Fake Accounts Detection in LinkedIn

1. Shwet Kamal, 2.Sanjeev Kumar, 3.Rahul Kumar, and 4.Vivek Singhal

Department of Information Science
Cambridge Institute of Technology
Bangalore 560036, INDIA

Dr. Preethi S

Department of Information Science
Cambridge Institute of Technology
Bangalore 560036, INDIA
preethi.ise@cambridge.edu.in

Abstract - Social media like LinkedIn are an integral part of our lives. People all over the world are actively engaged in it. But at the same time, it faces the problem of fake profiles. Fake profiles are generally human-generated or bot-generated or cyborgs, created for spreading rumours, phishing, data breaching, and identity theft. Therefore, in this article, we discuss a detection model, which differentiates between fake profiles and genuine profiles on LinkedIn based on visible features like avg_time_in_previous_position,avg_current_position_lengt,n_follo wer, m_urn_id and more by using various machine learning methods. We used the dataset of LinkedIn profiles, TFP and E13 for genuine and INT, TWT and FSF for fake accounts. Here we talk about Neural Networks, Random Forest, XG Boost, and LSTM. The significant features are selected for determining the authenticity of a social media profile. Further, the architecture and hyper parameters are discussed. Finally, the models are trained, and results are obtained. As a result we get output as 0 for real profiles and 1 for fake profiles. After a profile is detected fake it can blocked/deleted and cyber security threats can be avoided. The language used for implementation is Python3 along with all the required libraries like Numpy, Sklearn, and Pandas.

Keywords: Neural Network, Random Forest, XG Boost, Social Media, Fake profile.

I. INTRODUCTION

The Social media has become a vital part of our lives. everyone is active on social media. It is a great platform to share information and interact with people. But everything has a downside. As social media is footing a firm spot in our lives, there are instances where it has turned out to be a problem.

There are 900 million members in more than 200 countries and territories worldwide. LinkedIn is the largest professional network in the world. Users can create a profile that highlights their education, work experience, skills, and accomplishments, and connect with other professionals in their industry or field. LinkedIn also offers a range of features for job seekers, recruiters, businesses, and marketers to leverage the power of the platform for career and business growth. Fake accounts can be human-generated or computer-generated or cyborgs [2]. Cyborgs are accounts initially created by humans but later operated by computers.

Fake profiles usually get created in pseudo names and misleading and abusive posts and pictures are circulated by these profiles to manipulate the society, or to push anti-vaccine conspiracy theories, etc. Every social media platform is facing the problem of fake profiles these days.

The goal behind creating fake profiles is mainly spamming, phishing, and obtaining more followers. The malicious accounts have full potential to commit cyber crimes. The counterfeit accounts propose a major threat like identity theft and data breaching. These fake accounts send various URLs to people which when visited. Send the entire user's data to faraway servers that could be utilized against an individual. Also the fake profiles, created seemingly on behalf of organizations or people, can damage their reputations and decrease their numbers of likes and followers.

Along with all these, social media manipulation is also an obstacle. The fake accounts lead to the spread of misleading and inappropriate information which in turn give rise to conflicts.

These fake accounts get created to obtain more followers too. Who doesn't want to be voguish on social media? To achieve a high figure of followers, people tend to find fake followers. Over all, it has been observed that fake profiles because more harm than another cyber crime. Thus it is important to detect a fake profile even before the user is notified.

In this very context here, we talk about detecting fake profiles on LinkedIn. We deploy various machine learning models. The dataset of LinkedIn profiles E13 and TFP for genuine, and INT, TWT, FSF for fake is taken into use. To combat the creation of fake profiles, common defences are:

Methods such as user verification must be incorporated while creating accounts on social media.

To detect abnormal activities, user behaviour analysis must be employed. Bot detection solution consisting of analyzation based on real-time AI will be beneficial.

An automated bot protection tool must be used. As a technical contribution, we designed a multi-layer neural network model, a random forest model, an XG boost model, and an LSTM model. The mentioned models are supervised machine learning models.

Also, the LSTM classifies based on posts; the result can be combined with a convolution neural network in the near future [6].

The paper is organized into sections. The past researches, data pre-processing, methodology, experimental results, the accuracy of models, conclusion, and future work are described in order.

II. RELATED WORK

Social media: A Boon or Bane, this question has always subsisted. And all companies have aimed at providing a platform with the least errors and better experience. Hence, every day new developments and updates are done. Seeing that not enough is done so far for the detection of fake human identities on social media platforms like Twitter, we looked toward past research addressing similar problems.

