , Renewable and sustainable energy reviews 70(2017) 314-329 , Elsevier Ltd.

Satellite Selection Algorithm for RAIM Applications

D.Sony

dept. Electronics Communication Engineering.
Chaitanya Bharathi Institute of Technology(A).
Hyderabad-500075,India.
sonyd_ece@cbit.ac.in.

S.Chandravadhan

dept.Electronics and Communication Engineering.
Chaitanya Bharathi Institute of Technology(A).
Hyderabad-500075, India.
pgs19004_ece.chandravadhan@cbit.org.in.

Dr.D.Krishna Reddy

dept.Electronics and Communication Engineering.
Chaitanya Bharathi Institute of Technology(A) .
Hyderabad-500075,India.
dkreddy@cbit.ac.in.

Dr.P.Naveen Kumar

dept. Electronics and Communication Engineering.
Univeristy College of Engineering.
Osmania University,
Hyderabad-500007,India.
drnaveenkumar.agrl@gmail.com

Abstract: Accuracy is one of the most important parameter to be analyzed for receiver autonomous integrity monitoring (RAIM) applications. Accuracy can be defined in terms of DOP, which specifies the geometry of the satellites. The multi-constellation receiver systems receive signals from many satellites, so it is very important to select a set of satellites from the visible set corresponding to a particular constellation. RAIM is used to assess the trust that the user can place on the information received from satellites for position estimation. Hence it is required to select the satellites with better geometry (to provide more accuracy) from the visible set. The optimal subset with computation of minimum GDOP value will be best suited for selecting satellites subset for receiver autonomous integrity monitoring (RAIM). In this paper, the subset selection is implemented for IRNSS and GPS systems based on minimum DOP values estimated.

Keywords: GDOP, RAIM (Receiver autonomous integrity monitoring), Satellite subsets.

I. Introduction to Satellite Selection

Satellite navigation systems accuracy depends on the constellation geometry (DOP) [2]. The satellite selection is made by choosing the subset of satellites with criteria of minimum Geometric dilution of precision (GDOP) [1] value among the group of subsets of satellites in view. The subsets are different for different constellations; it is difficult to choose the satellite subset from the geometric distribution of satellites in space. The GDOP value varies based up on geometric distribution of satellites in space. The closely spaced geometry of satellites gives poor GDOP (results in high position errors), similarly the wider distribution gives good GDOP[2] (results in low position errors).Maintaining the Integrity of the Specifications.

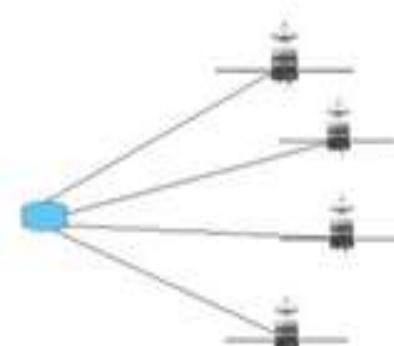


Fig 1: Poor GDOP

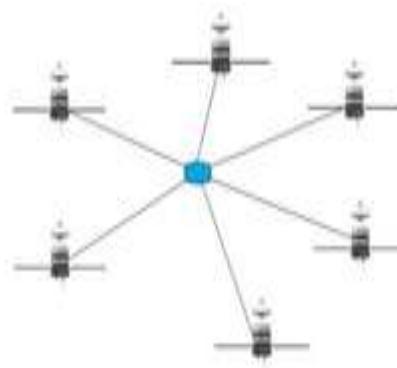


Fig 2: Good GDOP

Table 1: Typical values of DOP

DOP value	Rating
1	Ideal
1-2	Excellent
2-5	Good
5-10	Moderate
10-20	Fair
>20	Poor

III. Introduction to RAIM

Receiver autonomous integrity monitoring is used to provide integrity for navigation systems. Whenever the satellite system cannot be used to for the navigation the trust on the services provided by satellite navigation system is issued by providing timely warnings[3],[4]. The failures may be caused by various factors such as electronic failures on satellites, satellite ephemeris and clock model biases of satellite broadcast, abnormal atmospheric delays and receiver failures [6]. The integrity monitoring is used to control the occurrence of these events up to a large extent. Receiver Autonomous Integrity Monitoring (RAIM) [3] is used to monitor the consistency of the receiver's internal redundancy observations. It is mandatory to identify the fault associated with the satellites and provide reliable services (fault exclusion). The inclusion of traditional Geometrical dilution of precision method with minimum value provides the RAIM algorithm for selecting the satellites subset for integrity monitoring.

IV. Implementation of Satellite Selection Algorithm

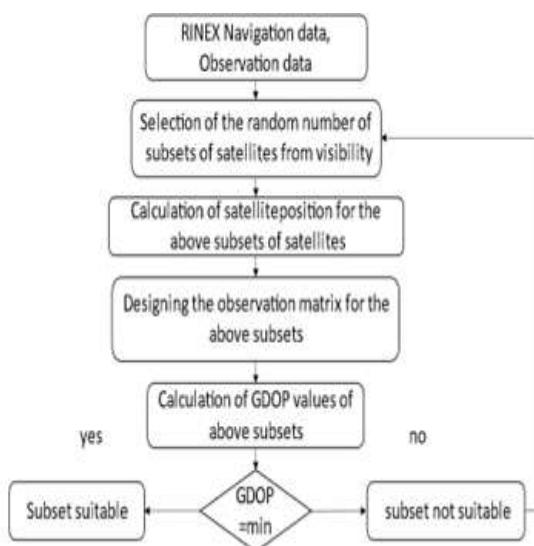


Fig 3: Flow chart for Satellite selection algorithm for IRNSS & GPS.

The following steps to be followed for satellite selection algorithm

A. RINEX Navigation data, Observation data:

The RINEX Navigation data, observation data obtained from the Receiver.

B. Selection of random number of subsets of satellites from the visibility:

Random number of satellites are selected from visible number of satellites available.

Ex:2,3,5,8,7.....N

N=number of satellites.

C. Designing of observation matrix for above subsets:

If there are N visible satellites, the observation matrix [4] is

$$H = \begin{bmatrix} L_{11} & L_{12} & L_{13} & -1 \\ L_{21} & L_{22} & L_{23} & -1 \\ \vdots & \vdots & \vdots & \vdots \\ L_{N1} & L_{N2} & L_{N3} & -1 \end{bmatrix}$$

H= pseudo range observation matrix of size Nx4
Where

$$L_{11} = (X_c - X_e)/R_i$$

$$L_{12} = (Y_c - Y_e)/R_i$$

$$L_{13} = (Z_c - Z_e)/R_i$$

$$R_i = \sqrt{(X_c - X_e)^2 + (Y_c - Y_e)^2 + (Z_c - Z_e)^2}$$

$$i=1,2,3,5.....N$$

$$(X_c, Y_c, Z_c) = \text{Satellite position}$$

coordinates.

$(X_e, Y_e, Z_e) = \text{ECEF receiver}$
coordinates.

D. Calculation of GDOP values for above subsets:

GDOP: (geometric dilution of precision)

It is the error caused by the relative position of the satellites [1],[5].

$$\text{GDOP} = \sqrt{\text{trace}(H^T H) - 1}$$

H= Pseudo range observation matrix of size Nx4.

V. Data Acquired

The Satellite Selection Algorithms of GDOP values of IRNSS system are obtained from the navigation data. The broadcast ephemeris data is acquired from ACCORD receiver (CBIT). The navigation data collected in 21st September 2017. Similarly of GDOP values of GPS system are obtained from the navigation data. The broadcast ephemeris data is acquired from the navigation data the Crustal Dynamics Data Information System (CDDIS) archives maintained by NASA. The daily files are accessed from the following link

<https://cddis.nasa.gov/archive/gnss/data/daily/2019/059/19n/>

VI. Results & Discussions

Table 2: GDOP values of different subsets for GPS system

PRN numbers of Satellite Subsets	GDOP Values
(10,14,15,20,24)	8.2307
(10,14,15,20,27)	2.5730
(10,14,15,24,27)	2.8106
(10,14,20,24,27)	2.4407
(10,15,20,24,27)	2.9697

Table 2 indicates that the GDOP values of GPS for different subsets of satellites. The subset (10,14,15,20,24) has maximum GDOP value i.e., 8.2307 the subset (10,14,20,24,27) has minimum GDOP value i.e., 2.4407. Therefore, based up on criteria, the combination of satellites with minimum value of GDOP i.e., 10,14,20,24,27 would be suggested for RAIM applications.

Table 3: GDOP values of different subsets for IRNSS system

PRN numbers of Satellite Subsets	GDOP Values
(2,3,4,5,6)	5.9504
(2,3,4,5,7)	12.2849
(2,3,4,6,7)	4.5134
(2,3,5,6,7)	4.5097
(2,4,5,6,7)	7.0871

Table 3 indicates that the GDOP values of IRNSS for different subsets of satellites the subset (2,3,4,5,7) has maximum GDOP value i.e., 12.2849

and the subset (2,3,5,6,7) has minimum GDOP value i.e., 4.5097. Therefore, based up on criteria the minimum value of GDOP with combination of satellites 2,3,5,6,7 is selected for RAIM applications.

VII. Conclusions

To implement the receiver autonomous integrity monitoring (RAIM) for the IRNSS & GPS the selection of satellites is mandatory. The satellite selection algorithm is implemented for GPS&IRNSS systems. From the Table (3) it can be indicated that for the IRNSS system the DOP value is better if the subset consists of maximum number of GEO satellites (i.e., the set consisting of 3GEO satellites and 2 GSO satellites is giving minimum DOP value-4.5097) than the subset consisting of maximum number of GSO satellites (DOP value -12.2849).

References

- [1] Tian, Anhong, Fu, Zhou, Mu. A new satellite selection algorithm in GNSS.2013 6th International Conference on Information Management, Innovation Management and Industrial Engineering. doi:10.1109/iciii.2013.6703671. ,pp81- 84.
- [2] Langley, R.B. "Dilution of Precision", 1999 GPS World, pp 52-59.
- [3] D.Sony,V.Satya Srinivas,P.Naveen, D.Krishna Reddy. IRNSS User Range Accuracy Evaluation for Receiver Autonomous Integrity. 2019 URSI Asia-Pacific Radio Science Conference (AP-RASC). doi:10.23919/ursiaprasc.2019.8738325.
- [4] Wang, Ershen, Yang, Fuxia & Pang, Tao. GNSS receiver autonomous integrity monitoring algorithm based on least squared method. 2017 12th IEEE Conference on Industrial Electronics and Applications (ICIEA). doi:10.1109/iceia.2017.8283169.
- [5] R. Nicole, "Title of paperWei, M., Wang, J., & Li, J. (2012). A new satellite selection algorithm for real-time application. 2012 International Conference on Systems and Informatics (ICSAI2012). doi:10.1109/icsai.2012.6223578 .
- [6] Joardar, Susmita, Siddique, Tanveer Ahmed, Alam, Sakila, & Hossam-E-Haider. Analyses of different types of errors for better precision in GNSS. 2016 3rd International Conference on Electrical Engineering and Information Communication Technology (ICEEICT). doi:10.1109/ceeict.2016.7873127 .
- [7] M. Udaya, D. Sony, D. Krishna Reddy "Design of IRNSS Tracking System using 1.5-bit ADPLL and Correlator" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, August 2020, Volume-9, Issue-10.,pp413-420.
- [8] Du Xiaojing, Liu, Li& Li, Experimental Study on GPS Non-linear Least Squares Positioning Algorithm. 2010 International Conference on Intelligent Computation Technology and Automation. doi:10.1109/icicta.2010.651.
- [9] Zhang Pengfei,Hu Chumsheng,Li Guangyao. A modified satellite selection algorithm based on satellite contribution for GDOP in GNSS.2012, v176,doi:10.1007/978-3-642-31507-7_67,pp415-421.

Design and Analysis of High Speed Parallel Meander Transmission Lines

Dr.B.HariPrasad Naik

Nalla Narasimha Reddy Educational Society's
Group of Institutions
Hyderabad-500075, India
bhattu.hariprasadnaik@gmail.com

Gopal.Aare

Nalla Narasimha Reddy Educational Society's
Group of Institutions
Hyderabad-500075, India
aaregopal@gmail.com

Dr.D.Krishna Reddy

Department. of ECE,
Chaitanya Bhaathi Institute of Technology, BIT,
Hyderabad-500075, India
dkrishnareddy_ece@cbit.ac.in

Abstract: In this paper, analysis of planar transmission lines (PTLs) and parallel meander transmission lines (PMTLs) is performed in frequency domain using S-parameters. Here, characteristics of transmission line such as reflection (S_{11}), transmission (S_{21}) coefficients, near and far end crosstalk (S_{31} and S_{41}) of coupled meander lines with various bend angles are investigated. In the analysis, parallel meander lines with bend angles (θ) 450, 600 and 750 are compared with bend angles 1350, 1200 and 1050 respectively. PMTLs analysis is performed with FR-4 (ϵ_r) as the dielectric substrate and copper as the conducting lines. Further, electro-magnetic co-simulation of PTLs and PMTLs meander lines with bend angles 1350, 1200 and 1050 is performed using ADS tool. The analyzed results showed that PMTLs with bend angles of 1050, 1200 and 1350 have low signal losses and crosstalk noise when compared to its counter bend angles. Hence, for routing in high-speed designs parallel meander lines with bend 1050, 1200 and 1350 can be used as an alternative to reduce the signal loss and decrease the crosstalk noise between the adjacent lines.

Keywords: Parallel meander transmission lines (PMTLs), Electro-magnetic (EM), Crosstalk, Electromagnetic Interference (EMI), PCB, Signal Integrity, Planar Transmission Line (PTL), Advanced Design System (ADS).

