



**PARVATHAREDDY BABUL REDDY  
VISVODAYA INSTITUTE OF TECHNOLOGY & SCIENCE**

(Affiliated to J.N.T.U., Anantapur & Approved by AICTE, New Delhi, Accredited by NBA-AICTE)

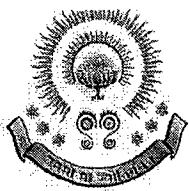
KAVALI - 524 201, S.P.S.R. Nellore Dist., A.P., India. ☎ 08626 - 243930



Late Dr. Doda Ramachandra Reddy  
Founder, Visvodaya.

### 3.3.2

Number of research papers per teachers in the Journals  
notified on UGC website during the last five years



**PARVATHAREDDY BABUL REDDY**  
**VISVODAYA INSTITUTE OF TECHNOLOGY & SCIENCE**  
(Affiliated to J.N.T.U.A, Approved by AICTE and Accredited by NAAC with 'A' Grade)  
KAVALI – 524201, S.P.S.R Nellore Dist., A.P. India. Ph: 08626-243930



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**Number of research papers in the Journals notified on UGC website during the last five years**

Academic Year	No.of publications
2019-20	23
2018-19	24
2017-18	10
2016-17	10
2015-16	09

  
Faculty Incharge

  
HOD  
Head of Department  
COMPUTER SCIENCE ENGINEERING  
Visvodaya Institute of Technology & Science and  
KAVALI - 524 201, SPSR, Nellore Dt.



**PARVATHAREDDY BABUL REDDY**  
**VISVODAYA INSTITUTE OF TECHNOLOGY & SCIENCE**  
(Affiliated to J.N.T.U.A, Approved by AICTE and Accredited by NAAC with 'A' Grade)  
**KAVALI – 524201, S.P.S.R Nellore Dist., A.P. India. Ph: 08626-243930**



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**List of faulty Publications for the academic year 2019-20**

S.No	Name of the Faculty	Title of the Paper	Journal Name and ISBN/ISSN	Vol.No. Issue No.	Month & Year	Link to relevant document
1	T.Manjula	Cognitive computing for sustainable agriculture	AJCST: 2249-0701	Volume VIII, No.S3	June 2019	<a href="https://www.trp.org.in/wpcontent/uploads/2019/06/NCICT-AJCST-Vol.-8-No.-S3-2019-pp.-159-161.pdf">https://www.trp.org.in/wpcontent/uploads/2019/06/NCICT-AJCST-Vol.-8-No.-S3-2019-pp.-159-161.pdf</a>
2	PVN.Rajeswari	Network Intrusion Detection Techniques and Network Attack Type	IJRTE,ISSN: 2277-3878	Volume-8 Issue-2S8	August 2019	<a href="https://www.ijrte.org/wp-content/uploads/papers/v8i2S8/B11780882S819.pdf">https://www.ijrte.org/wp-content/uploads/papers/v8i2S8/B11780882S819.pdf</a>
3	K.Sireesha	Network Intrusion Detection System And Network Attack Types- A Review	(IJRTE) ISSN: 2277-3878,	Volume-8 Issue-2S8,	August 2019	<a href="https://www.ijrte.org/wp-content/uploads/papers/v8i2S8/B11780882S819.pdf">https://www.ijrte.org/wp-content/uploads/papers/v8i2S8/B11780882S819.pdf</a>
4	PVN.Rajeswari	Concept Drift based identification of suspicious activity at specific IP Address using ML	IJRTE,ISSN: 2277-3878	Volume-8 Issue-3	September 2019	<a href="https://www.ijrte.org/wp-content/uploads/papers/v8i3/C5699098319.pdf">https://www.ijrte.org/wp-content/uploads/papers/v8i3/C5699098319.pdf</a>
5	P.Eswaraiah	Detection of financial fraud using codetect framework	IJITEE ISSN: 2278-3075	Volume-9 Issue-1	November 2019	<a href="https://www.ijitee.org/wp-content/uploads/papers/v9i1/L30951081219.pdf">https://www.ijitee.org/wp-content/uploads/papers/v9i1/L30951081219.pdf</a>
6	B.Murali Krishna	Secure and lightweight Access Control for personnel Health Information in cloud based IOT Devices	JES, ISSN NO:0377-9254	Volume 10 Issue 11	November 2019	<a href="https://jespublication.com/upload/2019-V10-I11-03.pdf">https://jespublication.com/upload/2019-V10-I11-03.pdf</a>
7	J.Vamsinath	Implementation of privacy protection access Control and keyword search scheme for Cloud storage systems	JES ISSN NO:0377-9254	Volume 10 Issue 11	November 2019	<a href="https://jespublication.com/upload/2019-V10-I11-01.pdf">https://jespublication.com/upload/2019-V10-I11-01.pdf</a>
8	P Srinivasulu	Elliptic Curve Digital Signature for third party Auditing	IJEAT ISSN: 2249-8958	Volume-9 Issue-2	December 2019	<a href="https://www.ijeat.org/wp-content/uploads/papers/v9i2/B3109129219.pdf">https://www.ijeat.org/wp-content/uploads/papers/v9i2/B3109129219.pdf</a>
9	D.Srinivasulu Reddy	Secure And Fast Biometric Verification Scheme For Cloud Storage Systems	IJITEE ISSN:2278-3075	Volume-9 ISSUE-2	December 2019	<a href="https://www.ijitee.org/wp-content/uploads/papers/v9i2/B6312129219.pdf">https://www.ijitee.org/wp-content/uploads/papers/v9i2/B6312129219.pdf</a>
10	PVN.Rajeswari	An Efficient fine grained keyword based search scheme in fog computing	IJRTE ISSN: 2277-3878	Volume-8 Issue-5	January 2020	<a href="https://www.ijrte.org/wp-content/uploads/papers/v8i5/E5095018520.pdf">https://www.ijrte.org/wp-content/uploads/papers/v8i5/E5095018520.pdf</a>
11	PVN.Rajeswari	A Hybrid secure storage scheme to avoid Edos Attacks in Cloud Computing ,	IJRTE,ISSN: 2277-3878	Volume-8 Issue-5	January 2020	<a href="https://www.ijrte.org/wp-content/uploads/papers/v8i5/E5861018520.pdf">https://www.ijrte.org/wp-content/uploads/papers/v8i5/E5861018520.pdf</a>
12	Dr.V.V.Sunil Kumar	Replica Node	IJRTE ISSN: 2277-3878	Volume-8 Issue-5	January 2020	<a href="https://www.ijrte.org/wp-content/uploads/papers/v8i5/E5021018520.pdf">https://www.ijrte.org/wp-content/uploads/papers/v8i5/E5021018520.pdf</a>
13	Dr.D.Srujan Chandra Reddy	RAN Method that performs Nested Scalable NO SQL Transaction and Data	IJARET ISSN:0976-6499	Volume11 issue 1	January 2020	<a href="https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3526831">https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3526831</a>