Some methods classified profiles based on the activity of the account, the number of requests responded, messages sent, and more. The models use a graph-based system. Some methods also aimed at identifying between bots and cyborgs. Some past researches are mentioned below.

If certain words appear in a message, then the message is considered spam. This concept has been used to detect fake profiles on social media. For the detection of such words on social media, pattern matching techniques were used. But the significant drawback of this rule is that with time there is the continuous development and use of new words. Also, the use of abbreviations like lol, gbu, and gn is becoming popular on Twitter.

Sybil Guard [13] developed in 2008 aimed at limiting the corrupting influence of Sybil attacks via social media. It had constrained random walk by every node and was based on the occurrence of random-walk interactions. The dataset used was Kleinberg's synthetic social network.

Along with Sybil guard, another approach called the Sybil limit was also developed around the same time. Like Sybil guard, it also worked on the assumption that the non-Sybil region is fast mixing. It worked on the approach of multiple random walks by every node. And ranking was based on the occurrence of tails of walk intersection.

Sybil-infer was developed in 2009. It made use of methods like greedy algorithm, Bayesian inference technique, and Monte Carlo sampling with the assumptions like the non-Sybil region is fast mixing, and random walks are fast-mixing. The selection technique is threshold based on probability.

Mislove's algorithm,2010 worked on the Facebook dataset using greedy search and selected profiles based on metric normalized conductance.

In 2011, came a new model named facebook immune system that used random forest, SVM, and boosting techniques. It also used the Facebook dataset, and the feature loop was the selection technique.

An algorithm is used by Facebook to detect bots based on the number of friends which could be either related to tagging or relationship history. The rules stated above can identify bot accounts but are not successful to identify fake accounts created by humans. Unsupervised ML was used for detecting bots. In this technique instead of labeling, information was assembled based on closeness. The bots were recognized by grouping functions so admirably because of co-attributes. Sybil rank [1][13] designed in 2012, is based on a graph-based system. The pro- files were ranked based on interactions, tags, wall posts. The profiles with a high rank are labeled as real profiles and the ones with lower as fake. But this method was unreliable as there were instances where a real profile was ranked low.

Next, there was another model developed called the Sybil frame. It used a multi- stage level classification. It worked in two steps, firstly on a content-based approach and secondly on a structure-based method.

Filtering is also among one of the past approaches. A new threat or malicious activity is detected, and the account is added to the blacklist. But as far as human-fake accounts are concerned they tend to adapt and yet somehow avoid the blacklist.

Researches were also done to detect fake accounts based on factors like engagement rate and artificial activity. An engagement rate is the percentage of the interaction of the audience with a post. The engagement rate is calculated as (Total number of interactions/ Total number of followers) x100. These interactions could be in the form of likes, shares, or comments.

Artificial activity is based on the number of shares, likes, and comments made by a particular account. Insufficient information and the status of verification of email are also considered as an artificial activity.

In our model, we used a multi-layered neural network, random forest [9] approach, and XG Boost that work on the visible features of a profile. These extracted features are stored in a comma-separated file(CSV) that is easy to read by the model. Finally, after all, training, testing, and evaluating the model can label a profile as legitimate or not. We trained our models on Google Colab because Google provides the use of free GPU. The Google Colab 12GB NVIDIA Tesla K80 GPU that can be used up to 12 hours continuously. All the models were coded down in Python3.

A. Methodology:

For the detection of fake LinkedIn profiles, we incorporated various supervised methods, all with the same goal yet different accuracy. Each model detects a fake profile based upon visible features only.

All these supervised models are fed the same dataset, and corresponding accuracy and loss graphs are plotted. Also, a comparison graph of the accuracy of different models is indicated. The models are trained using appropriate optimizers, loss functions, and activation functions. The models used, mentioned below.

B. Pre-processing:

Before proceeding for the models, we append one more stride i.e pre-processing. The data set is pre-processed before it is fed to a model. Our model aims at detecting a profile as a hoax or legitimate based on the visible characteristics. Henceforth, all the precise aspects are determined. Only the numerical data has been selected and the categorical features are discarded. The following traits are picked [10]:

avg_time_in_previous_position	avg_current_position_length	avg_previous_position_length	m_urn_id	lang_num	no_of_promotions	no_of_previous_positions	current_position_length	age	n_followers

Then the data set of fake and genuine users are merged into one with an additional label for each profile i.e. ”is Fake” that is a Boolean variable. It is then stored in the Y variable that is the response concerning a profile X. Finally the blank entries or NAN are substituted with zeros.