I. Introduction

Advancement in the electronic technology has led to the design of high density and high frequency system designs with high band width. These developments will certainly challenge and increase the difficulties to integrated circuit or PCB layout designers. Because the layout designers will have to manage the designs with several design constraints during designing process. At microwave or radio wave frequencies, EMI effects should be considered in high-speed designs. Because signal integrity becomes a challenging task in high-speed designs which are operating at high frequencies.

Traditionally, in high-speed designs planar transmission lines (PTL) were used for routing of cells or logical blocks on the integrated circuit or PCB designs. Planar lines occupy large area for routing because of its directional lengths. But with advancement in technology, now a days both planar and meander transmission lines are used for routing with bend angles. In today's high-speed designs parallel meander transmission lines are often used on the PCB or integrated circuit mainly to reduce effective length and skew in conducting lines [3]. PMTL saves the layout space while routing and provides better layout routing integration to reduce the signal loss [6]. Therefore, it is necessary and important to understand the behaviour of PMTLs with different bend angles. For the analysis and evaluation of parallel meander transmission lines some of the analytical approaches have been discussed in the literature for the elimination of crosstalk noise [5-7]. For elimination of common mode noise, a blended differential transmission line with short circuited coupled line was proposed. For routing in high-speed designs, PMTLs with bend angle (θ) of 900 and 450. The bend angles (θ) used between adjacent meander lines should be able to suppress the crosstalk noise during the signal propagation. This improves the signal to noise ratio in conducting lines.

Here, behavioral analysis of PTLs and PMTLs with different bending angles (θ) is discussed. This also detail the effects of mutual coupling between the parallel lines. With various bending angles; parallel meander lines are analysed by using the Advanced Design System (ADS) for estimating the signal loss and crosstalk noise. The transmission line performance metrics such as reflection, transmission, near-end and far-end because of inductive and capacitive coupling are analyzed in detail. For analysis of parallel meander lines; physical geometry and parameters along with different bend angles as in reference [1] and [2] are considered.

II. Configuration of Transmission Lines

A. Planar Parallel Transmission Lines

Typically, planar transmission lines (PTL) are used for routing various logical blocks in high-speed designs. But these PTLs increases the signal skew and occupies layout space during routing as well. Here, the schematic and layout view of coupled planar transmission lines is shown in Fig. 1. Planar lines are designed using the following parameters as given in reference [1], [2]: length (l)=20mm, spacing (s)=1mm and width (g)=0.95mm.

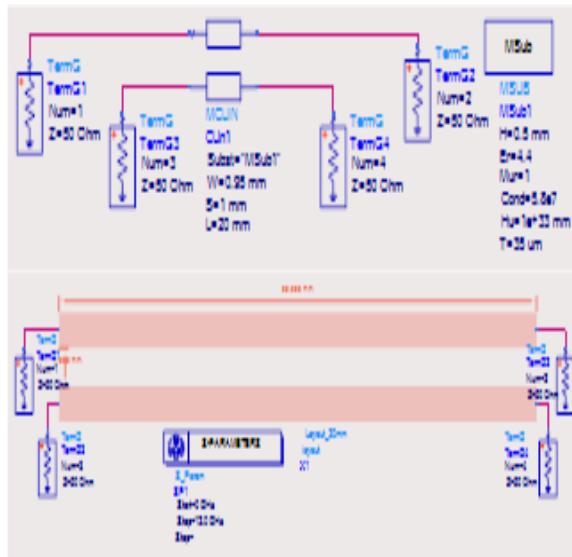


Fig 1: Geometry of PMTLs: $l=20\text{mm}$, $h=0.5\text{mm}$, $s=1\text{mm}$, $g=0.95\text{mm}$.

In the design of planar transmission lines, copper lines with conductivity $5.8e7$ is used. The two copper lines are placed on the FR-4 substrate with thickness $h=0.5\text{mm}$ and relative permittivity $\epsilon_r=4.4$ is shown in Fig. 2.

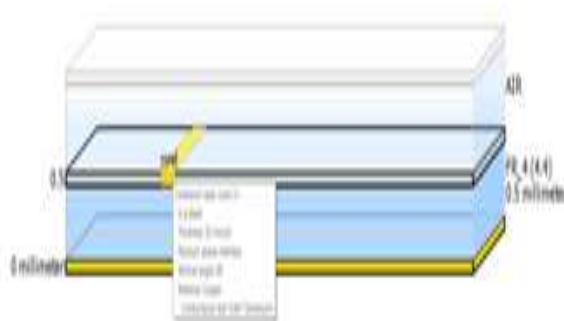


Fig 2: FR-4 Substrate with Copper conductor.

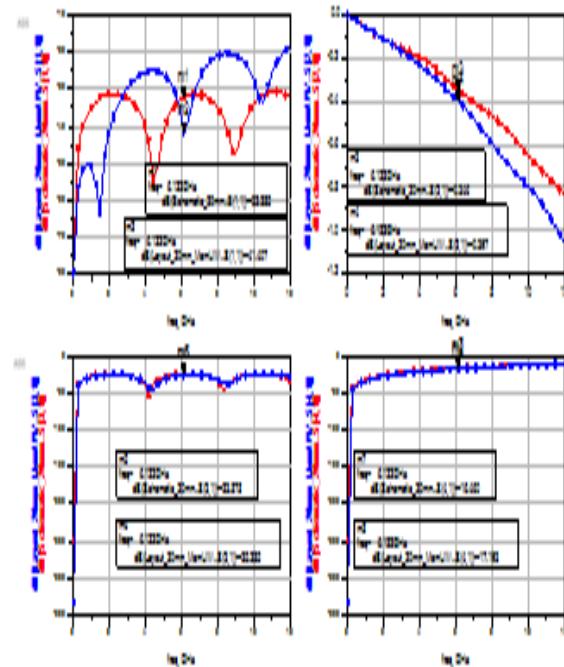


Fig 3: S-parameter response of planar transmission lines.

Frequency domain analysis of both schematic and electromagnetic models of planar transmission lines is performed over a frequency range 0-12GHz. The simulated response using S-parameters is shown in Fig. 3. Comparison of responses shows that schematic and EM model responses are not equal.

B. Layout of Parallel Meander Transmission Lines

Basically, parallel conductors with narrow bend angles are termed as “Meander” lines. In differential transmission lines; meander lines are commonly used to compensate the signal skew. Moreover, meander lines can cause impedance discontinuity resulting in signal reflections. In high-speed designs; conventional PTLs and PMTLs with bend angles are used for routing. The PMTLs layout configuration referred in [1], [2]; with length and bend angle $00=750$ $00=1050$ which is implemented in ADS is illustrated in Fig. 4. The configuration ports (P1-P4) are configured as TML at high frequencies. The meander transmission lines with bend angles are used in high-speed PCB or integrated circuit design. Here, PMTL of length $l=20\text{mm}$, width (g)= 0.95mm , spacing $s=1\text{mm}$ is considered.

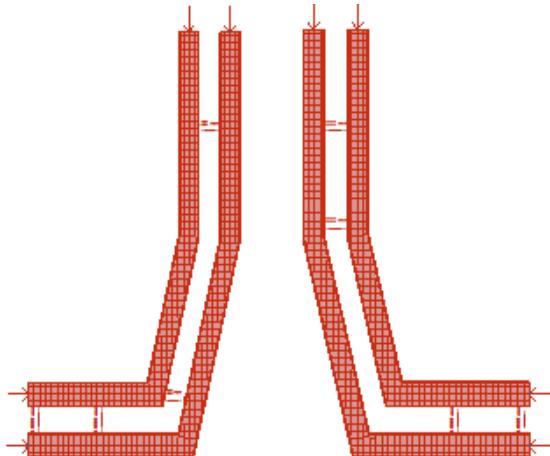


Fig 4: Geometry of PMTLs with bend angles 750 and 1050.

C. Equivalent Schematic of PMTL

From the geometry of PMTLs depicted in Fig 4, the extracted equivalent schematic with bend angle of $\theta=1050$ is shown in Fig 5. The circuit components values are extracted from the results of S-parameters [8].

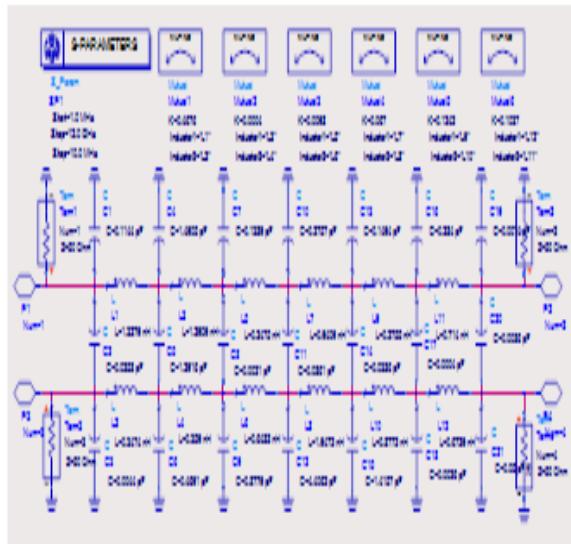


Fig 5: Extracted Equivalent of 1050 PMTL.

The extracted equivalent circuit of the PMTLs with coupling capacitances ($C_2, C_5, C_8, C_{11}, C_{14}, C_{17}$ and C_{20}) and mutual coupling inductances ($L_{m1}-L_{m6}$). The self inductance (L), self capacitance (C) between two bend transmission lines are

$$\begin{aligned} C_1 &= 0.1144, \quad C_2 = 0.0258, \quad C_3 = 0.0044, \quad C_4 = 1.4905, \\ C_5 &= 1.2916, \quad C_6 = 0.4691, \quad C_7 = 0.1389, \quad C_8 = 0.0021, \\ C_9 &= 0.8779, \quad C_{10} = 0.2757, \quad C_{11} = 0.0861, \quad C_{12} = 4.4062, \\ C_{13} &= 0.1494, \quad C_{14} = 0.0386, \quad C_{15} = 1.4157, \quad C_{16} = 0.284, \\ C_{17} &= 0.0004, \quad C_{18} = 0.0026, \quad C_{19} = 0.0074, \quad C_{20} = 0.0086 \\ (\text{all in pico-farads}) & \quad L_1 = 1.3279, \quad L_2 = 0.3474, \\ L_3 &= 1.2909, \quad L_4 = 0.359, \quad L_5 = 0.2475, \quad L_6 = 0.6488, \end{aligned}$$

$L_7 = 0.9409, \quad L_8 = 1.9472, \quad L_9 = 0.2755, \quad L_{10} = 0.8772,$
 $L_{11} = 0.714, \quad L_{12} = 0.6729, \quad L_{m1} = 0.4676, \quad L_{m2} = 0.0004,$
 $L_{m3} = 0.0098, \quad L_{m4} = 0.067, \quad L_{m5} = 0.1242,$
 $L_{m6} = 0.1037$ (all in nano-henrys).

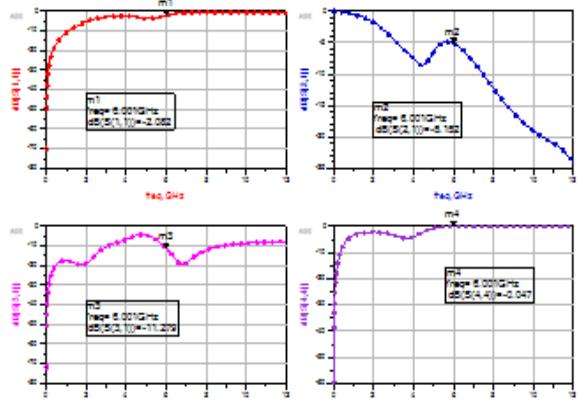


Fig 6: S-parameter response of extracted schematic at 1050.

The performance characteristic of exacted equivalent schematic with bend angle of 1050 is shown in Fig. 6. Analysis is performed in frequency domain with a frequency range 0-12GHz. Response shows that as the operating frequency increases reflection (S_{11}), transmission (S_{21}) and crosstalk noise (S_{31} and S_{41}) also increase linearly.

III. Design of PMTLs with Bend Angles

A. Synthesized PMTLs

In this section, geometry of PMTLs synthesized with various bend angles $\theta = 450, 600, 750$ and $1050, 1200, 1350$ using the ADS tool is illustrated in Fig. 7. The PMTLs synthesized are symmetric to each other. PMTLs designed with different bending angles are investigated to the know amount of coupling and signal loss. Analysis of PMTLs is performed to reduce the signal loss and estimate the crosstalk noise between two meander lines.

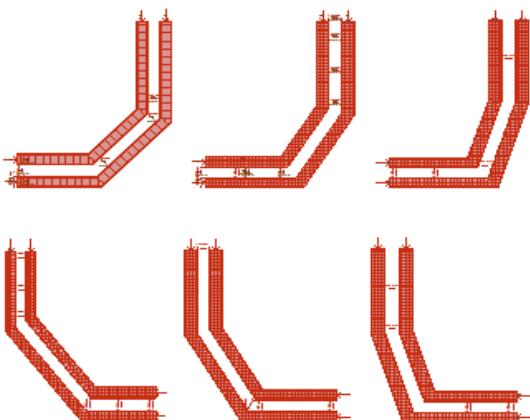


Fig 7: Synthesized PMTLs with bend (450, 600, 750, 1050, 1200, 1350).

Parallel meander transmission lines are designed on a dielectric substrate with relative permittivity $\epsilon_r=4.4$. The thickness of the substrate is $h= 0.5\text{mm}$ and copper with thickness $t = 35$ micron as the conducting material.