**PARVATHAREDDY BABUL REDDY**  
**VISVODAYA INSTITUTE OF TECHNOLOGY & SCIENCE**

(Affiliated to J.N.T.U.A, Approved by AICTE and Accredited by NAAC with 'A' Grade)

KAVALI – 524201, S.P.S.R Nellore Dist., A.P. India. Ph: 08626-243930



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

14	Dr.D.Srujan Chandra Reddy	A NoSQL Database Model with Nested Transactions Using Multi-Tenant Architecture	JES ISSN:0377-9245	Volume 11 issue 1	January 2020	<a href="https://jespublication.com/issue.php?cid=22&amp;scid=54">https://jespublication.com/issue.php?cid=22&amp;scid=54</a>
15	Dr.D.Srujan Chandra Reddy	Handling geo tagging data using no sql Databases in big data era	IJAEM ISSN NO: 0886-9367	Volume XII, Issue I,	January 2020	<a href="https://app.box.com/s/cd7dkpjcl1r499a9fxnpszidap3j57h6">https://app.box.com/s/cd7dkpjcl1r499a9fxnpszidap3j57h6</a>
16	T.Manjula	Cognitive IOT:An eco-friendly technology	ISSN:0193-4120	Volume 10 8724-8727	February 2020	<a href="https://www.trp.org.in/issues/cognitive-computing-for-sustainable-agriculture">https://www.trp.org.in/issues/cognitive-computing-for-sustainable-agriculture</a>
17	A.Prasmitha	A Review On Iot Devices	IJITEE ISSN:2278-3075	Volume-29 NO.4	July 2020	<a href="http://sersc.org/journals/index.php/IJAST/article/view/4036">http://sersc.org/journals/index.php/IJAST/article/view/4036</a>
18	B.Murali Krishna	Cryptographically Enforced Dynamic Access Control In Cloud Computing	ISSN NO:0377-9254	Volume 11 Issue 7	July 2020	<a href="https://jespublication.com/upload/2020-110780.pdf">https://jespublication.com/upload/2020-110780.pdf</a>
19	B.Murali Krishna	Implementation of an efficient data Sharing scheme for mobile cloud data	JES ISSN NO:0377-9254	Volume 11 Issue 7	July 2020	<a href="https://jespublication.com/upload/2020-110726.pdf">https://jespublication.com/upload/2020-110726.pdf</a>
20	B.Muralikrishna	Cloud Wizard	JES ISSN NO:0377-9254	Volume 6, ISSUE 7	July 2020	<a href="Https://www.ijrte.org/wp-content/uploads/papers/v8i3/C5699098319.pdf">Https://www.ijrte.org/wp-content/uploads/papers/v8i3/C5699098319.pdf</a>
21	B.Muralikrishna	Death Prediction And Analysis Using Web Mining Techniques	JES ISSN NO:0377-9254	Volume 11 ISSUE 7	July 2020	<a href="https://jespublication.com/upload/2020-110719.pdf">https://jespublication.com/upload/2020-110719.pdf</a>
22	Dr.V.V.Sunil Kumar	Improving Online Quantization In Dynamic Databases	JES ISSN NO:0377-9254	Volume 11 ISSUE 7	July 2020	<a href="https://jespublication.com/issue.php?cid=22&amp;scid=60">https://jespublication.com/issue.php?cid=22&amp;scid=60</a>
23	G.Venkateswarlu	tracking cyber-attacks and scrutiny of breaches	JES ISSN NO:0377-9254	Volume 11 issue 7	July 2020	<a href="https://jespublication.com/issue.php?cid=22&amp;scid=60">https://jespublication.com/issue.php?cid=22&amp;scid=60</a>

Faculty Incharge

D. AOD  
 Head of Department:  
**COMPUTER SCIENCE ENGINEERING**  
 Parvathareddy Visvodaya Institute of Technology & Science  
 KAVALI - 524 201, S.P.S.R Nellore Dt.