C. Artificial Neural Network:

Neural networks [8] are the deep learning models that work similarly to the neuron network of a human brain. The neural network has layers, and each layer has neurons (nodes). We used the sequential from Keras. The model design with an input layer, three hidden layers, and an output layer has activation function ReLU for all but the output layer. Sigmoid, used as an activation function for the output layer. The model compiled using optimizer: Adam, loss functions: bi- nary cross-entropy. In our model, ANN of the stated above architecture is used. Sigmoid function finally provides the output between 0 and 1 and based on the prediction of a particular profile, labelled as fake or genuine.

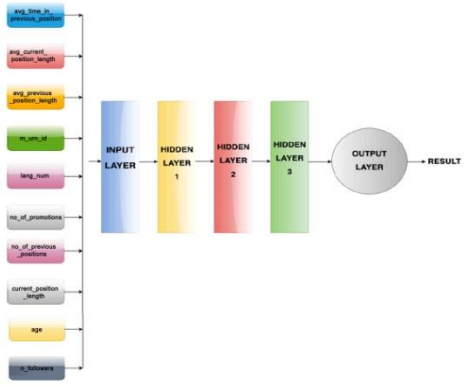

Fig. 1. ANN Architecture

D. Hyper parameters:

Rectified Linear Units (ReLU): Rectified Linear activation function is a piecewise linear function. ReLU (Fig. 2) is the default activation function for many neural networks as it is easier to train and produces better results

$$R(z) = \max(0, z) \qquad (1)$$

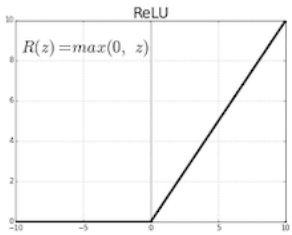

Fig. 2. Rectified Liner Units.

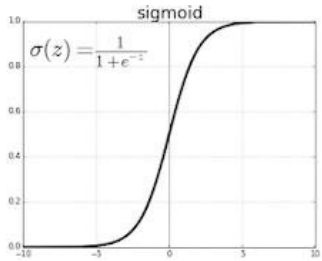

Fig. 3. Sigmoid Function.

Sigmoid Function: This is also known as the logistic function. When values between 0.0 and 1.0 are required sigmoid function(Fig. 3) is used. It is a non-linear activation function and is differentiable and hence slope can be found at any two points.

$$\sigma(z) = \frac{1}{1 + e\text{-}z} \qquad (2)$$

If z is very large then e^z is close to zero and

$$\sigma(z) = \frac{1}{1 + 0} \approx 1 \qquad (3)$$

If z is very small then e^z is large and

$$\sigma(z) = \frac{1}{1 + \text{large number}} \approx 0 \qquad (4)$$

E. Random Forest:

Random-forest also known as random-decision-forest is one of the methods that correspond to the category ensemble learning methods. This method is used in machine learning due to its simplicity in solving regression problems as well as classification. Random-forest, unlike the decision tree method, generates multiple decision trees, and the final output is collectively the result of all the decision trees formed. Similarly, we deployed the random forest [9] method for profile detection. The data is fed to the model and corresponding outputs are obtained. While train- ing, the bootstrap aggregating algorithm is applied for the given set of X = x1, x2.....xn and Y = y1, y2 yn responses, repeatedly (B times) random sample is selected and fits the trees(fb) to the sample. After training the predictions for a given sample (x’) is calculated by the formula specified below:

$$\hat{f} = \frac{\sum_{b=1}^{B} f_b(x')}{B} \qquad (5)$$

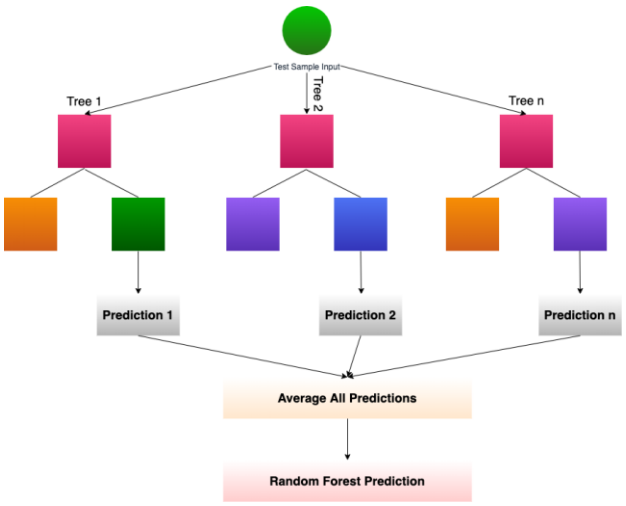

Fig. 4. Random Forest Architecture

F. Extreme Gradient Boost:

XG Boost is another ensemble learning method used for regression. this implements the stochastic gradient boosting algorithm.