B. Electromagnetic Analysis of PMTLs

The synthesized electro-magnetic models of parallel meander lines at bend angles of 45° , 60° , and 75° is illustrated in Fig. 8. Electromagnetic analysis of PMTLs is performed by exiting Port 1 with a signal frequency of (0-12GHz) in steps of 200 MHz. Upon excitation, the signal propagates from Port 1 to Port 2 and induces partial signal to adjacent line.

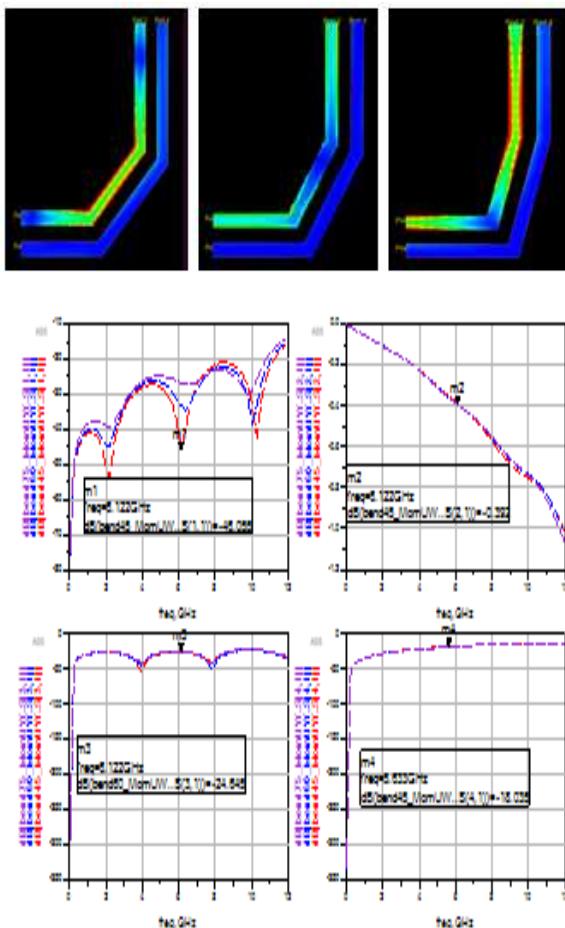


Fig 8: EM Analysis of PMTLs with bend angles (45° , 60° , 75°).

The electromagnetic simulation responses of parallel meander lines using momentum microwave simulator with bend angles of 45° , 60° , and 75° is shown in Fig. 8. Results show that PMTLs with bend angle of 45° have low signal loss and also less crosstalk noise when compared with PMTLs with bend angles of 60° , and 75° .

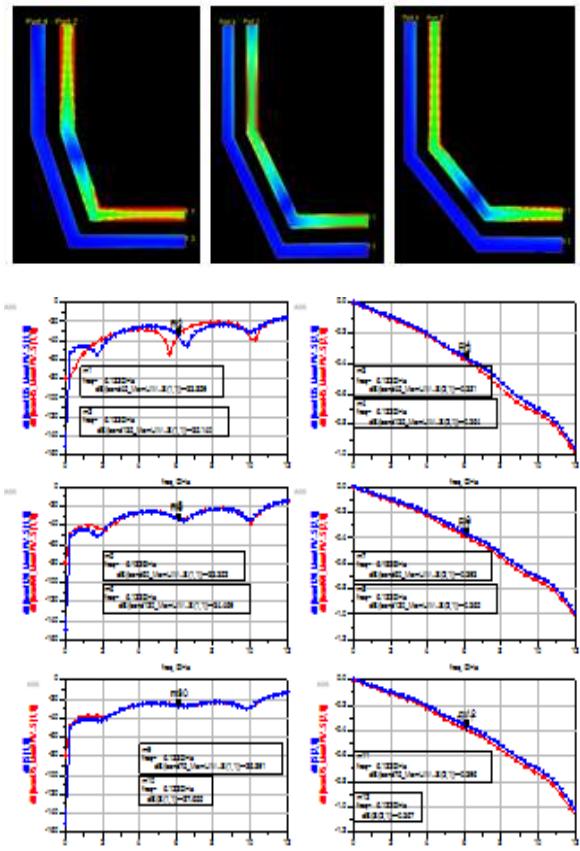


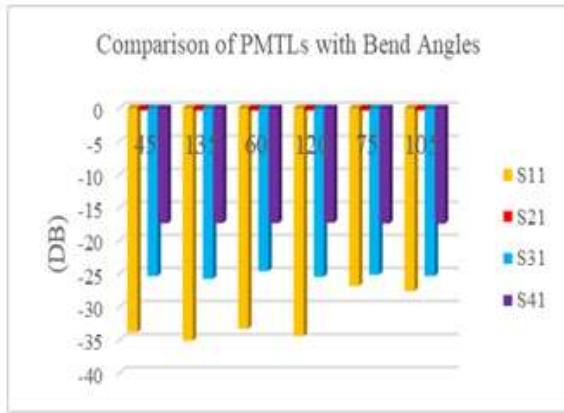
Fig 9: EM Analysis of PMTLs with bend angles (105° , 120° , 135°).

Electro-magnetic analysis and simulation responses of PMTLs with bend angles 105° , 120° , and 135° using momentum microwave simulator is shown in Fig 9. Comparative analysis results of PMTLs with different bend angles is listed in Table 1. It shows that PMTLs with bend angles 135° , 120° , 105° have less signal loss and crosstalk noise than its counterpart 45° , 60° , 75° respectively. Moreover, near end and far-end crosstalk between meander lines are also less in PMTLs with bend angle of 135° than its counter part of 45° .

Table 1: Comparison of Pmtls with Bend Angles.

PMTLs With Bend Angles 45° , 60° , 75° [1]				
	S_{11}	S_{21}	S_{31}	S_{41}
45°	-33.859	-0.381	-25.401	-17.450
60°	-33.352	-0.393	-24.645	-17.422
75°	-26.891	-0.396	-25.173	-17.470
Proposed Bend Angles 105° , 120° , 135°				
	S_{11}	S_{21}	S_{31}	S_{41}
135°	-35.140	-0.364	-25.823	-17.380
120°	-34.469	-0.365	-25.516	-17.332
105°	-27.655	-0.367	-25.395	-17.496

Here, performance metrics of parallel meander transmission lines in frequency domain such as S11, S21, S31, and S41 is measured in dB with various bend angles measured is shown in Fig 10.



IV. Conclusion

In this paper, a comparative analysis of planar and meander transmission lines is discussed in detail. Here, performance analysis of parallel meander transmission lines (PMTLs) with different bend angles is presented. Analysis is performed in frequency domain using S-parameters. Evaluated results showed that PMTLs with bend angles 1350, 1200, 1050 has less signal loss and minimal crosstalk when compared to PMTLs with 450, 600, 750 angles. Therefore, in high-speed design routing PMTLs with angles 1350, 1200, 1050 could be used as alternative. This method can avoid signal loss and coupling effects.

References

- [1] Xiaomin Liu, Yingsong Li , Luyu Zhao, Investigation and Analysis on Crosstalk of the Parallel Meander Transmission Lines, International Applied Computational Electromagnetics Society Symposium (ACES), IEEE, 2018.
- [2] Xiaomin Liu, Yingsong Li1, Yuting Zhao, Luyu Zhao, Crosstalk Reduction Design and Analysis of the Planar Meander Transmission Lines, 2018 International Symposium on Antennas and Propagation (ISAP), IEEE, 2018.
- [3] T. Jiang, Y. Wang, and Y. Li, Design and analysis of a triple stop-band filter using ratioed periodical defected microstrip structure, Frequenz, vol.71, no.7-8, pp:341-347, 2017.
- [4] Y. Li, W. Li, W. Yu, A switchable UWB slot antenna using SIS-HSIR and SIS-SIR for multi-mode wireless communications applications, Applied Computational Electromagnetics Society Journal, vol.27, no.4, pp.340-351, 2012.
- [5] M. A. Khorrami, Noise reduction of bended differential transmissionlines using compensation capacitance, IEEE International Symposiumon Electromagnetic Compatibility, 2013:150-155.
- [6] C. H. Chang, R. Y. Fang, C. L. Wang, Bended differential transmission line using short-circuited coupled line for common-mode noise suppression, Conference on Electrical PERFORMANCE of Electronic Packaging and Systems. IEEE, 2011:291-294.
- [7] L. S. Wu, J. F. Mao, W. Y. Yin, Slow-wave structure to suppress differential-to-common mode conversion for bend discontinuity of differential signaling, Electrical Design of Advanced Packaging and Systems Symposium. IEEE, 2012:219-222.
- [8] R. Mongia, I. Bahl and P. Bhartia, RF and Microwave Coupled-Line Circuits,Boston, MA: Artech House, 1999, pp. 123–180.

Session- A5:
Health Monitoring and
Forecasting Pandemic

Preliminary Result of COVID-19 Detection through Chest X-Ray using Artificial Intelligence

Nikhila Raj Nitta

Department of ECE

Chaitanya Bharathi Institute of Technology,

Hyderabad-500075, India

nikhilrajnitta@gmail.com

Abhishek Adire

Department of ECE

Chaitanya Bharathi Institute of Technology,

Hyderabad-500075, India

abhishekadire295@gmail.com

Vyshnavi Cheedepudi

Department of ECE

Chaitanya Bharathi Institute of Technology,

Hyderabad-500075, India

vyshnavi.cheedepudi@gmail.com

T Sridher

Department of ECE

Chaitanya Bharathi Institute of Technology,

Hyderabad-500075, India

tsridhar_ece@cbit.ac.in

Abstract: The outbreak of the novel coronavirus disease, COVID-19, turned into a global pandemic. The standard test for diagnosis is the reverse transcription Polymerase chain reaction (RT-PCR) but it is a time consuming process. Chest X-Ray(CXR) imaging is a promising method which can be employed in the detection of COVID-19. This method is comparatively faster, low cost and available easily. A Residual Network (ResNet)-18 model is being used and trained on a COVID-19 radiography dataset. The designed Artificial Intelligence(AI) enabled framework can predict CXR scans and produce a result with a reasonably high accuracy.

Keywords: Artificial Intelligence, ResNet-18, COVID-19, coronavirus, chest x-ray.

I. Introduction

In December 2019, a novel coronavirus disease was identified in the capital city of Hubei province i.e., Wuhan, China. This infectious disease is named COVID-19. The symptoms can be characterized as fever, cough, difficulty in breathing, headache [1].

The disease began to spread widely in China and has been identified in other parts of the world by the end of the year. Laboratory tests were conducted on the confirmed cases and found a new type of coronavirus, novel coronavirus (nCov) and also other respiratory pathogens like adenovirus, influenza, avian influenza, Middle East Respiratory Syndrome (MERS), Severe Acute Respiratory Syndrome (SARS) were the cause of this syndrome [2].

The World Health Organization (WHO) received a detailed information from the National Health Commission on 11 and 12 January 2020. The reason for the outbreak is associated with the exposures in Huanan seafood market in Jianghan district, Wuhan[3], a major domestic and international transport hub. According to the

preliminary epidemiological investigation, most of the COVID-19 confirmed patients worked at or were frequent visitors to this seafood market. So, that it indicates animal to human spread initially. The person-to-person spread was known when people who did not have any direct contact with a live animal markets were diagnosed with this disease.

The WHO declared it as a pandemic on March 11,2020 [4] because most people are not immune to its fast person-to-person spread. As of March 11, number of confirmed cases were 115,000 with more than 4000 deaths. As this viral disease continues to spread around the globe, strict measures have been taken by every country to slowdown the spread of corona virus. It began with travel restriction to other countries, quarantine of patients and then lockdown and city shutdown.

This pandemic has been a health crisis from the beginning but because of the lockdown , it became a financial crisis too. All the sectors of economy have been affected as manufacturing and buying has reduced drastically. Daily wage workers and small businesses had the most impact in every country.

The standard clinical confirmation test for COVID-19 is Reverse Transcription Polymerase Chain Reaction(RT-PCR) [5], which is manual, time consuming and complex. In developing and underdeveloped countries, there is a limited availability for testing kits because the financial cost for these laboratory kits is a significant issue and to afford the testing price by most people in those countries is not easy while fighting the disease. Rapid increase of infected patients requests for a screening system where the physicians can quickly identify the patients who need immediate clinical help. A published multinational consensus statement from the Fleischner society recommends to use chest radiography to manage the disease [6],[7].

Chest X-Ray(CXR) is a non-invasive clinical supplement in identification of pulmonary abnormalities. Chest X-Ray imaging is comparatively less cost and easily available for testing. Recent findings found that COVID-19 infected patients have distinct visual characteristics, like multi-focal,bilateral ground glass opacities in non-ICU patients and dense pulmonary consolidations in ICU patients, in the CXR images [8]. These subtle characteristics interpretation is quite challenging and can be done by expert radiologists. But the exponential increase in the confirmed patients makes it difficult for the limited expert radiologists to diagnose in time which leads to increasing mortality rate.

Artificial Intelligence (AI) tools have been helpful in the applications using image based data by producing stable and highly accurate results. Machine learning(ML) techniques have been embedded to develop an automatic diagnosis system. Deep learning(DL) models have been implemented to automatically analyze different radiological disease characteristics [9]. The promising performance of these models can be used to overcome the problem of limited experts and thus an automatic alternate screening system can be designed to fight the disease.

II. Data Acquisition

This section gives us the detailed information about the data used for the proposed approach. We have collected the data from the Kaggle Website [10].The collected data is CXR images. The images are in portable graphics format (.png) and the resolution is (1024 x 1024) pixels. These images are classified into three different sets of data they are:

1. COVID affected patients
2. Pneumonia affected patients
3. Healthy person

We have taken 1341 normal samples, 1345 viral samples and 1200 COVID positive samples of data to train the model. Therefore we have 3886 training samples and 20 testing samples. Image augmentation technique is applied for the training and testing set to build a general model. Possible variations in images, because of diverse imaging conditions, have been incorporated into it.