# Network Intrusion Detection Techniques and Network Attack Types

Rajeswari P. V. N., B. Rasagna, K. Sireesha, Sk. Shahina Begum

**Dynamic:** With the huge improvement in innovation and with the big utilization of internet, massive increment in internet dangers has been seeing which activates contriving of latest strategies in device protection, those types of gadget attacks as some distance as unapproved get to, unordinary assaults can be remedy making use of network Intrusion Detection device(NIDS). machine Anomaly Detection(NAD) framework is a particular assortment of IDS. it's miles a corresponding innovation to frameworks that distinguish safety dangers depending on parcel marks. In NAD, the device is unendingly decided for event of anomalous activities or unexpected assaults. by way of utilising this NAD techniques, it is plausible to select out in the occasion that all and sundry tries to attack property or particular has with the aid of using and contrasting and the records accrued from past regarded assaults. This paper gives diagram on severa classifications NID techniques and moreover numerous styles of structures assaults. We bear in mind that this audit will provide a advanced keen of the special commands of attack sorts records, which gives degree to analyze to retain similarly.

**Keywords:** laptop systems, network safety, community interruption discovery, attacks, dispensed DoS assault.

## I. ADVENT

With the developmental changes in innovation, and with the presentation of web idea, web become the wellspring of records for an applications. Parallelly, currently a-days it's miles established because the purpose for wonderful virtual assaults. As in keeping with Anderson [1], an interruption challenge or a peril is a practical and unlawful venture to (I) get entry to on mystery information, (ii) regulate or control the prevailing facts, or (iii) to reason the framework dishonest or not appropriate to anybody. for instance, (a) Denial of issuer (DoS) assault endeavors to be malnourished a large corporation of its assets, which can be required for making ready the data correctly; (b) Worms and infections get gain of greater has through the machine for breaking down; and (c) Compromises acquire unique get right of entry to a number with the aid of way of taking focal elements of diagnosed vulnerabilities. diverse calculations and techniques are familiar with cozy the system framework and correspondence over the net, among them the

utilization of firewalls idea, one of a type varieties of encryption strategies, and digital private systems are

Revised Version Manuscript Received on August 19, 2019.

**Rajeswari P. V. N.**, Dept of Comp. Sc. & Engg., Visvodaya Technical Academy, Kavali, AP, India.(email: rajivrphd@gmail.com)

**B. Rasagna**, Dept of Comp. Sc. & Engg., Visvodaya Technical Academy, Kavali, AP, India.(email: rasagnabheema87@gmail.com)

**K. Sireesha**, Dept of Comp. Sc. & Engg., Visvodaya Technical Academy, Kavali, AP, India.(email: kalapati.sireesha85@gmail.com)

**Sk. Shahina Begum**, Dept of Comp. Sc. & Engg., Visvodaya Technical Academy, Kavali, AP, India.(email: shaheena.vits@gmail.com)

assuming a essential manner. For execution of NIDS, basically methodologies are applied specifically: signature primarily based and abnormality based completely

vicinity [10]. The primary approach has showed as a business enterprise fulfillment. In mark based totally definitely strategy, NIDS will assist with a variety of marks, in which each considered one in every of which separate the diagram of a fantastic safety danger (for instance an contamination, or a trojan horse or a Denial of provider(DoS) assault). what's more, Anomaly based NIDS constantly check out device site visitors and look at it towards a conventional wellknown of regular site visitors layout. Contingent on this gave modern we are capable of separate what's "ordinary or normal" traffic inside the framework – for example, elegant information transmission use, the numerous conventions applied normally, proper combination of ports numbers for numerous applications in various gadgets. In mild of this distinction, the framework will act both because the pinnacle or the consumer at some thing factor uncommon web site traffic flow into is visible it's extensively divergent as of the benchmark. The method, oddity primarily based interruption reputation in computer structures alludes as an answer for the issue of coming across extraordinary examples in device site visitors that goes amiss from the regular everyday behavior. This form of bizarre examples are usually named as irregularities, anomalies, special instances, distortions, astonishments or attacks. As of now, Anomaly identification has extensively required in a part of makes use of, as an example, extortion discovery in budgetary branch to verify rate playing cards exchanges, interruption acknowledgment in remember or digital safety, and moreover in military supervision to observe the foe activities.

## II. CLASSIFICATION OF NETWORK INTRUSION DETECTION (NID)STRATEGIES

In fig1, severa styles of NIDS strategies are given.