Random forest has a drawback, it is efficient only when all inputs are available i.e there is no missing value. To overcome this we use a gradient boosting algorithm.

As per the boosting algorithm, firstly, F0(x) is initialized.

$$F_0(x) = \underset{\gamma}{\operatorname{argmin}} \sum_{i=1}^{n} L(y_i, \gamma) \quad (6)$$

Then iterative calculation of gradient of loss function takes place

$$r_{im} = -\alpha \left[\frac{\partial L(y_i, F(x_i))}{(F(x_i)} \right] \quad (7)$$

Finally the boosted model $F_m(x)$ is defined

$$F_m(x) = F_{m-1}(x) + \gamma_m h_m(x) \quad (8)$$

α is the learning rate

γ_m is the multiplicative factor

G. Long short-term Memory:

LSTM is recurrent neural network architecture. This architecture is capable of learning long-term dependencies.

In our project, we have developed a model using LSTM that classifies the profile as fake or genuine based on posts. Before training the LSTM on the posts, we pre-processed the data by forming a string of tokens from each activities.

1. We have converted all tokens into lower case.
2. We have removed the stop words from posts.

Then, we have transformed these tokenized posts into an embedding layer to create word vectors for incoming words. The resulting sequence of vectors is then fed to the LSTM that outputs a single 32- dimension vector that is then fed forward through sigmoid activated layers to give the output.

H. Experimental Results:

We used the dataset available on MIB [17]. The data set consisted of 3454 genuine profiles and 3352 fake profiles. The data set selected was TFP and E13 for genuine and INT, TWT and FSF for fake accounts. The data is stored in CSV file format for easy reading by the machine.

All the labels on the x-axis depict the features used for the detection of the fake profile. These got selected during the pre-processing. The y-axis depicts the number of entries corresponding to each feature available in the dataset.

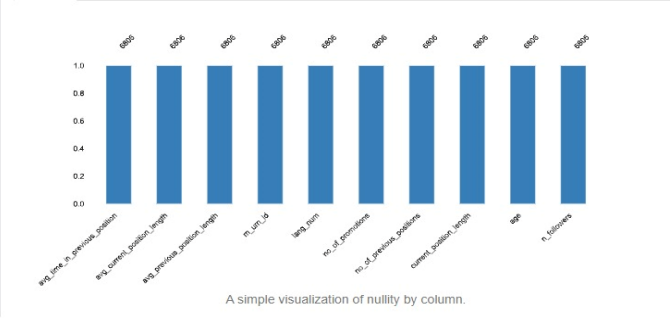

Fig. 5. Data set

I. Graphs and Charts

After training and testing all the models, the following results were obtained. The model accuracy, model loss vs the epochs graphs are plotted for neural network LSTM, and model accuracy comparison, and ROC curve for random forest, XG boost and other methods.

Neural Network: The model accuracy graph and model loss graph for the trained neural network are as follows:

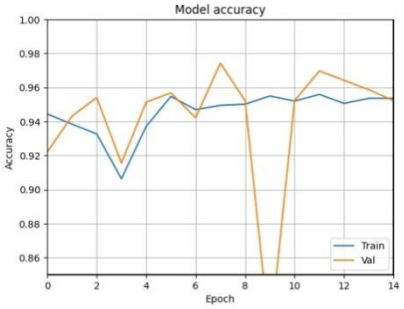

Fig. 6. Model Accuracy

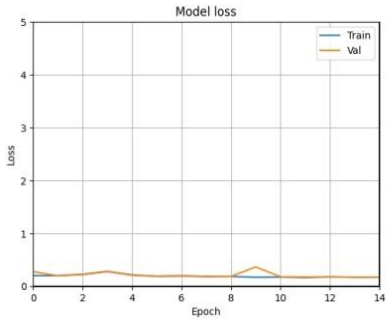

Fig. 7. Model loss

After running for 15 epochs the above accuracy and loss graphs are obtained. Initially, starting from 0.93 the accuracy varies along the path and finally reaches its maximum i.e. 0.952. Similarly, the loss graph for testing data begins from 1, and for validation data begins from 4 and eventually reaches a minimum point, less than 0.5.
To calculate the loss Binary cross-entropy function is used. Initially, random weights get assigned to each feature and finally the machine defines a unique weigh to each feature.