III. Proposed Frame Work

In this project, normal, pneumonia and COVID-19 infected chest X-Ray images were considered for identification of COVID-19 using Residual Network (ResNet)-18 architecture of most widely used image recognition conventional neural network (CNN).

The classification is performed between COVID, normal, pneumonia images to provide highly effective detection of COVID in chest X-Ray and differentiate COVID from both normal and pneumonia infected images [11].

Resnet-18 is a CNN (conventional neural network) with 18 layers deep. The pre-trained network can classify images into 1000 object categories [12]. The network has a rich feature representations for wide range of images.

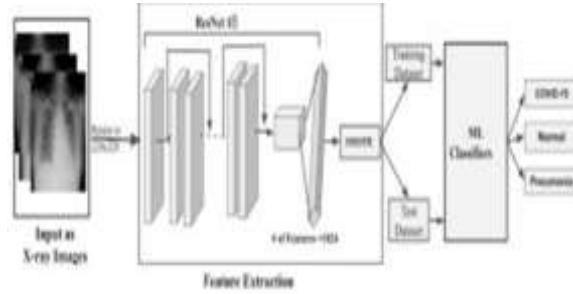


Fig 1: Flowchart for the proposed framework

The core-idea of project is ‘identity short-cut connection’, that skips one or more layers in the network as shown in Fig. 1. This kind of model is used when there is a wide range of images and when the network is too deep.

IV. Results

The data is divided into 648 training batches and 10 test batches. Each batch consists of 6 samples. Before training the model,we predict the images and after training is completed, we will know if our predictions are correct or not. While testing the model, our evaluating starts from comparing the samples in testing batch with different batches in training data set.

In the Fig. 2, the x-axis is the prediction and y-axis is the label. If our predictions are exact with the labels, labels will be displayed in green colour and if they are not, they will be displayed in red colour. At each step, we will get accuracy, which tells how many predictions are actually correct(i.e., same as that of the labels). The testing process iterates till it reaches the accuracy of 96% which indicates all our predictions are same as that of the labels. At the final result, we are calling ‘show_predictions’ function which will display the images which are correctly predicted.

The evaluation table tells about the validation loss and accuracy levels. Initially, accuracy of only 45% is indicated which tells us that not all predictions are correct. As we continue our iterations, at step 20, the accuracy reached 83%.

Since the required accuracy level is not reached, we continue the iterations. Finally at step 40, we reached an accuracy of 95% which indicates that most of our predictions are correct.

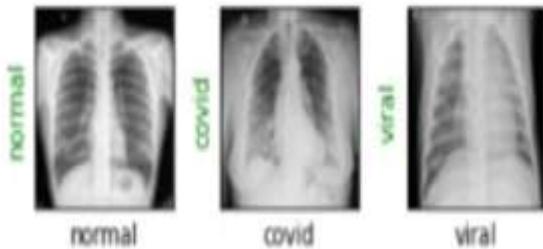


Fig 2: Final predictions with accurate result

Table 1: Evaluation Table

Steps	Validation Loss	Accuracy Level(%)
Step 0	1.1041	45
Step 20	0.6827	83.3
Step 40	0.3687	95

V. Conclusion

A comparatively low cost, faster and easily available system has been proposed for the detection of COVID-19. The method proposed here i.e., Chest X-Ray(CXR) is few of the most promising methods that can be deployed for efficient detection of the disease. Also the AI enabled framework designed for this system can give highly accurate results.

The accuracy of the proposed method can be improved by incorporating different data such as breathing etc. Also, in the coming future, a large dataset should be used to validate our proposed system so as to increase the accuracy more and make the system more generalized. This dataset may include data such as age, gender, medical history etc. As per recent surveys a part of COVID-19 patients has shown skin abnormalities as part of the symptoms [13]. Hence, including skin images would help improve the diagnosis in a more impactful way.

References

- [1] Halgurd S. Maghded, (et al., 2020),“A novel AI-enabled framework to diagnose coronavirus COVID-19 using smartphone embedded sensors”, Design Study, IEEE, 2020.
- [2] Wang D, Hu B, Hu C, et al., “Clinical characteristics of 138 hospitalized patients with 2019 novel coronavirus-infected pneumonia in Wuhan, China.” JAMA. 2020;323(11):1061–1069. doi:10.1001/jama.2020.1585
- [3] “Novel coronavirus – china. world health organization. Available: <https://www.who.int/csr/> don/12-january-2020-novel-coronavirus-china/en/,” Jan. 2020.
- [4] “WHO director-general's opening remarks at the media briefing on COVID-19”, Mar. 11, 2020.
- [5] Yang, H., Lan, Y., Yao, X. et al. ”The chest CT features of coronavirus disease 2019 (COVID-19) in China: a meta-analysis of 19 retrospective studies.” Virol J 17, 159 (2020). <https://doi.org/10.1186/s12985-020-01432-9>
- [6] Boran Sekeroglu, Ilker Ozsahin, “Detection of COVID- 19 from chest x-ray images using convolutional neural networks”, Research Article, First Published Sept. 18, 2020.
- [7] Geoffrey D.Rubin, (et al., 2020),“The role of chest imaging in patient management during the COVID-19 pandemic”, April, 2020.
- [8] Tej Bahadur Chandra, Kesari Verma, Bikesh Kumar Singh, Deepak Jain, Satyabhuwan Singh Netam, “Coronavirus disease (COVID-19) detection in chest x-ray images using majority voting based classifier ensemble”, Expert Syst Appl. 2021 Mar 1; 165: 113909. Published online 2020 Aug 26
- [9] M. I. Razzak, S. Naz, and A. Zaib, “Deep learning for medical image processing: Overview, challenges and the future”, In Classification in BioApps. Springer, 2018, pp. 323–350.
- [10] “COVID-19 radiography database”, Available: <https://www.kaggle.com/tawsifurrahman/covid19-radiography-database>.
- [11] “Detecting COVID-19 with chest x-ray using PyTorch”, coursera tutorial.
- [12] Mathworks helpcentre, Available: <https://www.mathworks.com/help/deeplearning/ref/resnet18.html>.
- [13] Ali Imran, (et al., 2020),“AI4COVID-19: AI enabled preliminary diagnosis for COVID-19 from cough samples via an app”, June, 2020.

Applying Relu and Tanh Functions for the Detection of Lung Cancer using Deep Learning

Madhavi Aluka

Department of Computer Science Engineering,
Annamalai University, Chidambaram,
Tamilnadu-608002, India.
1alukamadhavi2000@gmail.com

Sumathi Ganesan

Department of Computer Science Engineering,
Annamalai University, Chidambaram,
Tamilnadu-608002, India
2summi.ganesan@gmail.com

Vijaya Pal Reddy

Matrusri Engineering College,
Hyderabad, Telangana-500059, India
3drpvijayapalreddy@gmail.com

Abstract: The diagnosis of medical images for detecting lung cancer involves screening, diagnosis, planning, and a careful treatment. Most of the radiologists find it difficult to analyse the data that comes in the form of accumulated material and manual methods of assessing the data for detecting the lung cancer. In this paper, A Model has proposed to detect the lung cancer using the deep learning techniques. A convolution neural network (CNN) based model was implemented by applying Relu and Tanh functions on a dataset with 900 lung images to study the overall performance of cancer detection. Initially, a comparison of machine learning (ML) algorithms such as linear regression, random forest, and support vector machine (SVM) was carried out to test the accuracy, precision, and recall. However, the results obtained using ML techniques was not reaching the expectation and therefore deep learning methods were implemented using Relu and Tanh functions. The results obtained from the proposed model found to be more reliable and enhanced accuracy was obtained when compared with the existing techniques.

Keywords: Deep Learning, Lung Cancer, Annotations, CNN

I. Introduction

The lung cancer is malignant tumour that causes uncontrolled growth of cells in the tissues of a lung. The tissue growth is a cause of concern in much cancer patients and sometimes this may spread in a massive way beyond the lung size. Analysis of such lung images in them declares research is possible since the introduction of computers. In this work, the Kaggle dataset with a sample of 900 lung images have been collected in jpg or .png formats, and they are not in .dcm format in order to fit in to the proposed model for the study. To construct a model ,the image data has been classified into four(4) categories: adenocarcinoma, largecellcarcinoma, squamouscellcarcinoma, andnormaldataset.

Adenocarcinoma: It grow in the gland that secrete mucus and help us breathe in the outer region of the lung and is most common form of lung cancer, Accounting for 40% of all non-small lung cancer cases and 30% over all cases.Coughing, hoarseness, weight loss, and fatigue are some of the symptoms.

Large cell carcinoma: Lung cancer spreads rapidly and can affect any part of the lungs. This form of lung cancer accounts for 10% to 15% of all Non-small cell lung cancer (NSCLC) cases.

Squamous cell carcinoma: Lung cancer of this type is located in the middle of the lung, where the larger bronchi connect the trachea to the lung, or in one of the major airway branches. Accounts for about 30% of all non-small cell lung cancers and is usually associated with smoking.

Normal: Normal CT-Scan Lung images

II. Machine Learning Algorithms Comparisons

To carry out with the present work, the data has been processed for the following three steps: A. Pre-processing, B. Model Selection, and C. Performance.

Pre-Processing

It is a preliminary processing of data in order to transform the raw data before it feeds to the machine learning. With the support of open-cv, all of the CT images in.png format were flattened to fit in the model. Additionally, the dataset has been divided into two set of 70% and 30% for training and testing respectively.

Model Selection

Model selection is the method of choosing final machine learning model for a training dataset from a collection of machines learning models with

the help of different machine learning algorithms, now tries to fit the data.

- **Logistic Regression:** The Supervised Learning technique includes the popular Machine Learning algorithm of logistic regression. It is used for predicting the categorical dependent variable using a given set of independent variables. It gives the probabilistic values which lie between 0 and 1. The classification problems are solved using logistic regression.
- **Random Forest-Supervised Learning Technique:** In machine learning, it can be used for both classification and regression problems. It is based on ensemble learning, which is a method of combining multiple classifiers to solve a complex problem and improve the model's efficiency. It is a classifier that contains a number of decision trees on various subsets of the given dataset and takes the average to improve the predictive accuracy of that dataset.
- **Support Vector Machine (SVM):** The SVM algorithm's aim is to find the best line or decision boundary for categorising n-dimensional space into classes so that new data points can be conveniently placed in the correct category in the future. This best decision boundary is called a hyperplane. The extreme points/vectors that help construct the hyperplane are chosen by SVM.

Performance

In this scenario, three well-known machine learning classification algorithms(linear regression, random forest, and SVM) are used to decide whether the given CT-Lung images contain cancer cells or not. These algorithms are compared for accuracy, precision, and recall to determine the best out of the three for a real-time environment.

III. Proposed Deep Learning Model

Deep Learning is a class of machine learning (ML) that uses layers to extract features from the input. It uses a model working for human lung which process data and create pattern for making a decision. In this work, the dataset is collected from Kaggle (website) to create a model which will classify the lung images into four (4) classes. Further, it splits the dataset into training set (80%) and test set (20%). The following steps explain the flow process of the data for the proposed model as shown in Fig. 1.

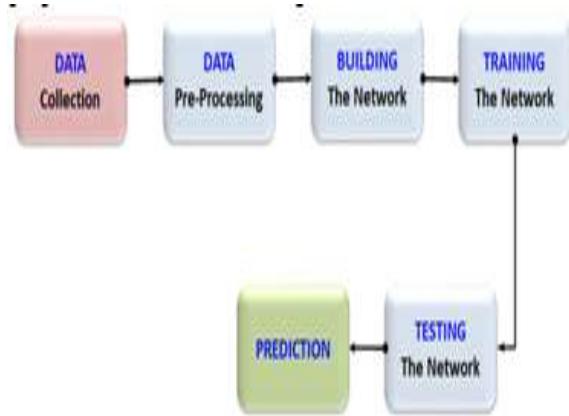


Fig 1: A Simple Block-Diagram of a CNN Model

- **Data pre-processing:** The CNN is a multilayer network with hidden layers. In this work, these layers are used to extract features from CT lung images as an input to the deep learning algorithm, which is a data cleaning step for pre-processing to build the model and transforms to train a CNN using Keras that leads to classification. Outlier detection and the elimination of noisy data from the images are examples of the data pre-processing [1]. In the similar context, Chon et al. uses the methods from computer vision and deep learning to build a 2D and 3D CNN which helps in detecting the lung cancer [2].
- **Building the Network:** CNN allows you to build a model layer-by-layer. In Keras, the best way to construct a model is sequential. To add layers to our model, we use the 'add()' feature. Conv2D layers make up our first two layers. These are convolution layers that will deal with our 2-dimensional matrices as input images.
- **Training the Network:** To train a network model that uses the original images as input layer parameters. A training dataset is used to update the model weights and create a mapping of inputs to outputs to fit in a neural network. As a result, the training dataset yields good result. This is done by back propagation network, which is iterative, recursive and efficient method for training the functions [3].
- **Testing the Network:** Functioning of the designed neural network is carried out by applying the new lung images at the input of the model. This neural network model is divided into three sections: train, validate, and evaluate.
- **Prediction:** While predicting the probability of a specific outcome, the performance of an algorithm after it has been trained on a historical dataset and applied to new data.

IV. Design of Convolutional Neural Networks

The layers in CNN consists of input layer, Convo layer (Convo +ReLU), Max Pooling layer, fully connected (FC) layer, Soft-max layer, and output layer. The design of CNN consists of two main parts as explained below:

- A *convolution tool* extracts the feature and defines the different features of an image for analysis.
- A *fully connected layer* that uses the performance of the convolution process to predict the image's class using the features extracted in previous stages.