### 2.1 Statistical primarily based strategies

Factually, an oddity or exception is an exam that is associated with being in component or honestly unessential motion as it isn't made via the stochastic version created and used[3]. by means of the usage of and large, for a measurable model those genuine techniques healthy (for the maximum issue for ordinary conduct) to the appropriate records and upon this information, a mathematical conclusion check is

# Concept-Drift Based Identification of Suspicious Activity at Specific IP Addresses using Machine Learning

P V N Rajeswari, M. Shashi

**Abstract –** Network Intrusion detection systems(IDS), especially those that monitor Denial of Service(DoS) attack, aim at monitoring the network traffic continuously in order to identify suspicious activity possibly initiated at one or more nodes at specific IP addresses. Traditional anomaly detection based IDS methods rely on preset bounds on the magnitude of network traffic based on statistical measures and hence are not programmable based on the changes in the network traffic dynamics. The authors proposed a methodology for monitoring the changes in the network traffic received from individual source nodes based on concept drift in order to identify suspicious activity at specific nodes. The framework applies machine learning techniques to capture the normal traffic patterns of various source nodes and accordingly defines lower and upper bounds dynamically for each node. Based on the temporal analysis in successive time windows, it is able to discriminate an abrupt change from a gradual change in the magnitude of traffic received in a time window from a node to identify suspicious activity at the corresponding IP address. The effectiveness of the methodology is tested on real world data.

**Keywords:** Network anomaly detection, Concept drift measure, Parametric learning and Packet sniffer.

## I. INTRODUCTION

Machine learning enables computers to improve their performance of doing a task through experience represented in the form of data records. Often statistical measures and models are used to extract the general patterns from the large collection of accumulated data records to capture the patterns of normality. Identification of suspicious activity in real time calls for anomaly detection methods that compare every activity with the patterns representing normality to check for the compliance. Any deviation from the normality implies either an anomaly or a changing trend. However, in domains with dynamically changing trends, in order to capture the changing trends, machine learning algorithms need to process data streams of records rather than accumulated collection of data records. Stream of records are processed in the order of their arrival to check for deviations from the extracted patterns which may possibly change with time representing time-variant trend that leads to identification of new patterns or otherwise anomalies. In this paper, the changing trends are identified based on concept drift with time, while differentiating them from anomalies specifically for anomaly based network intrusion detection systems.

**Revised Manuscript Received on September 23, 2019**

PVN Rajeswari, Assoc. Professor, Dept. of Computer Science and Engineering, Visvadaya Engineering College, Kavali, AP, India.

Email: rajivrphd@gmail.com

Dr. M. Shashi, Professor, Dept. of Computer Science and System Engineering, Andhra University, Visakhapatnam, AP, India.

Email: smogalla2000@yahoo.com

## A. Streaming Based Network Anomaly Detection

Internet is accepted as a vital and the most essential element of modern life to fulfill the communication and information requirements of people anywhere anytime; people are kept connected alleviating the differences in their geographical location, language and nationality. The other side of the coin of this global connectivity opens door for malicious users to attack the genuine users for gaining undue benefits or for destruction. Computers connected to other systems are prone to a variety of attacks which are termed as cyber-attacks. Competent Intrusion Detection System (IDS) is required for protection against such attacks, threats and vulnerabilities, etc. Based on the scope of their activity, Intrusion Detection Systems are categorized as Host based and Network based. The Host based IDS is used to detect attacks /intrusions into individual computer systems whereas Network based IDS is used to trace anomalies in complex and large networks.

Broadly there are four categories of cyber-attacks namely Probe, User to root, Denial of service and Remote to super user. Denial of Service attack when initiated from multiple systems in a distributed environment referred to as Distributed Denial of Service (DDoS) attack has become more popular in the recent past and is considered as the most popular and brutal attack type in real-time networks.

### B. Distributed Denial of Service Attack(DDoS)

The DDoS attacks mainly focus on the internet or cyber resources provided by the network service providers and its purpose is to disrupt normal operation of the server. The DDoS attacker, through multiple channels, overwhelms the target system by sending a constant flow of fraudulent requests causing severe disruption / delay in providing services to the legitimate users. An example for DDoS attack is BOTNET which is an army of hundreds or thousands of infected computers scattered all over the world to do a DDoS attack.

The main problems identified in the existing attack detection methods for dealing with real time systems:

1. Signature based attack detection is not effective since the network traffic dynamics change from time to time.
2. The algorithms such as D-FACE etc., are unable to predict DDoS attack if the input stream possess more number of features.
3. Traditional anomaly based machine learning models have high false positive rate along with high mean-squared error rate while handling real time traffic flow.

# Detection of Financial Fraud using Codetect Framework

P.Eswaraiah, Priyanka

*Abstract – Financial Fraud, for example, tax evasion, is known to be a genuine procedure of wrongdoing that makes misguidedly got assets go to psychological warfare or other crime. This sort of criminal operations include complex systems of exchange and money related exchanges, which make it hard to recognize the extortion elements and find the highlights of fraud. Luckily, exchanging/exchange system and highlights of elements in the system can be developed from the mind boggling systems of exchange and money related exchanges. Exchanging/exchange system uncovers the association among substances and consequently irregularity discovery on exchanging systems can uncover the elements engaged with the misrepresentation movement; while highlights of elements are the depiction of elements and abnormality identification on highlights can reflect subtleties of the extortion exercises. In this manner, system and highlights give integral data to extortion discovery, which can possibly improve fraud recognition execution. Nonetheless, most of existing strategies center on systems or highlights data independently, which doesn't use both data. In this paper, we propose a novel fraud identification framework, CoDetect, which can use both system data and highlight data for money related extortion discovery. What's more, CoDetect can all the while identifying money related fraud exercises and the component examples related with the extortion exercises. General examinations on both real world information and certifiable information exhibit the productivity and the adequacy of the proposed structure in battling monetary extortion, particularly for tax evasion.*