Random Forest and other methods: In the comparison chart below we observe accuracy of different models namely random forest, xg boost, ada boost, and decision tree.
The maximum accuracy is achieved by XG boost that equals to 95.22. Further we have decision tree and random forest with approx similar accuracy of 0.96. At last we have ADA boost.
Histogram for accuracy comparison and the ROC curves are as follows:

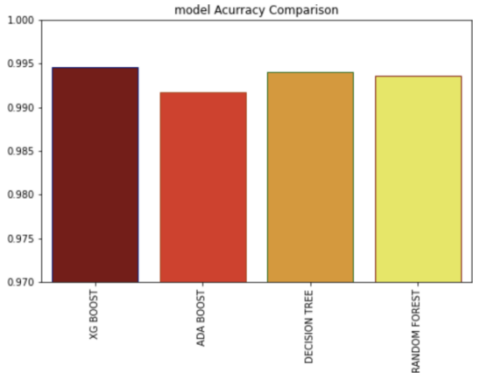

Fig. 8. Accuracy of Different Models

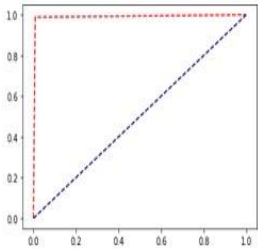

Fig. 9. ROC curve XG Boost

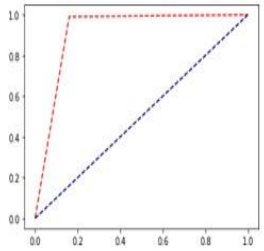

Fig. 10. ROC cruve Random Forest

II. Conclusion

In this design, we implemented the Neural Network, Random Forest, and XG Boost machine learning methods to train our system to detect fake LinkedIn pro- files based on visible data. After training, validating, and testing our models on the MIB data set we finally arrive at an inference that the maximum accuracy achieved is 95.22% by XG Boost method followed by ANN and random forest. Further work can be done by combining images of profiles along with the categorical and numeric data and implement using a CNN. Also, including other parameters, combining different models, and assembling a real-time model may achieve better results.

References

[1] Gergo Hajdu, Yaclaudes Minoso, Rafael Lopez, Miguel Acosta, Abdelrahman Ellei- thy: Use of Artificial Neural Networks to Identify Fake Profiles.
[2] Est´ee Van Der Wal: Using Machine Learning to Detect Fake Identities: Bots vs Humans.
[3] Aleksei Romanov, Alexander Semenov, Oleksiy Mazhelis and Jari Veijalainen: De- tection of Fake Profiles in Social Media.
[4] Yasyn ELYUSUFI, Zakaria ELYUSUFI, M'hamed Ait KBIR:Social Networks Fake Profiles Detection Based on Account Setting and Activity.
[5] Stefano Cresci, Roberto Di Pietro, Marinella Petrocchi, Angelo Spognardi, Maur-izio Tesconi: Fame for sale: Efficient detection of fake LinkedIn followers.
[6] Sneha Kudugunta, Emilio Ferrara:Deep Neural Networks for Bot Detection
[7] Rohit Raturi: Machine Learning Implementation for Identifying Fake Accounts in Social Network August International Journal of Pure and Applied Mathematics (2018) .
[8] M. Likitha, K. Rahul, A. Prudhvi Sai, A.Mallikarjuna Reddy: Design and Devel- opment of Artificial Neural Networks to Identify Fake Profiles.
[9]Yasyn Elyusufi, Zakaria Elyusufi, A¨ıt Kbir M'hamed: SocialNetworksFakePro- filesDetectionUsingMachineLearningAlgorithms https://www.researchgate.net/ publication/339012245/
[10] Naman Singh, Tushar Sharma, Abha Thakral, Tanupriya Choudhury: Detection of Fake Profile in Online