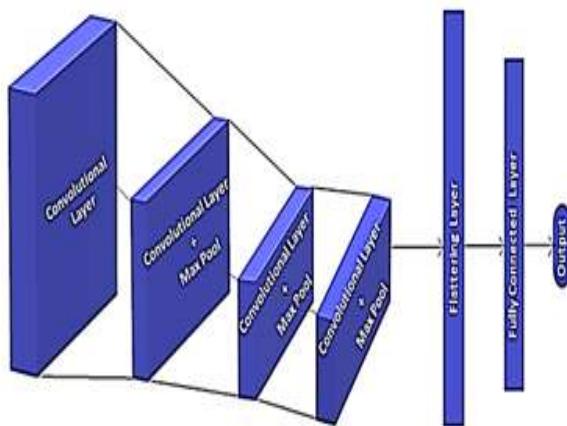


Fig 2: Design of Convolutional Neural Network

A. Image Normalization

Image normalization is a process in image processing, that changes the range of pixel intensity values. The RGB values for these images are given., These values are taken to be as channels. The value 1 and 3 corresponds to grey scale and RGB. To normalize the images to RGB using scale 3, in the first layer normalize these values in a common range, then use of neural networks for training is successful.

B. Activation Function

Activation function's aim is to introduce non-linearity into a neuron's output which allows back propagation and measures a weighted number and then applies bias to it to determine if a neuron should be triggered or not., because the gradients are given along with the error to update the weights and bias.

- **Tanh Function:** Tanh is the hyperbolic tangent function its range from (-1 to 1), non-linearity and sigmoidal (s - shaped).

The activation works better than sigmoid function is Tanh function is given by
 $\text{Tanh}(x)=2\text{sigmoid}(2x)-1$.

- **Rectified Linear Unit:** ReLUs is simple and fast; they use a threshold as an input and produce dead neurons, which means that the network will produce regions where it won't update, and the output is always 0. Given as $f(x)=\max(0, x)$.

C. Convolutional Neural Networks (CNN)

CNN fed to the input layer, and the neurons perform a linear transformation on it. Using the layers, it extracts features from the input image and learns image features using set of filters over the input. A high filter response implies that the filter is being used as an input, and vice-versa. The filter output obtained in this layer enables it to make a decision about the class of the input image. It does linear transformation from input to output without changing the dimension of the input image but changing the number of channels in the output image. As the weights and biases. Weights are defined for each input. These weights help us to reduce the errors when back propagate the error value and adjust it so that it improves the model.

D. Maxpool Layer

Maximum pooling is a technique for determining the highest value in each patch of a function map. This operation is used to down-sample the images. It takes an image size as input and transforms it to desired size. It changes the number of rows and columns but the depth remains the same. This operation is critical because it will not over fit to our data.

E. Fully Connected Layer

In a neural network, completely connected layers are those where all of the inputs from one layer are connected to every activation unit of the next layer (Maxpool and Relu). which compiles together the data extracted by previous layers to create the final output.

F. Soft-max Layer

In our work used SoftMax layer, The SoftMax function reduces a vector of K real values to a vector of K real values that add up to 1. A SoftMax classifier or an SVM is typically used at the end of a convolutional neural network. The SoftMax classifier takes an array as input and generates output for each of the dataset's categories.

V. Methodology

To study the performance of the proposed model, the work has been considered in three following steps:

Step 1: The dataset was collected and divided into 4 classes which has multiple images. Further, splits the dataset into training set (80%) and test set (20%). This model was designed in Keras with TensorFlow and a mix of convolutional and max pooling layers. Layers are flattened in this model (fully connected layer). The validation accuracy was obtained is 65%.

Step 2: As model is ready, to improve our model's performance on 4 classes, used 2 activation functions (Tanh and Relu) and then compare the results. It's initial step to learn the working of the neural network using keras, to visualize the output of every convolutional and max pooling layer. In tanh activation able achieve 40% accuracy. For the same model, the Relu activation function was able to achieve 94% accuracy.

Step3: Throughout the work, plotted multiple graphs comparing training accuracy vs validation accuracy and training loss vs validation loss for the models. The comparison graphs for the tanh and Relu activation functions were plotted.

Results and discussions

From the experimental results as shown in Table I, SVM proved to deliver better accuracy as compared to the other two algorithms. Hyper-tuned SVM provided better results, but it is having its own limitations. Therefore, in this work, the researchers considered to incorporate the deep learning convolution neural networks (CNN) algorithms in order to improve the proposed deep learning model.

Table 1: Comparison of Machine Learning Algorithms

Algorithm	Accuracy	Precision	Recall
Linear Regression	78%	78%	77%
Random Forest	80%	79%	80%
SVM	83%	83%	82%

There are so many differences between SVM and logistic regression (LR) towards finding the distance between lines and support vectors. SVM helps to identify the best margin between the support vectors and helps to support the classes, to reduce the overall risk of errors in the data. It can also handle the non-linear solutions and linear SVM proves to be the best method to handle the outliers in an effective manner. However, in logistic regression it does not support the above method, but it has got different decision boundaries consisting of different weights

which are near to the optimal points. It can also handle the linear solutions very effectively[5]. On the other hand, SVM is based on geometrical properties and can be implemented with semi-structured and unstructured data (i.e., text and images). Whereas in case of logistical regression, it is based on the statistical approaches and implemented only on the identified independent variables. Due to these factors risk of overfitting is minimum by using SVM and it is quite opposite in the case of logistic regression, where it is vulnerable to overfitting in many ways. Apart from the SVM and logistic regression, random forest method is also one of the popularly used machine learning algorithm. This method needs huge number of datasets and proves to deliver solutions for a problem with robust models. It is a tedious process to train the machine with huge amounts of dataset using this method.

The performance of a model under different activation functions (Tanh and Relu) was evaluated. Successfully loaded the dataset into training and predicting the class of a new test image. In this work, plotting of two activation functions Tanh (orange) and Relu (blue), where on the x-axis number of epochs means number of passes forward and backward through the neural network which is grouped into batches. On the y-axis has Accuracy % or Loss % means it has training Accuracy (Train Data) and validation Accuracy (Test Data).

Table 2: Comparison of Deep Learning by applying on Lung Images for tanh and relu

	Tanh	Relu
Validation Accuracy	30%	90%
Training Accuracy	40%	94%
Loss	0.5	2.0

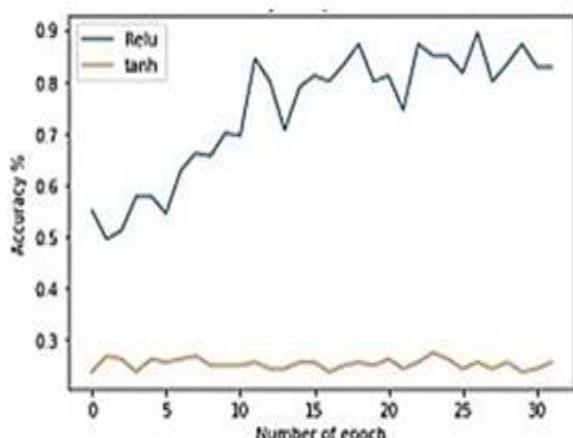


Fig 3: Plotting the validation accuracy between Relu and Tanh activation functions

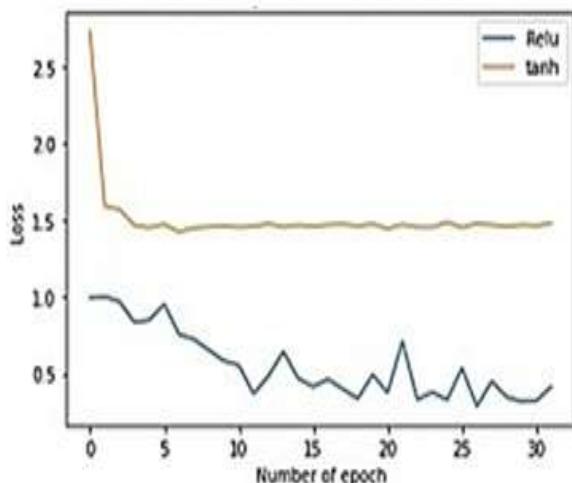


Fig 4: Plotting the loss between ReLu and Tanh activation functions

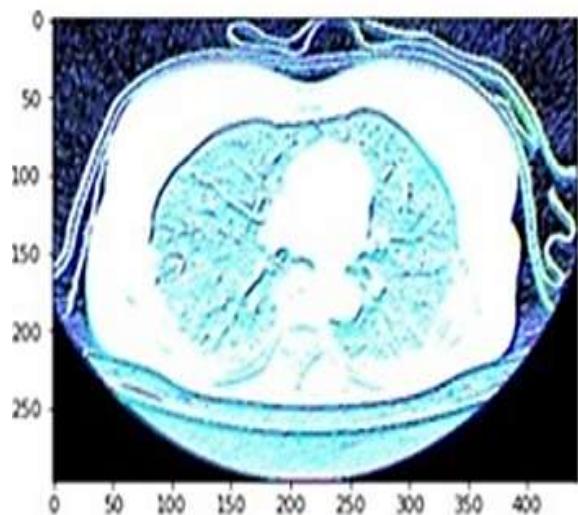


Fig 6: After first convolution layer

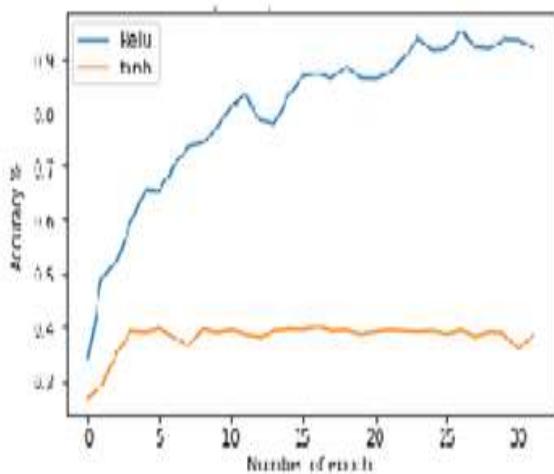


Fig 5: Visualizing the impact of each layer on an input image

Due to the involvement of simple mathematical operations ReLu is less expensive as compared to Tanh in terms of computational process. Sparsity and reduced vanishing gradient are other advantages of ReLu over Tanh. Also, reduced gradient to vanish is major advantage of ReLu, which arises when $a > O_a > 0$ and during regime gradient has a constant value leading to a faster learning process. Sparsity arises when $a < O_a < 0$, which is another major advantage of ReLu.

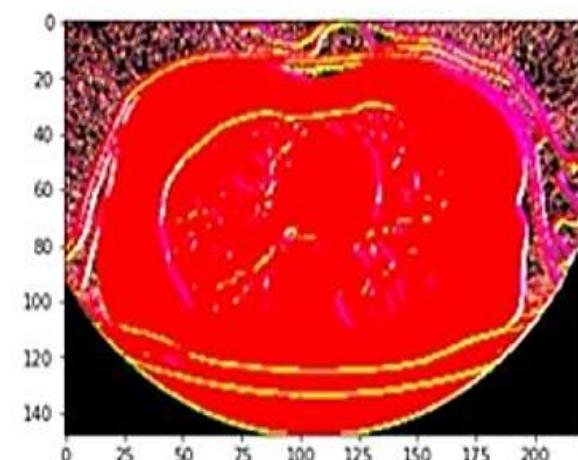


Fig 7: Adding another layer to the model

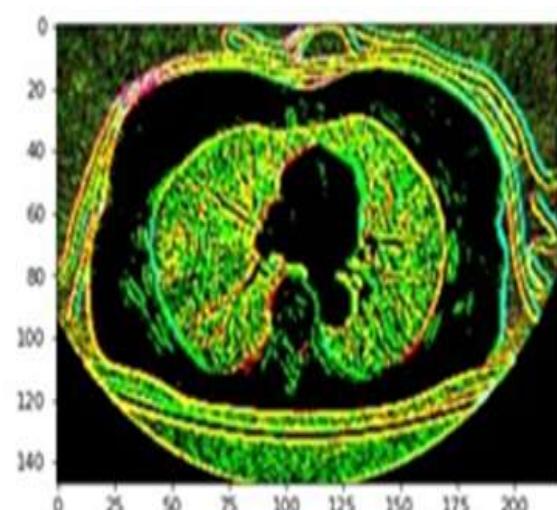


Fig 8: Adding another layer to the model

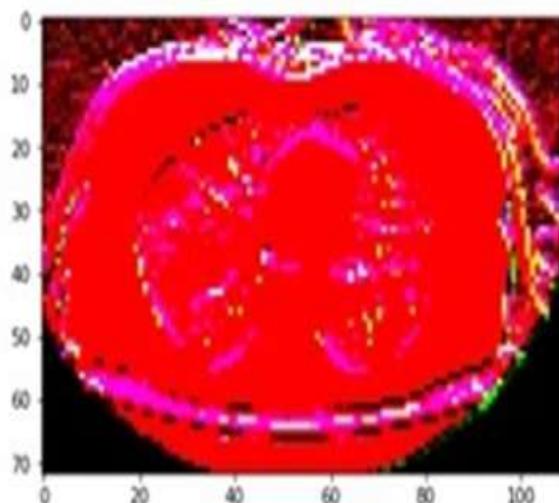


Fig 9: Final max pooling layers

VI. Conclusions

Relu activation function performed better as compared to Tanh. For the proposed model, the training of data has been considered with training set of 80% data and test set of 20% of data has been considered to increasing the number of convolution layers in a fully connected model to enhance the accuracy. ReLu proved to be more advantageous when compared to Tanh in terms of sparsity and limited vanishing gradient under different conditions of $a > 0, a > 0$ and $a < 0, a < 0$. It also exhibits the non-saturation of the gradient, due to which it accelerates the convergence of stochastic gradient descent when compared with the Sigmoid Tanh functions.