**Keywords –** Financial Fraud, Anomaly Detection, Credit card fraud.

## I. INTRODUCTION

Recently, financial fraud exercises, for example, Credit-card fraud, illegal tax avoidance, heightens continuously. These exercises cause the loss of individual as well as undertakings' properties. Even worse, they imperil the security of country since that the benefit from fraud may go to terrorism [1]. Along these lines, precisely detecting financial fraud and tracing fraud are essential. Be that as it may, financial fraud detection isn't a simple errand because of the mind boggling trading systems and exchanges included. Taking money-laundering for instance, tax evasion is characterized as the way toward utilizing exchanges to move cash/merchandise with the purpose of clouding the source of assets. More often, the costs, amount or nature of merchandise on a receipt of money-laundering are phony. The deception of costs, amount or nature of products on a receipt simply unveils slight contrast from normal premise on the off chance that we utilize these numbers as highlights to create detection approach. In specific situations, this sort of locator may function admirably with moderately stable exchanging substances.

Revised Manuscript Received on November 05, 2019.

P.Eswaraiah, Associate Professor, Dept. of CSE, PBR VITS, Kavali, AP, India.

Priyanka, M.Tech, Dept. of CSE, PBR VITS, Kavali, AP, India

Sadly, this circumstance is increasingly entangled, particularly inside Free Trade Zones (FTZs) where global exchange includes complex systems and trade of data between exchanging substances. The fraud exercises, particular illegal tax avoidance, are more profound stealth. Illegal tax avoidance exercises may take various structures [1], for example, the disguising transportation of money utilizing exchanging tasks; the procurement and clearance of intangibles; and related gathering exchanges. Not just the exchanging of merchandise appears on considerably more diversified, yet in addition several kinds of organizations, shell and front organizations include in to encourage illegal tax avoidance. Conversely with other fraud exercises, illegal tax avoidance exhibits extraordinary trademark which introduces high hazard to monetary framework with conceals the cash trail, collectivization conduct and wild exchanging areas FTZs.

Numerous fraud detection models perform with quality worth information-points that are produced from transactions-information. Some collection techniques are likewise exploited to advance the data. Subsequently, producing highlight from exchanges, managed and unaided techniques can be utilized to accomplish detection. More often, these information points are thought to be free and indistinguishably disseminated (i.i.d.). Be that as it may, the normal for tax evasion is unique in relation to attribute-values. The collectivization conduct implies the information is characteristically connected or mostly connected. Clearly, exchanging action includes in any event two business substances. Connected information is obviously not free and indistinguishably distributed, which negates the suppositions of conventional regulated and unaided strategies. On the opposite side, some connected information is auto corresponded. Graph based mining strategies are one of the most significant speculations that endeavour to recognize relations between information focuses [3][7][13], as Fig. 1(a) disclose. Financial exercises can be demonstrated as a directed-graph, at that point a sparse adjacent matrix can accompanies this chart. With graph-mining technique, the sparse-matrix can be approximated as summation of low-rank lattice and outlier -matrix. The outlier lattice is an indication of suspicious fraud exercises. Misusing the chart based mining gives another point of view to fraud-detection and empowers us to do enhanced research on fraud identification. With the fraud exercises detected by graph based recognition method we can reach the inference that a few business elements associated with fraud, in any case, despite everything we don't have the idea how these fraud-activities are worked and why these exercises marked as fraud, i.e., the certain highlights of the fraud exercises.

# SECURE AND LIGHTWEIGHT ACCESS CONTROL FOR PERSONAL HEALTH INFORMATION IN CLOUD BASED IOT DEVICES

B. MURALI KRISHNA<sup>1</sup>, K. SWARNA LATHA<sup>2</sup>

<sup>1</sup>Asst. Professor, Dept. of CSE, PBR VITS, Kavali, A.P, India

<sup>2</sup>M.Tech, Dept. of CSE, PBR VITS, Kavali, A.P, India

**Abstract** – The eHealth trend has spread globally. Internet of Thing s (IoT) devices for medical service and pervasive Personal Health Information (PHI) system s play important roles in the eHealth environment. A cloud based PHI system appears promising but raises privacy and information security concerns. We propose a cloud based fine grained health information access control framework for lightweight IoT devices with data dynamics auditing and attribute revocation functions. Only symmetric cryptography is required for IoT devices, such as wireless body sensors. A variant of ciphertext policy attribute based encryption, dual encryption and Merkle hash tree s are used to support fine grained access control, efficient dynamic data auditing, batch auditing and attribute revocation. Moreover, the proposed scheme also defines and handles the cloud reciprocity problem wherein cloud service provider s can help each other avoid fine s resulting from data loss. Security analysis and performance comparisons show that the proposed scheme is an excellent candidate for a cloud based PHI system.