Social Networks Using Machine Learning in International Conference on Advances in Computing and Communication Engineering.(2018).
[11] Dr. Preethi S, Dr. Jayanthi M G and Ms. Yashaswini S, "An Efficient Hybridization Approach for Tissue Segmentation and Classification in Brain MRI Images", International Journal of Novel Research and Development, ISSN 2456-5184, 03-03-2023.
[12] Prof. Priyanka R and Dr. Satyanarayan Reddy, "An end-to-end securitu aware WSN approach with localization & Authentication and data exchange security", International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies,ISSN 2228-9860,23-05-2022.
[13] Mr. Krishna Kumar P R, Dr. Udaya Kumar and Dr. Chandramouli, "Traffic Management with Emergency Services using SmartIoT", IJCRT,ISS:2320-2882, 08-08-2022.
[14] Prof. Triveni N, "Literature Survey on early detection of breast cancer using IOT supervised learning techniques", Gradiva Review Journal,ISSN 0363-8057,22-05-2023.
[15] Mr. Krishna Kumar P R, Dr. Udaya Kumar and Dr. Chandramouli, "An e-office Applications using a Light weight and quick authentication using IOT", IJSREM, ISSN 2582-3930, 22-07-2023.
[16] Prof. Bharani B R, "Hybrid feature selection with parallel multi-class support vector machine for land use classification", INASS, ISSN:1882-708X, 21-10-2023.
[17] Prof. Priyanka R and Dr. Satyanarayan Reddy, "An efficient routing mechanism for node locaization,cluster based approach and data aggregation to extend WSN lifetime", INASS, ISSN:1882-708X, 16-09-2021.
[18] Mr. Krishna Kumar P R, Dr. Udaya Kumar and Dr. Chandramouli, "Preventing Vehicle accidents using Banana Pi and Multiple sensors", Gradiva Review Journal, ISSN 0363-8057, 21-06-2023.
[19] Prof. Priyanka R and Dr. Satyanarayan Reddy, "Design and Implementation of contact-less face mask dispenser", GIS SCIENCE, ISSN NO:1869-9391, 2021.
[20] Dr K. Satyanarayan Reddy and PundalikChavan, " Integrated Cross Layer Optimization Approach for Quality of Service Enhancement in Wireless Network", Indian Journal of Computer Science and Engineering (IJCSE), Volume 12 Issue 4 Pages 885-898, 2021.
[21] Dr. K Satyanarayan Reddy and Ajith Kumar V, "Secure device to device communications using lightweight cryptographic protocol", IJCSNS, Journal ISSN : 1738-7906,2021.
[22] Prof.Bharani B R, "Efficient Technique for Tagging and Archiving the Data Sets and Computation of Performance for Remote Sensing Data using Decision Tree", Journal of Huazhong University of Science and Technology,ISSN-1671-4512, 2021.
[23] Ms.Preethi and Ms.Aishwarya P , "An efficient wavelet based image fusion for brain tumor detection and segmentation over PET and MRI image", Journal Multimedia tools and applications,doi.org/10.1007/s11042-021-10538-3,2021.
[24] Dr. K Satyanarayan Reddy and Ms. Sonia Maria D'Souza, "Design and development of efficient cost saving algorithms for guiding customer purchasing patterns in modern consumerism scenario using feed forward back propogation neural networks", Springer Nature, DOI: 10.32628/IJSRSET218127, 2021.
[25] Dr. K Satyanarayan Reddy and Ms. Sonia Maria D'Souza, "Design and development of efficient cost saving algorithms for guiding customer purchasing patterns in modern consumerism scenario using Fuzzy Logic System", International Journal of Scientific Research in Science, Engg& Tech,ISSN:2395-1990, 2021.
[26] Ms. Preethi S and MARIA KIRAN L, "Security approach for data migration in a cloud computing environment",JETIR, (ISSN-2349-5162),2020.
[27] Dr K Satyanarayan Reddy, Ms. Tejashwini N and Dr. D R Shashi Kumar, "Multistage Secure Clusterhead Selection using Discrete Ruleset against Unknown Attacks in Wireless Sensor Network", International Journal of Electrical and Computer Engineering, ISSN 2088-8708,2020.
[28] Dr. K Satyanarayan Reddy and Mr. Ajith Kumar V, "D2d Communication Security Lightweight Crytographic Approach: Critical Survey", International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878,2020.
[29] Dr. Satyanarayan Reddy K and Ms.Priyanka.R, "A Comprehensive Survey on Energy Efficient Routing Techniques and Various Attacks in Wireless Sensor Networks", Scopus Indexed Journal (Unpaid) International Journal on Emerging Technologies (IJET), ISSN No. (Online): 2249-3255 0975-8364,2020.
[30] Dr. K. Satyanarayan Reddy and Mr.Pundalik Chavan, "Qos Aware Video Transmission in Wireless Network: Successful and Failure Existing Technique", International Journal of Recent Technology and Engineering (IJRTE),ISSN:2277-3878,2020.
[31] Mr. Krishna Kumar P R, Dr. Chandra Mouli and Mr. Udaya Kumar, "Gadget based cloud utilization for smart lighting system using IoT and Bluetooth", IJESC, ISSN:2321 3361,2020.
[32] Dr. K. Satyanarayan Reddy, Mr.Rahul and Ajithkumar, "Watermarking Schemes for High Security with Applications and Attacks: Research Challenges and Open Issues", International Journal of Recent Technology and Engineering (IJRTE), ISSN:2277-3878, 2019.
[33] Dr K Satyanarayan Reddy, Ms. Tejashwini N and Dr D R Shashi Kumar, "Novel Framework for Maximizing Security over Wireless Net", International Journal of Innovative Technology and Exploring Engineering(IJITEE),ISSN: 2278-3075, 2019.
[34] Ms. Bharani B R, "A survey on predictive analytics and parallel Algorithms for knowledge extraction from date received through various satellites", IRJET, e-ISSN: 2395-0056, 2019.
[35] Ms. Sapna and Dr. Shashi Kumar D R, "Revisiting security aspects of Internet of things for self-managed devices", IRJET,e-ISSN: 2395-0056 p-ISSN: 2395-0072, 2019.