VII. Acknowledgment

The authors would like to thank the management of Annamalai University for their support and giving us the opportunity to carry out this scientific research.

References

- [1] M. Shakeel, A. Tolba, Z. Al-Makhadmeh, and M. M. Jaber. "Automatic detection of lung cancer from biomedical data set using discrete AdaBoost optimized ensemble learning generalized neural networks." *Neural Computing and Applications* 32, no. 3 (2020): 777-790.
- [2] Chon, N. Balachandar, and P. Lu, 2017. Deep convolutional neural networks for lung cancer detection. Standford University.
- [3] J. Kuruvilla, and K. Gunavathi. "Lung cancer classification using neural networks for CT images." *Computer methods and programs in biomedicine* 113, no. 1 (2014): 202-209.
- [4] J. Zhang, &Li.J "Testing and verification of neural-network-based safety-critical control software: A systematic literature review." *Information and Software Technology* 123 (2020): 106296.
- [5] A.Krizhevsky I. Sutskever, and G. E. Hinton. "Imagenet classification with deep convolutional neural networks." *Advances in neural information processing systems* 25 (2012): 1097-1105.

Survey on Diabetic Retinopathy Detection

Pravallika Elluri

Information Technology

Chaitanya Bharathi Institute of Technology
Hyderabad-500075, India
pravallikaelluri13@gmail.com

Abstract: Diabetic retinopathy is a diabetes (occurs when your blood glucose is too high) problem where the eyes get effected. The blood vessels are important as they transport glucose and insulin all over the body. Due to High level of glucose, the blood vessels get damaged and organs like heart and eyes get most effected in this condition. The tissues which are sensitive to light that are present at backside of eye get highly effected. This paper explains various stages of diabetic retinopathy detection, to classify the stages of disease the Convolutional Neural Network (CNN) is used. The diagnosis of retinal image with maximum resolution are done automatically. Taking the severity of disease as basis, classified into 5 stages. The unevenness is the major difficulty for classification of images as there exists the retinal proliferation of new blood vessels and segmentation of retina. To get the best result the blood vessels are to be analyzed properly. The process of detection of blood vessel edges or boundaries automatically is called retinal segmentation. The features get restored during region merging which are lost during the segmentation process. In order to classify these, they are sent through the image classifier. For the segmentation of retinal images U-Net is used and is trained on database called DRIVE. Diabetic Retinopathy database is taken to classify the level of Diabetic Retinopathy by training it on Convolutional Neural Network. Our approach of detection is to train Convolutional Neural Network as well as classify the Diabetic Retinopathy image levels. The Diabetic Retinopathy database is taken from Kaggle detect the Diabetic Retinopathy. The database used for training the image are taken under different conditions. These are labelled and image resolution is high. The database is approximately of 35,126 labelled images.

Keywords: Diabetic Retinopathy, U-Net Segmentation, Convolutional Neural Network.

I. Introduction

Diabetes is a metabolic disease is caused due to release of excess amount of glucose in the blood. The key factor which leads to Diabetic Retinopathy is hyperglycemia. The people with diabetes have a greater number of chances to get

Sirisha Alamanda

Information Technology

Chaitanya Bharathi Institute of Technology
Hyderabad-500075, India
asirisha_it@cbit.ac.in

diabetic retinopathy. With proper medication and frequent monitoring of eyes this can be reduced. Diabetic retinopathy has a major chance to increase if the cholesterol and blood pressure levels are high. Deep Neural Network is used for detection and classification of Diabetic Retinopathy as there is the availability of large dataset. In case of retinal proliferation and detachment of blood vessel fundus image classification becomes difficult due to high variability

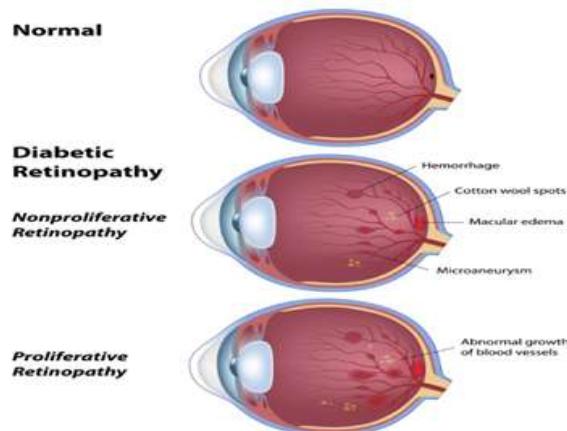


Fig 1: Diabetic Retinopathy Classification

The model called U-Net is used for segmentation of the images which are present in DRIVE database. The classification is done by using the database present in Kaggle. Convolutional Neural network is used for classification of the images. Some amount of data loss occurs during segmentation of the images; the lost data can be brought back by merging the regions.

A. U-Net Architecture

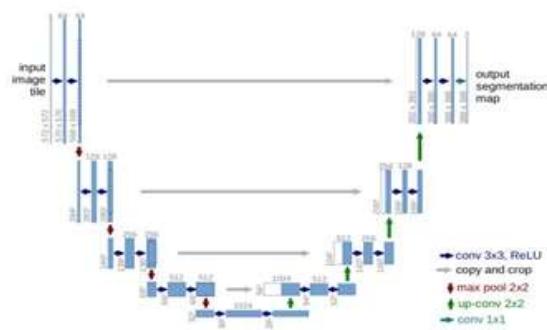


Fig 2: U-net

- It is of “U” shape.
- Symmetric architecture with 2 major parts.
- left part -contracting path constituted by the general convolutional process;
- Right part-expansive path, constituted by transposed 2d convolutional layers.

B. Convolutional Neural Network

- Convolutional Neural Network is used in this, which has a max pooling layer (MPCNNs) as sub sampling layers which consist of sequence of convolutional (denoted by c), max-pooling (denoted by MP), and fully connected (denoted by FC), MPCNNs for input samples into output class to extract features.
- 2D filtering is applied for each C layer between input and bank of filters. The input output maps of FC are combined linearly. Then that is applied to nonlinear activation function. The forward propagation which is in front of C layer. Drive database is used for demonstrating the high effectiveness and to achieve average accuracy.

C. Stages of Diabetic Retinopathy

Diabetic Retinopathy is classified into several stages they are mild non proliferative retinopathy, Moderate non proliferative retinopathy, severe non proliferative retinopathy, and Proliferative diabetic retinopathy.

- **Mild non-proliferative retinopathy:** Micro aneurysm occurs at the early stage of disease. Here a fluid is leaked into the retina due to the swelling occurred in blood vessel.
- **Moderate non proliferative retinopathy:** With the time being the transportation of blood to retina get effected and which results in change of retinal appearance.
- **Severe non proliferative retinopathy:** In severe stage blood vessels gets blocked, stopping the supply of blood to retinal area
- **Proliferative diabetic retinopathy:** This is the final stage of severity of Diabetic Retinopathy. Retinal detachments caused due to the leakage of blood and contraction of scar tissues. This leads to the permanent vision loss.

D. Causes of Diabetic Retinopathy

The high amount of sugar presence in the blood leads to blockage of the retinal blood vessels and stops the blood supply. In such a situation the eye attempt to grow new blood vessels results in blood vessels which do not develop precisely and leads to the leakage of the blood vessels. The main risk factor is the control of blood sugar in diabetics is very poor. The risk will increase with increase in the High blood

pressure, High cholesterol, consumption of Tobacco and the duration of the disease.

E. Complications caused due to Diabetic Retinopathy

Diabetic retinopathy involves the uncommon growth of retinal blood vessels which lead to severe vision problems.

- **Vitreous hemorrhage:** Here the blood gets extravasated around the vitreous humor of the eye which is the clear fluid which is in between lens and the retina. It doesn't cause permanent vision loss. This is recognized by the symptoms like blurred vision, photopsia (brief flashes of light in the peripheral vision)

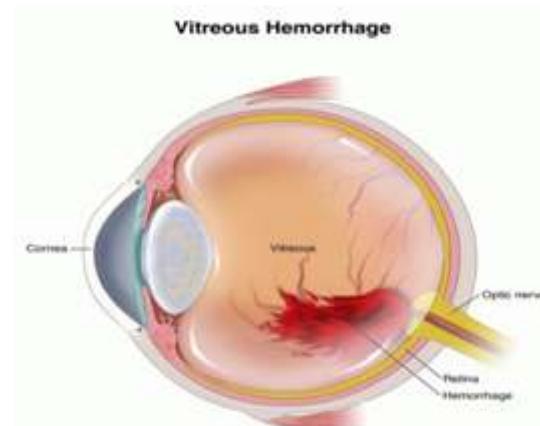


Fig 4: Vitreous hemorrhage

- **Retinal detachment:** Here the retina gets detached from its normal position. This can be identified by observing the changes like sudden appearance of many floaters, flashes of light.

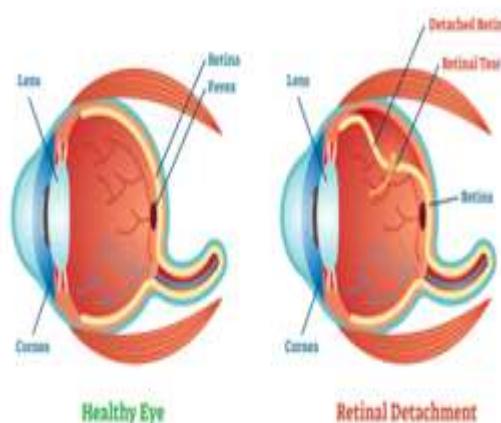


Fig 5: Retinal detachment

- **Glaucoma:** It is a condition where the new blood vessels grow in the front portion of eye and interfere with the normal flow of fluids out of the eye which causes pressure and damage may

occur in the nerve which carries image from eye to brain.

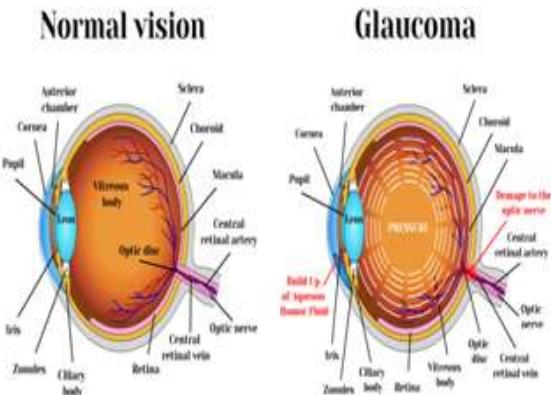


Fig 6: Glaucoma

- **Blindness:** Diabetic retinopathy and glaucoma eventually lead to the loss of vision and cause complete blindness.

F. Prevention of Diabetic Retinopathy

It's not possible to prevent diabetic retinopathy completely but taking some preventive measures may reduce the chances which lead to the condition. Some of them are attending annual eye screening, avoid alcohol and tobacco, treat hypertension, lose weight, regular exercise.,

Table 1: Signs of diabetic retinopathy

Sign	Description
Microaneurysms	It is a small swelling formed in the walls in the blood vessels which may break and allow the blood to leak into the nearby tissues. It is the primary clinical sign of diabetic retinopathy.
Dot and Blot hemorrhages	Blood gets leaked due to the rupture of damaged vessels.
Hard exudates	These are the intra retinal deposits of fluids which may evolve into rings.
Cotton wool spots	This is found mainly on funduscopic exam of the retina which appears fluffy white patch on the retina.
Venous beading	The blood is passed through various capillaries and organs except the lungs, this is mainly found in veins, right chambers of heart and pulmonary arteries.
IRMA's	Intra Retinal Microvascular abnormalities are irregular formations of wider capillary beds.

II. Key Concepts

Some of the concepts that are to be known in order to understand this paper are:

A. Diabetic Retinopathy

It is an eye disease in which the blood vessels of the retina are deformed by swelling fluid leakage and bleeding which causes blindness or loss of vision.

B. Insulin

Insulin is a hormone which plays a key role in regulation of blood glucose levels. It instructs cells to take in glucose from blood.

C. Hyperglycemia

It is a condition in which the excessive amount of glucose circulates in the blood plasma.

D. Fundus images

It is the inner surface of the eye that is present opposite to the lens that include optic disk, retina, fovea and posterior pole.

E. Diabetic Retinopathy Detection

This is detected by the ophthalmologist by observing the symptoms like leakage of blood vessels, swelling of retina known as macular edema, and deposits on the retina.

III. Literature Survey

Retinal Vessel Segmentation Using Deep Neural Networks [1] is an IEEE journal paper published in the year 2015 in the Karlovac University of Application Sciences, The University of Zagreb, J. J. Strossmayera 9, 47000 Karlovac, Croatia by Martina Melinscak, Faculty of Electrical Engineering and Computing, The University of Zagreb, Unska 3, 10000 Zagreb, Croatia by Pavle Prentasic and Sven Loncaric. Here the segmentation of retinal vessel is explained where these retinal vessels are connected and forms a tree like structure. In eye diseases the automatic segmentation of blood vessels in the image has much importance. To segment the blood vessels, GPU implementation of Deep maxpooling Convolutional Neural Network DNN is used as a pixel classifier. CNN are used in this, subsampling layers have a max pooling layer (MPCNNs) which consists of sequence of Convolutional (denoted by c), max-pooling (denoted by MP), and fully connected (denoted by FC) MPCNNs for input samples into output class to extract features. Parameters of feature extraction and classification are jointly optimized during the network training. Image processing layer have non changeable filters which are predefined. For every c layer 2D filtering is applied between input and bank of filters. FC input output maps are linearly combined. Then that is applied on the nonlinear

activation function. The forward propagation which is in front of C layer is of size $n \times n \cdot m \times m$ filter. The size of C layer output is $(n - m + 1) \times (n - m + 1)$. DRIVE dataset is used for demonstrating the high effectiveness and to achieve average accuracy. Blocks of images are taken to do segmentation, by using U-Net segmentation the segmenting of image is obtained with good accuracy.