**Keywords** – Personal Health Information, Cloud computing, Access control scheme.

## I. INTRODUCTION

Internets of Thing s (IoT) devices for medical services are an emerging technology for caring for disabled or chronic patients. Combined with wearable medical sensor s and wireless communication, IoT devices can gather patient's health related parameters remotely and continuously. As a result, the electronic Health (eHealth) care business is emerging. The eHealth vision is to utilize state of the art medical technologies to prolong life expectancy significantly. Imagine physicians being able to access a tourist's Personal Health Information (PHI) regarding food allergy history from a medical record for a rapid diagnosis. A patient with chronic heart disease uses body sensors to detect irregular blood pressure and rushes to the hospital in time to survive. In these scenario s, the patient's medical record plays a key role in diagnosis therefore pervasive PHI service is essential for doctors and nurses to offer real time treatment.

One solution for an effective PHI system is to adopt cloud based storage to mitigate the burden of building and maintenance cost. However, outsourced PHI faces the challenge of security and privacy issues, for instance, how to ensure that only the authorized requester can access the sensitive PHI or to prevent a

semi trusted Cloud Service Provider (CSP) from leaking stored information. In addition, the Health Insurance Portability and Accountability Act (HIPAA) comprise a list of privacy requirements for protecting confidentiality from the data storage server. Data integrity at a semi trusted CSP is another important concern. CSP s facing occasional catastrophic failures might decide to hide data errors from a patient for their own benefit. Although the data owner backs up his or her extremely important data in multiple CSPs, some CSPs might exercise mutual aid to avoid the huge cost of data loss. We call this the cloud reciprocity problem. The fact that a stored PHI would not only be accessed by medical workers but also updated by the patient requires support for data integrity verification for dynamic data operations.

One promising approach to solving such problems is to encrypt data in advance, prior to uploading to the cloud server. However, most existing PHI systems are not suitable for lightweight IoT devices because of the heavy cost of cryptographic computation. Furthermore, no scheme has dealt with the cloud reciprocity issue.

We propose a fine grained health information access control framework in the cloud for lightweight IoT devices with data dynamics auditing and attribute revocation functions. Regarding security and privacy, we use Ciphertext Policy Attribute Based Encryption (CP ABE) to perform fine grained access control on the part of a decryption key that is used to decrypt sensitive patient PHI. Basically, each Data Access Requester (has his/her own private keys associated with a set of attributes, and an essential decryption parameter TSK specifies an access policy over a defined universe of attributes. DAR can extract TSK to decrypt the encrypted PHI if and only if his/her attributes satisfy the access policy.

The main contribution s of this paper is as follows. (1) To the best of our knowledge, this is the first work suitable for lightweight IoT devices in PHI system s to achieve fine grained access control, dynamic data auditing, and user revocation simultaneously. (2) We first define and handle the problem of cloud reciprocity. (3) We propose a novel variant of proxy encryption to eliminate the involvement of HSP while DAR is accessing encrypted PHIs from a CSP and adapt the notion of CP ABE, MHT s, and dual encryption to offer the dynamic data operations, auditing, and user revocation functions. (4) Our

# IMPLEMENTATION OF PRIVACY PROTECTION ACCESS CONTROL AND KEYWORD SEARCH SCHEME FOR CLOUD STORAGE SYSTEMS

J. VAMSINATH<sup>1</sup>, B. TEJASWINI<sup>2</sup>

<sup>1</sup>Assoc. Professor, Dept. of CSE, PBR VITS, Kavali, A.P, India

<sup>2</sup>M.Tech, Dept. of CSE, PBR VITS, Kavali, A.P, India

**Abstract** – Secure search over encrypted remote data is crucial in cloud computing to guarantee the data privacy and usability. To prevent unauthorized data usage, fine-grained access control is necessary in multi-user system. However, authorized user may intentionally leak the secret key for financial benefit. Thus, tracing and revoking the malicious user who abuses secret key needs to be solved imminently. In this paper, we propose a Privacy Protection Access Control and Keyword Search Scheme (PP-ACKS). The key escrow free mechanism could effectively prevent the key generation centre (KGC) from unscrupulously searching and decrypting all encrypted files of users. Also, the decryption process only requires ultra lightweight computation, which is a desirable feature for energy-limited devices. In addition, efficient user revocation is enabled after the malicious user is figured out. Moreover, the proposed system is able to support flexible number of attributes rather than polynomial bounded. Flexible multiple keyword subset search pattern is realized, and the change of the query keywords order does not affect the search result. Security analysis indicates that PP-ACKS is provably secure. Efficiency analysis and experimental results show that PP-ACKS improves the efficiency and greatly reduces the computation overhead of users' terminals.

**Keywords** – Privacy protection, Access Control, Cloud Computing, Key Generation.

## I. INTRODUCTION

With the development of new computing paradigm, cloud computing [1] becomes the most notable one, which provides convenient, on-demand services from a shared pool of configurable computing resources. Therefore, an increasing number of companies and individuals prefer to outsource their data storage to cloud server. Despite the tremendous economic and technical advantages, unpredictable security and privacy concerns [2], [3] become the most prominent problem that hinders the widespread adoption of data storage in public cloud infrastructure.

Encryption is a fundamental method to protect data privacy in remote storage [4]. However, how to effectively execute keyword search for plaintext becomes difficult for encrypted data due to the unreadability of ciphertext. Searchable encryption provides mechanism to enable keyword search over encrypted data [5], [6].