[36] Dr. K. Satyanarayan Reddy, Mr. Mahesha A.M and Dr. Ganashree T.S, "Survey on Adaptive Particle Swarm Optimization based Watermarking of Digital Images for High Security", International Journal of Research and Analytical Reviews (IJRAR),E-ISSN 2348-1269, P- ISSN 2349-5138, 2019.
[37] Dr. K. Satyanarayan Reddy and Ms. P.Soubhagyalakshmi, "Empirical Survey on BYOD Security and Usage",International Journal of Recent Technology and Engineering (IJRTE),ISSN:2277-3878, 2019.
[38] Dr. K. Satyanarayan Reddy and Ms. Nidhi Agarwal, "Local Debugging of Efficient Monitoring Mechanism Using AWS Beanstalk: A Case Study", UGC Approved, Journal of Emerging Technologies and Innovative Research, [ISSN: SSN-2349-5162], 2019.
[39] Mr. Krishna Kumar P R, Dr. Chandra Mouli and Mr. Udaya Kumar, "Traffic management with emergency servicesbnusingSmartIoT", International Journal of Engineering Science and Computing,2019.
[40] Dr. K. Satyanarayan Reddy and Mr. Vybhav V Kadam, "Real Time Home Automation Using Google Assistant",UGC Approved journal of Emerging Technologies and Innovative Research, ISSN: SSN-2349-5162,2019.
[41] Dr. K. Satyanarayan Reddy and Ms. M. B. Yashoda, "Intelligent Routing Protocols for Communication in Internet of Things: A Survey", Scopus Indexed Journal of Computational and Theoretical Nanoscience, American Scientific Publishers, California USA, ISSN: 1546- 1955 (Print): EISSN: 1546-1963, 2018.
[42] Mr. Krishna Kumar P R, Mr. Chandra Mouli and Mr. Udaya Kumar, "Web Architecture for Monitoring Field using Representational State Transfer Methods", International Journal of Intelligent Engineering and Systems, 2018.
[43] Dr. K.Satyanarayan Reddy and Yashoda M, "Intelligent Routing Protocols for Communication in Internet of Things : A Survey", International Conference on Topical Transcends in Science, Technology and Management ICTTSTM,ISSN: 1546- 1955 (Print): EISSN: 1546-1963, 2018.
[44] Mr. Krishna Kumar P R, Mr. Chandra Mouli and Mr. Udaya Kumar, "Low energy smart lighting system using IoT and Bluetooth", International Journal of Intelligent Engineering and Systems, ISSN:2250-1371,2017.
[45] Dr. K. Satyanarayan Reddy and Ms. Dulam Bhavya Sree, "A Systematic Approach Towards Classification and Description of Cyber Crime Incidents", International Journal of Engineering Development and Research (IJEDR), [ISSN:2321-9939], 2017.
[46] Dr. K. Satyanarayan Reddy and Ms. T S Nisha, "Profiling Based Reduce Memory Provisioning for Improving the Performance in HADOOP", UGC Approved Journal, Indian Journal of Scientific Research,ISSN: 0976-2876, 2017.
[47] Dr. K. Satyanarayan Reddy and T S Nisha, "A Survey on Optimization in Hadoop Big data Environment", International Journal for Research & Development in Technology, ISSN:-2349-3585, 2017.
[48] Dr. K.Satyanarayan Reddy and Ms. Pavithra R, "e-Commerce Recommendation over Big Data Based on Structural Balance Theory with the Prediction Rates", Imperial Journal of Interdisciplinary Research (IJIR), ISSN:2454-1362, 2017.
[49] Dr. K. Satyanarayan Reddy, Ms. PamidiSrinivasulu, Ms. V Lakshmi Chetana and Mr. R Venkat, "A New Approach for Clustering Large Data using Fuzzy C-Means (FCM) Clustering and Optimizing with Gravitational Search Algorithm", International IEEE Conference ICSTM, DOI: 10.1109/ICSTM.2017.8089157, 2017.
[50] Dr. K. Satyanarayan Reddy and Mr. AjithkumarVyasarao, "Application of Elliptic Curve Cryptography for Mobile and Handheld Devices", International Conference on Contemporary Issues in Science, Engineering & Management, ISSN: 2250-0138 (Online), 2017.