A Deep Learning Ensemble Approach for Diabetic Retinopathy Detection [2] is an IEEE Journal published in 2019 by Sehrish Qamar, Fiaz Gul Khan, Sajid in Ton Duc Thang University, Ho Chi Minh City, Vietnam, Information Technology. The paper aims to find all the stages of Diabetic retinopathy are classified. A CNN ensemble-based framework is proposed for detection and classification of the stages by using color fundus images. Thus, Ensemble model is able to detect all the stages including the initial stage of diabetic retinopathy. As it is an ophthalmic disease which leads to damage in the retinal blood vessels of retina. The diabetic retinopathy mainly classified into 2 types:

1. The Non-Proliferative Diabetic Retinopathy (NPDR)
2. Proliferative Diabetic Retinopathy (PDR) NPDR is further divided into Mild, Moderate, Severe stages.

Retinal image dataset is taken from Kaggle to train 5 Deep Convolution Neural Network models. By using end-to-end deep ensemble network DR of all stages is detected. The approach ensembles the five deep CNN models Resnet50, Inceptionv3, Xception , Dense - 121, Dense169. These are all pretrained models. Ensemble model is used to combine several Machine Learning techniques to one predictive model. The methods are meta-algorithms that combine several learning techniques into one predictive model, which helps in improving the results of Machine Learning models by combining them. The approach ensembles the five deep CNN models Resnet50, Inceptionv3, Xception , Dense - 121, Dense169. These are all pretrained models. The performance parameters used are accuracy, sensitivity, specificity, precision, F1 measures, AUC and ROC as performance metrics. The performance is better when compared to state-of-the-art method of Kaggle dataset. It is used to detect the different stages of Diabetic Retinopathy but the performance and accuracy is reduced.

Automated Detection of Diabetic Retinopathy Using Deep Learning [3] is published in IRJET in the year 2019 by Carson Lam, Darwin Yi. In this paper the grading system of Diabetic Retinopathy capable of classifying images based on

severity levels. Weight matrix is used to determine best performance which enhances the sensitivities for the mild or early-stage classes multi-class models are to be trained. The max-pooling sample-based discretization process was performed with kernel. L2 regularization is used to reduce model overfitting, cross entropy, and Xavier method of initializing weights. Preprocessing is done that is the images were converted to hierarchical data format. Several steps are involved in preprocessing, using Otsu's method images are cropped, images are normalized by subtracting minimum pixel with range 0 to 1. By using contrast limited adaptive histogram equalization (CLAHE) filtering algorithm contrast adjustment was performed. Augmentation is done to images to reduce overfitting. It gains 95% of sensitivity. Due to classification models, CNN cannot detect subtle disease thus leads to misclassification. The Google Net model achieved the highest sensitivity as Binary model classification attains benchmark performance. The three consecutive convolution layers followed by ReLu layer are used to increase the accuracy, which are followed by a max pooling layer.

Hyperparameter Tuning Deep Learning for Diabetic Retinopathy Fundus Image Classification [4] is an IEEE open access journal published in 2020 by K. Shankar from Department of Computer Applications, Alagappa University, Karaikudi, Yizhuo Zhang, Viwei Liu , Ling Wu , and Chi-Hua Chen from College of Mathematics and Computer Science, Fuzhou University, Fuzhou. For classification of diabetic retinopathy from color fundus images a new automated Hyperparameter Tuning Inception-v4 (HPTI-v4) model is used. To improve the color fundus images CLAHE model is used that is contrast limited adaptive histogram equalization. MESSIDOR (Methods to Evaluate Segmentation and Indexing Techniques in the field of Retinal Ophthalmology) Diabetic retinopathy dataset to guarantee the goodness of the HPTI-v4 approach. This clearly shows the authority of HPTI-v4 model when compared to other methods. The model can be further improved with the application of classification models.

IV. Conclusion

Here we develop a model for detecting diabetic retinopathy using CNN. We build a model using Diabetic Retinopathy database and perform retinal segmentation using U-Net on the fundus images in the database and then the processed images are used for building the models using CNN. The images are trained (approximately 35000) and tested thus obtaining early stages of diabetic retinopathy with their accuracies. Now we compare the accuracy of the models with the previous models.

References

- [1] Martina Nelinscak, Pavle Pentastich, Sven Loncaric, “Retinal vessel segmentation using Deep Neural Network”, IEEE journal published in the year 2015.
- [2] Sehrish Qamar, Fiaz Gul Khan, Sajid, “A deep learning ensemble approach for Diabetic Retinopathy Detection”, IEEE journal published in the year 2019.
- [3] Carson Lam, Darwin Yi, “Automated detection of Diabetic Retinopathy using Deep Learning”, IEEE journal published in the year 2019.
- [4] R. Ghosh, K. Ghosh, and S. Maitra, “Automatic detection and classification of diabetic retinopathy stages using CNN” 2017.
- [5] K. Shankar, Yinzhuo Zhang, Chi-Hua Chen, “Hyperparameter Tuning Deep Learning for Diabetic Retinopathy Fundus Image Classification”, IEEE journal published in the year 2020.

A Simple Model for Forecasting Confirmed COVID-19 Casesin a Given System

A.D. Sarma

Department of Electronics and
Communication Engineering,
ChaitanyaBharathi Institute of Technology
(CBIT), Gandipet,
Hyderabad, Telangana-500075, India)
ad_sarma@yahoo.com

K. Lakshmanna

Department of Electronics and
Communication Engineering,
ChaitanyaBharathi Institute of Technology
(CBIT), Gandipet,
Hyderabad, Telangana-500075, India

T. Sridher

Department of Electronics and
Communication Engineering,
ChaitanyaBharathi Institute of Technology (CBIT),
Gandipet, Hyderabad, Telangana-500075, India)

Abstract: COVID-19 also known as Corona virus pandemic has changed world forever in all important fields including health and lifestyle, education system and employment opportunities. In this letter, we considered three prominent simple forecasting techniques for predicting the number of confirmed COVID-19 cases for the next one week. These are Holt's Linear Exponential Smoothing and Holt-Winters (additive and multiplicative) models and are tested for data of six severely affected countries. The performance of the models is evaluated by using statistical parameters namely MAPE, Standard Deviation and RMSE and found the results are very encouraging and would be helpful for health managers, government agencies and researchers working on coronavirus.

Keywords: COVID-19, Forecasting and Holt-Winters Model

I. Introduction

The entire world has been fighting against the outbreak of the most contagious coronavirus disease – that causes COVID-19, since January 2020. The first coronavirus positive case was found in Wuhan city in China which is the originating point of coronavirus in late 2019. Since then, the coronavirus is spreading worldwide without any boundaries and has become pandemic. It spreads very fast especially in densely populated areas such as malls, theatres, function halls etc, either through direct or indirect contact. Once infected, the symptoms keep showing within 5 to 14 days. Spreading of the virus assumes four different stages. In stage 1, the virus doesn't spread locally but the occurrence of cases is due to people who have had travel history to the affected country. Local transmission occurs in stage 2, when people get in contact with the affected people and the origin is traceable. When the spread reaches 3rd stage, the source of infection is untraceable and

becomes extremely contagious. When the spread reaches 4th and final stage, the spread is practically uncontrollable and confirmed cases occur in clusters all over the country. The prediction of the number of occurrences in advance would be helpful in controlling the spread and also in taking necessary precautions. Worldwide, several Health Research Organizations and educational institutes have been working round the clock to develop a coronavirus vaccine and predicting of the number of coronavirus cases.

Recently, a couple of researchers worked on forecasting of occurrences of COVID-19 cases globally and regionally. One research group reported their work on nowcasting and forecasting of spreading the virus and its association with weather variables in 30 Chinese provinces[1]. Limited work on forecasting of the potential domestic and international spread of the COVID-19 outbreak originating in Wuhan had been done by another group and used the number of airline passengers as one of the inputs [2]. Another research group also reported an informative work on Real-time Epidemic Forecasting: Challenges and Opportunities but general in nature and highlighted the importance of forecasting of epidemics [3]. In contrast to the techniques and their findings in the literature, the present work is very specific and forecast for the next week using the previous two weeks data in a given system. In this paper, we forecasted the occurrences of COVID-19 cases using Holt's linear exponential smoothing and Holt-Winters (additive and multiplicative) models for six countries. These proposed models are more appropriate for spreading stages 2 and 3 as the required coefficients can be obtained from the number of confirmed cases. The mathematical expressions of forecasting models, data acquisition, performance evaluation of the models and conclusions drawn from the results are explained.

II. Theoretical Background

We searched the literature for a simple and appropriate time series forecasting model for the prediction of daily occurrences coronavirus cases for a given set of environmental, logistical and other ambient health system parameters. In the process we identified Holt's model and its variants as more suitable. Earlier, Holt's Linear Exponential Smoothing (HLES) and its variants Holt-Winter Additive (HWA) and Multiplicative (HWM) are widely used for forecasting in business fields and ionospheric parameters [4-7].

A. Holt's Linear Exponential Smoothing (HLES): Holts linear exponential smoothing is an extension of the simple exponential smoothing. It considers level and trend variations of historical data for forecasting future behaviour (Table 1).

Table 1: Mathematical Expressions Of hles Model

Parameter	Expression
Level (L_t)	$\alpha(dt)+(1-\alpha)(L_{t-1}+T_{t-1})$
Trend (T_t)	$\beta(L_t-L_{t-1})+(1-\beta)T_{t-1}$
Predicted (F_{t+p})	L_t+T_{tp}

Where, α and β are level and trend smoothing coefficients. dt is confirmed number of cases / fatalities on the present day, ' p ' is forecast days ahead.

B. Holt-Winters model: This is an extension of Holt's model with an inclusion of seasonal variations [4]. This is also called triple exponential smoothing because it uses three smoothing coefficients. There are two versions of this model namely additive and multiplicative models (Table 2).

Table 2: Mathematical Expressions of HWA and HWM Models

Parameter	HWA	HWM
Level (L_t)	$\alpha(dt-S_{t-s}^a)+(1-\alpha)(L_{t-1}^a+T_{t-1}^a)$	$\alpha(dt/S_{t-s}^m)+(1-\alpha)(L_{t-1}^m+T_{t-1}^m)$
Trend (T_t)	$\beta(L_t^a-L_{t-1}^a)+(1-\beta)T_{t-1}^a$	$\beta(L_t^m-L_{t-1}^m)+(1-\beta)T_{t-1}^m$
Seasonal (S_t)	$\gamma(dt-L_t^a)+(1-\gamma)S_{t-s}^a$	$\gamma(dt/L_t^m)+(1-\gamma)S_{t-s}^m$
Fitted (F_t)	$L_{t-1}^a+T_{t-1}^a+S_{t-s}^a$	$(L_{t-1}^m+T_{t-1}^m)S_{t-s}^m$
Predicted (F_{t+p})	$L_t^a+T_t^a p+S_{t-s}^a p$	$(L_t^m+T_t^m p)S_{t-s}^m p$

Where, α , β and γ are level, trend and seasonal smoothing coefficients, dt is number of confirmed cases on the present day, ' p ' is forecast days ahead, ' s ' is seasonal cycle duration, ' a ' and ' m '

indicate additive and multiplicative models. The smoothing coefficients of level (α), trend (β) and seasonal (γ) components are varied from 0 to 1 and smoothing coefficient values are selected at the minimum value of absolute error [4]. Initially, the level smoothing coefficient $\alpha=0$ is fixed and trend, seasonal coefficients (β and γ) are changed from 0 to 1 with an increment of 0.1. Similar procedure is repeated for various values of level smoothing coefficient ($\alpha=0.1, 0.2, 0.3, \dots, 0.9, 1$) and found the minimum value of absolute error.

III. Data Acquisition

Data on COVID-19 confirmed active cases and total deaths in various countries are taken from open sources (John Hopkins University that collected from World Health Organization: 'csse_covid_19_data/csse_covid_19_time_series/time_series_covid19_confirmed_global.csv'). Indian data is taken from the Indian COVID-19 dashboard (<https://www.covid19india.org/>).

IV. Results and Discussion

The occurrences of COVID-19 confirmed cases and deaths are increasing day by day globally irrespective of the countries' economical status. There are several models which can predict for longer periods, but their algorithms are more complicated and the reliability of such algorithms depends on so many factors. Even if one parameter is taken wrongly, the whole prediction goes wrong. But the present algorithm depends only on previous two weeks data for a given environment, government measures such as lockdown rules and existing health system and forecast very reasonably.

COVID-19 data corresponding to six countries namely USA, Russia, UK, Brazil, Italy and India are considered in the present analysis. For all the models, two cycles (each one week) of data is used to train the algorithm and find the values of α , β and γ . The reason for fixing one week as one cycle is that the virus incubation period varies from 5 to 14 days. Therefore, it is very reasonable to consider 7 days as one cycle. This assumption is giving good forecasting results.

Two cycles of data (daily occurrence of confirmed COVID-19 cases) starting from 28 April to 11 May 2020 is considered as input to the algorithms to predict the occurrence of the cases one week ahead from 12-18 May 2020. The performance of forecasting models is evaluated using statistical parameters namely Mean Absolute Percentage Error (MAPE), Standard Deviation (SD) and Root Mean Squared Error (RMSE). For this analysis, we estimated the errors by comparing the forecasted results with the actual observations of the forecasted

week. The forecasted results due to HLES, HWA and HWM models along with actual observations for the selected countries are shown in Figures 1 to 6. Comparative performance analysis in terms of selected statistical parameters MAPE, SD and RMSE is done and are summarized in Table 3.