For the file sharing system, such as multi-owner multiuser scenario, fine-grained search authorization is a desirable function for the data owners to share their private data with other authorized user. However, most of the available systems [7], [8] require the user to perform a large amount of

# Elliptic Curve Digital Signature Algorithm for the Third Party Auditing

Srinivasulu Pathakamuri, B.V. Ramana Reddy, A.P. Siva Kumar

**Abstract:** Cloud computing usage has been highly increased in past decades, and this has many features to effectively store, organize and process the data. The major concern in the cloud is that security is low and user requires verification process for the data integrity. Third Party Auditing (TPA) technique is applied to verify the integrity of data and various methods have been proposed in TPA for effective performance. The existing methods in TPA has the lower performance in communication overhead and execution time. In this research, Elliptic Curve Digital Signature (ECDS) is proposed to increase the efficiency of the TPA. Bilinear mapping technique is used for verification process without retrieving the data and this helps to reduce the communication overhead. The performance of ECDS is measured and compared with the existing method to analyze the performance.

**Index Terms:** Bilinear mapping, Cloud computing, Communication overhead, Elliptic Curve Digital Signature and Third Party Auditing.

## I. INTRODUCTION

Cloud computing has provided a way to store large data and due to its advantages like flexibility, scalability and reliability, cloud computing attracts many users. Cloud computing incur some security issues such as data integrity, data encryption etc. Cloud auditing is the technique to verify the integrity of data [1]. Cryptographic keys are generated for cloud data, which are required to be stored and protected. The key storage facility compromise may also lead to data loss. The cryptographic key is required to be stored with security and single point of failure should affect the data availability [2]. Despite the powerful machine and strong security mechanism provided by the Cloud Service Providers (CSP), remote data still faces security issues due to hardware and administration errors [3]. Cloud auditing is used to verify data integrity in the cloud. To reduce the burden for the client and make more convenient, Third-Party Auditing (TPA) was introduced [4]. The owner can modify, delete the existing block by using dynamic support and also owner can insert a new block. This is important step in the cloud storage and many applications were not limited to store the data in cloud [5].

Generally, cloud denotes a public cloud, users were not

**Revised Manuscript Received on December 08, 2019**

Corresponding Author\*

**Srinivasulu Pathakamuri\***, Department of CSE, JNT University, Anantapur, India.

**Dr. B.V. Ramana Reddy**, Department of CSE, KSRM College of Engineering, Kadapa, India.

**Dr. A.P. Siva Kumar**, Department of CSE, JNT University, Anantapur, India.

limited on access of the data in the cloud. Several users and devices can access the cloud and this should have access control mechanism [6]. Authenticators security is protected by using the Binary tree structure before the key exposure [7]. Traditional integrity verification method is very limited in the computation and communication abilities and doesn't satisfy the required applications [8]. To effectively process cloud auditing for the large amount of data with limited computation time, an efficient method is needed [9 - 10]. In this research, ECDSA method is used to increase the performance of the TPA for cloud auditing. The proposed ECDSA method has advantages of a lower key size and suitable for a constrained environment like TPA. The lower key size helps to minimize the computation overhead and computation time of the integrity check. Bilinear mapping technique is used to verify the data without need of the original data from the cloud.

The organization of the paper is given as, the literature works of existing TPA method is detailed in section 2, proposed ECDSA method is detailed in section 3, experimental result is discussed in section 4 and conclusion is provided in section 5.

## II. LITERATURE WORKS

Cloud computing is highly used to run the application and store data due to its flexibility, scalability and reliability. One major concern in the cloud computing is that security and user require the proof for the integrity of data. Many research studies have been conducted in the TPA to check the data integrity. Recent research involved in the TPA in cloud storage is studied in this section.

Suguna and Shalinie, [11] proposed a technique for the generation of verification proof is called as a small signature that minimizes the client side auditing overhead. Bilinear mapping is applied to verify without retrieving the original data, is called as a blockless process. Merkel Hash Tree (MHT) is applied in the authentication process to increase security. The developed method has a higher performance for the verification process in the manner of storage and communication overhead. The de-duplication technique is used to increase the efficiency of the developed method.

Guo, et al. [12] proposed key generation authentication cryptosystem that creates a constant size key for the shared encrypted data in cloud computing. The authentication process is used to solve the key leakage problem. The cloud server uses the public key to identify the data owner to provide access.



# Secure and Fast Biometric Verification Scheme for Cloud Storage Systems

D.Srinivasula Reddy, M. Anuradha

*Abstract – Biometric verification of has turned out to be progressively well known as of late. With the improvement of cloud computing, database owners are enthused to outsource the enormous size of biometric information and verification activity to the cloud to dispose of the costly capacity and calculation costs, which anyway carries potential dangers to clients' security. This article presents an proficient and protection saving biometric verification outsourcing plan. In particular, the biometric information is encoded and redistributed to the cloud server. To execute a biometric verification, the database owner encodes the query information and submits it to the cloud. The cloud performs verification tasks over the encoded database and returns the outcome to the database owner. A careful security examination shows the proposed plan is secure regardless of whether aggressors can produce verification demands and intrigue with the cloud. Contrasted and past conventions, trial results demonstrate the proposed plan accomplishes a better presentation in both preparation and verification systems.*

**Keywords** – biometric identification, privacy preserving, cloud computing.

## I. INTRODUCTION

Biometric verification has raised progressively consideration since it gives a promising method to recognize clients. Contrasted and customary verification strategies dependent on passwords and recognizable proof cards, biometric verification is viewed as progressively solid and helpful [1]. Moreover, fingerprint verification has been generally applied in numerous fields by utilizing biometric characteristics, for example, unique finger impression [2], iris [3], and facial examples [4], which can be gathered from different sensors [5]–[9].