[51] Dr. K. Satyanarayan Reddy and Mr.Sumanth N, "A Comparative Study of Virtual Machine vs. Containers for Embedded systems such as Enterprise Routers", International Journal of Engineering Science & Computing (IJESC),ISSN: 2321-3361, 2017.
[52] Dr. K. Satyanarayan Reddy and Mr.Ajithkumar V, "A Survey on Security of Mobile Handheld Devices Through Elliptic Curve Cryptography", ACCENTS Transactions on Information Security, ISSN (Online):2455-7196, 2017.
[53] Mr. Krishna Kumar P R, Dr. Chandra Mouli and Mr. Udaya Kumar, "A Survey on the Internet of Things- Based Service Oriented Architecture", International Conference on Electrical, Electronics, Communication, Computer and Organization Techniques (ICEECCOT), DOI: 10.1109/ICEECCOT.2017.8284544 ISBN:978-1-5386-2362-6, 2017.
[54] Ms. Preethi S and Ms. Aishwarya P, "Combining Wavelet Texture Features and Deep Neural Network for Tumor Detection and Segmentation over MRI", De Gruyter, DOI 10.1515/jisys, DOI: 10.1515/jisys-2017-0090, 2017.
[55] Ms. Preethi S and Ms. Vanitha L B, "Detection of Neovascularization on Optic Disk Region based on Kernalized Fuzzy C-Means and ANN Classifier",International Journal of Innovative Research in Computer and Communication Engineering,ISSN : 2320-9801 ISSN : 2320-9798, 2017.
[56] Ms. Preethi S and Ms. Danya K, "A survey on time and attribute factors combined access control for time-sensitive data in public",IJEDR,ISSN: 2321-9939,2017,2017.
[57] Ms. Preethi S and Ms. Vanitha L B, "Performing an efficient Auditing and deduplication data process of the cloud systems", International Journal of Innovative Research in Computer and Communication Engineering,ISSN:0976-1353,2016.
[58] Santosh Hanchinal and Dr.K. Satyanarayan Reddy, "Cloud Information's Study for Typical Overlapping Social Networks", International Journal of Innovative Research in Computer and Communication Engineering,ISSN:2320-9801, 2016.
[59] Raghavendra G and Dr. K. Satyanarayan Reddy, "Virtual Calling Number for ESME", 10th INDIACom (IEEE Conference), 2016, 3rd International Conference on Computing for Sustainable Global Development,ISSN: 0973-7529, ISBN: 978-93-80544-19-9, 2016.
[60] Shilpa M, Preethi S and Dr Suresh, "Combining Left and Right Palm Print Images for more Accurate Personal Identification", International Journal of Innovative Research in Computer and Communication Engineering, DOI : 10.15680/IJIRCCE, 2016.
[61] Preethi S and AishwarayaPalaniappan, "Brain tumor detection by modified particle swarm optimization algorithm and multi-support vector machine classifier", International Journal of Intelligent Engineering and systems, 2022.
[62] DR Preethi S, DR Jayanthi M G and Yashaswini S, "An efficient hybridization approach for tissue segmentation and classification in brain MRI images", International journal of novel research and development, ISSN:2456-4184, 2023.