Fig.1represents forecasted results due to the models and actual daily confirmed cases for US which is the most affected country in the world. HWM model is predicting better than the other two models. MAPE due to HWM model is best (7.35). Considering the uncertainty factors such as more testing on a particular day, people not reporting even though they have symptoms etc.the achieved MAPE is good. Performance wise Holts Linear Exponential model is least preferable for predicting the number of daily occurrences of confirmed cases. Similar to MAPE, the values of other two parameters SD and RMSE are relative to the absolute number of occurrences and achieved values helps in planning the COVID-19 related works for the week ahead.

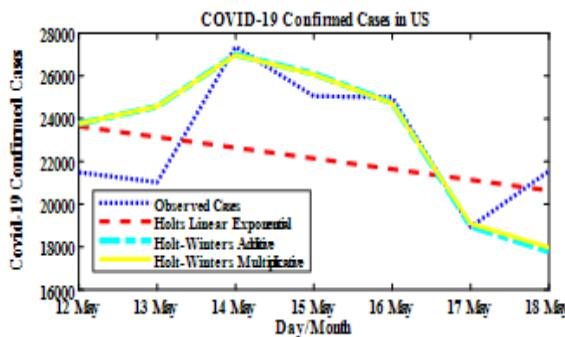


Fig 1: Comparison of forecasted COVID-19 daily occurrence of confirmed cases due to HLES, HWA and HWM with actual US data during 12-18 May 2020

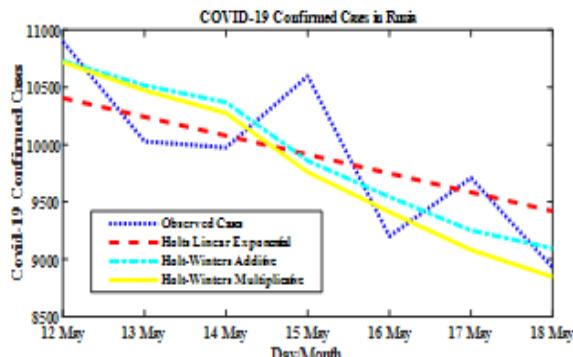


Fig 2: Comparison of forecasted COVID-19 daily occurrence of confirmed cases due to HLES, HWA and HWM with actual Russia data during 12-18 May 2020

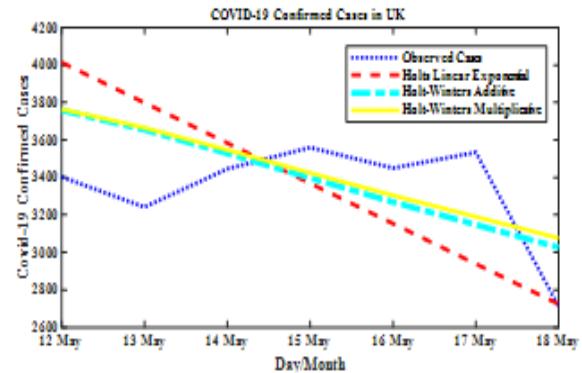


Fig 3: Comparison of forecasted COVID-19 daily occurrence of confirmed cases due to HLES, HWA and HWM with actual UK data during 12-18 May 2020

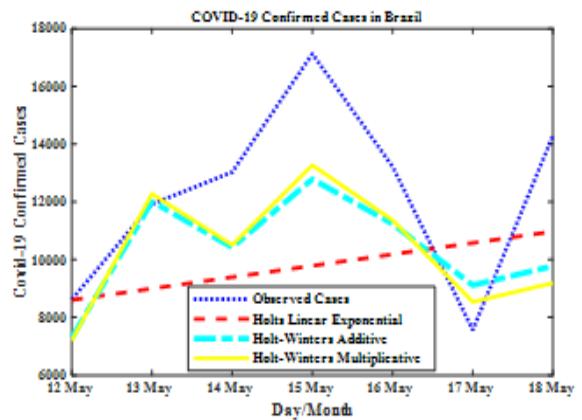


Fig 4: Comparison of forecasted COVID-19 daily occurrence of confirmed cases due to HLES, HWA and HWM with actual Brazil data during 12-18 May 2020

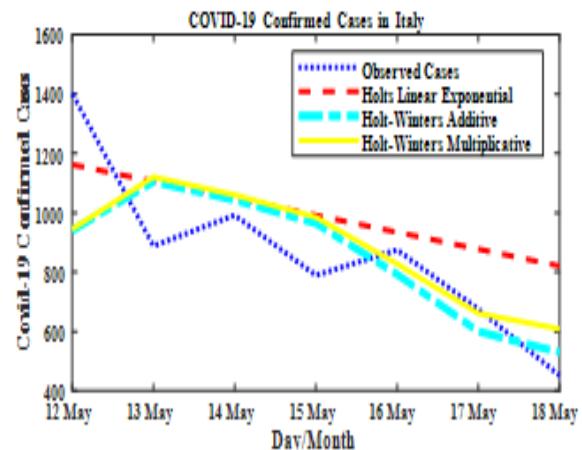


Fig 5: Comparison of forecasted COVID-19 daily occurrence of confirmed cases due to HLES, HWA and HWM with actual Italy data during 12-18 May 2020

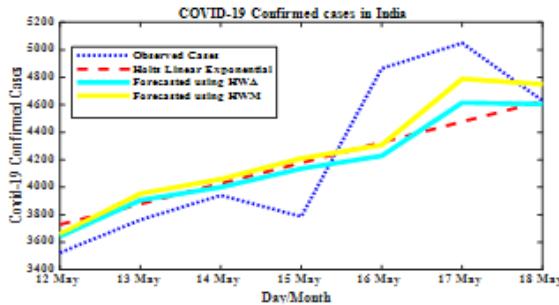


Fig 6: Comparison of forecasted COVID-19 daily occurrence of confirmed cases due to HLES, HWA and HWM with actual India data during 12-18 May 2020

Table 3: Comparison Of Absolute Errors Of Forecasted Results Due To Hles, Hwa And Hwm Models

Models	Errors	Countries					
		US	Russia	UK	Brazil	Italy	India
HLES	MAPE	11.1	3.84	10.05	25.91	27.3	6.2
	Std.	2960.3	470.4	442.2	3223.1	192.41	369.0
	RMSE	2848.3	435.6	410.7	3870.9	217.0	344.6
HWA	MAPE	7.37	3.95	8.27	18.35	17.5	5.7
	Std.	2315.7	469.9	311.8	2215.1	227.7	348.1
	RMSE	2174.0	435.1	295.3	2778.3	211.3	328.0
HWM	MAPE	7.35	3.81	8.26	17.67	19.0	6.0
	Std.	2260.3	480.2	304.3	2160.3	234.7	325.5
	RMSE	2129.1	458.0	295.6	2770.4	218.2	302.6

Similar analysis is carried out for another five countries (Fig. 2-6). In the case of Russia, all three models behaved very similar. Minimum MAPE is due to HWM model(3.81). In the case of UK also, even though all models behaved similarly, HWM shown a marginally better performance in all three parameters.

In the case of Brazil the occurrence of confirmed cases is very much random, reached a peak on fourth day and suddenly fallen the next two days. Even then, both HWA and HWM (MAPE:18.35 and 17.67) performed reasonably well and performance is similar, whereas the performance of HLES model is not upto the mark (MAPE: 25.9).

In the case of Italy, overall, more or less the daily occurrence of cases is falling. Both HWA and HWM performed better in terms of MAPE. Whereas RMSE due to HLE is least among the three models. Overall, the performance of all the models is very similar.

In contrast to Italy, in India overall the cases are increasing. Performance of all the three models is

very much similar. HWA and HWM models are marginally doing better than the HLES model. The MAPE due to these models are 5.7, 6.0 and 6.2 respectively.

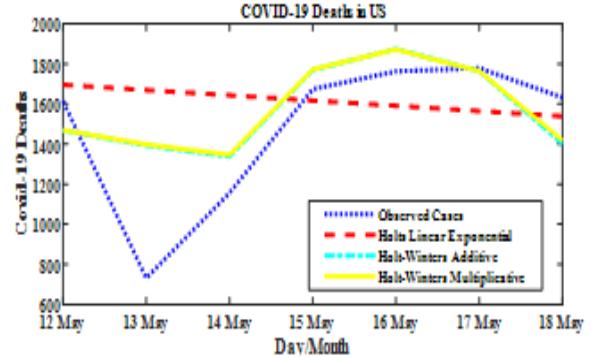


Fig 7: Comparison of forecasted COVID-19 daily occurrence of death cases due to HLES, HWA and HWM with actual US data during 12-18 May 2020

As US is the most affected country both in terms of number of confirmed cases and deaths, the proposed models are tested for predicting the deaths also and results are shown in Fig.7. For HLES, the absolute error values (MAPE=29.4, SD=423.87 and RMSE= 416.1) are high as compared to HWA (MAPE=20.34, SD=290.6 and RMSE=284.9) and HWM (MAPE=20.38, SD=288.9 and RMSE=285.17). Both HWA and HWM performed very similarly, whereas the performance of HLES is comparatively poor.

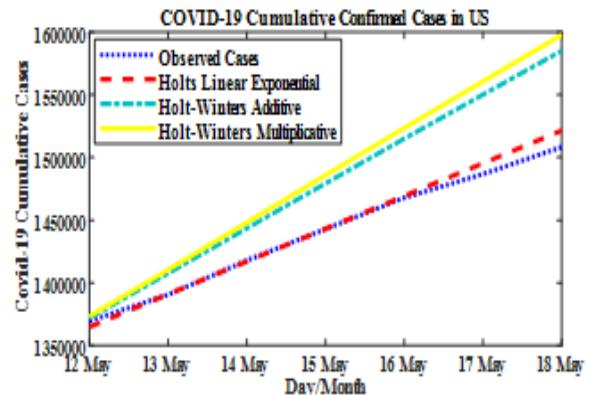


Fig 8: Comparison of forecasted COVID-19 daily occurrence of confirmed cases (cumulative) due to HLES, HWA and HWM with actual US data during 12-18 May 2020

Several countries' websites and dashboards show total cumulative cases and generally the cumulative graph increase or decrease depending on which stage the spread of virus is. The same models are tested for the same period,for cumulative data of confirmed cases for the case of US and the results are shown in Fig.8. The absolute errors are minimum in

HLES as compared to HWA are HWM models. For HLES, the absolute error values (MAPE=0.28, SD=6131.27 and RMSE= 6255.98) are minimum as compared to HWAmode (MAPE=2.61, SD=26171.0 and RMSE=45436.79) and HWM Model (MAPE=3.07, SD=30241.2 and RMSE=53181.73). Compared to the previous results (Fig.1) the forecasted cumulative results are very poor and are not acceptable.

V. Conclusion

In this letter, we proposed three variants of original Holt's model and tested for selected six countries where the pandemic is severe. Overall, for forecasting the number of daily occurrence of confirmed cases, Holt-Winter's Multiplicative model is performing better than the other two models. Also it is found for predicting the daily deaths the performance of both HWA and HWM is moderate and that of HLES is poor. These models are also tried for forecasting cumulative occurrence of confirmed cases and found that models' performance is poor. Therefore, it is suggested to use HWM model for forecasting the number of daily occurrence of confirmed COVID-19 cases.

VI. Acknowledgement

The work presented in this paper is the byproduct of a project entitled "A Local Short Model for Forecasting Ionospheric Scintillations for GNSS Applications over Indian Region" sponsored by RESPOND, ISRO Bangalore, vide sanction letter no:ISRO/RES/2/399/15-16, dated:13 July2015. The extensive work carried out on forecasting models by Late Mr. G.Venkateswarlu is greatly acknowledged.

References

- [1] Nadia Al-Rousan, Hazem Al-Najjar, 'Nowcasting and Forecasting the Spreading of Novel Coronavirus 2019-nCoV and its Association With Weather Variables in 30 Chinese Provinces: A Case Study', LANCET Conference, Feb 2020, DOI: 10.13140/RG.2.2.11932.85124
- [2] Joseph T Wu, Kathy Leung and Gabriel M Leung "Nowcasting and forecasting the potential domestic and international spread of the 2019-nCoV outbreak originating in Wuhan, China: a modelling study", Research article, Vol 395 February 29, 2020.
- [3] Desai AN, Kraemer MUG, Bhatia S, et al. Real-time epidemic forecasting: challenges and opportunities. Health Secur 2019;17: 268–75.
- [4] Winters, P. "Forecasting sales by exponentially weighted moving averages" Manage. Sci., 6:324-342, 1960.
- [5] Chatfield C., "The Holt-Winters Forecasting Procedure," Applied Statistics, 27, 264-279, 1978.
- [6] A.D. Sarma, K.C.T. Swamy and P.V.D. Somasekhar Rao, "Forecasting of Ionospheric Scintillations of GPS L-Band Signals Over an Indian Low Latitude Station", presented at IEEE International Symposium on Antenna and Propagation and USNC-URSI National Radio Science Meeting, Memphis, Tennessee, USA, 6-11 July 2014
- [7] G. Venkateswarlu and A. D. Sarma "A New Technique Based On Grey Model For Forecasting Of Ionospheric GPS Signal Delay Using GAGAN Data" Progress in Electromagnetics Research M (PIERM), Vol. 59, page 33-43, 2017, ISSN: 1937-8726, doi:10.2528/PIERM17041403.



Front View



Back View

Research and Entrepreneurship Hub, CBIT