In a biometric verification framework, the database proprietor, for example, the FBI who is dependable to deal with the national fingerprints database may want to redistribute the huge biometric information to the cloud server (e.g., Amazon) to dispose of the costly capacity and calculation costs. Be that as it may, to save the security of biometric information, the biometric information must be scrambled before redistributing. At whatever point a FBI's accomplice (e.g., the police headquarters) needs to validate a person's character, he goes to the FBI and creates a verification question by utilizing the person's biometric characteristics. At that point, the FBI encodes the question and submits it to the cloud to locate the nearby coordinate. In this way, the difficult issue is the manner by which to structure a convention which empowers productive and protection saving biometric verification in the distributed computing.

Various securities based biometric verification arrangements [10] have been proposed. Be that as it may, the vast majority of them essentially focus on protection conservation yet overlook the proficiency, for example, the plans dependent on similar encoding plus neglectful exchange prospering [10] since unique mark plus image recognizable proof individually. Experiencing execution issues of neighborhood devices, these plans are not productive once the size of the database is bigger than 10 MB. Afterward, Evans et al. introduced a biometric verification plan by using circuit structure and ciphertext packing procedures to accomplish productive verification for a bigger database of up to 1GB. Also, Yuan and Yu proposed a proficient protection preserving biometric verification plan. In particular, they built three modules and structured solid rules to accomplish the security of unique finger impression quality. To improve the effectiveness, in their plan, the database proprietor re-appropriates verification task into the cloud. Nonetheless, zhu et al. referred to that other authors convention might be unsmooth by an agreement assault propelled by a pernicious client, cloud. wang et al. proposed the plan CloudBI-II which utilized irregular inclining networks to acknowledge biometric ID.

In this article, we suggest a good and privacy-preserving fingerprint verification agenda which is able to oppose conspiracy violation driven by clients along with the cloud. in particular, our fundamental commitments are often condensed as pursues:

- Our own selves examine the fingerprint verification plan plus demonstrate its inadequacies plus safety shortcoming under the suggested level-3 violation. in particular, our own selves show that intruder will recoup their mystery formulas via plotting with cloud, in addition to that decode the fingerprint all things considered.
- We tend to propose a unique productive plus protection saving fingerprint verification plan. The whole safety examination demonstrates so the suggested plan can accomplish a necessary degree of protective cover assurance. In particular, in our own plan is safe under the fingerprint verification re-appropriating type plus can likewise oppose intrusion planned.
- Resemble the present fingerprint verification plans, exhibition investigation demonstrates so the proposed plan gives a less significant computational expense in both planning and recognizable proof strategies.

## II. BACKGROUND WORK

Related works away at protection preserving biometric verification are given in this area. As of late, some productive biometric recognizable proof plans have been recommended. wang

Revised Manuscript Received on December 05, 2019.

\* Correspondence Author

D.Srinivasula Reddy, Associate Professor, Dept. of CSE, PBR VITS, Kavali, AP, India.

M. Anuradha, M.Tech, Dept. of CSE, PBR VITS, Kavali, AP, India

# An Efficient Fine Grained Keyword Based Search Scheme in Fog Computing

PVN Rajeswari, Chadalawada Lakshmi Janaki

**Abstract—**In fog computing outsources the encoded information to many mist hubs on the border of the internet of things (IOT) to reduce delay and network congestion. However, the existing cipher text recovery plan infrequently focus on the fog computing area and most of them still enforce high computational and capacity burden on asset constrained clients. In this writing paper, we tend to better recommended a lightweight small-grained cipher texts search (LFGS) framework in fog calculation by extending cipher text-policy attribute-based encryption (CP-ABE) and searchable encryption (SE) technologies, which can accomplish small-grained fingerprint plus key-word search concurrently. The LFGS can transfer semi calculation and storage burden from clients to picked fog nodes. Furthermore, the fundamental LFGS framework is enhanced to cope with conjunctive keyword search and attribute revise to keep away from returning unrelated search outcomes and unauthorized accesses.

**keyword –**internet of things, fog Calculating, cloud computing.

## I. INTRODUCTION

The promising distributed computation [1] worldview can furnish on-request benefits with flexible assets and empower cloud customers to mitigate the high stockpiling and calculation costs [2] locally. Be that as it may, the commonness of Internet of Things (IOT) applications [3] represents an enormous test to the incorporated distributed computing worldview which brings about insufferable transmission inactivity and corrupted administrations between client demands and cloud responses. Plus, a lot of information created from the IoT applications is frequently put away in the cloud. To reduce delay and system congest, a mist registering worldview [4] which is associate augmentation of distributed computing administrations to network edge has been a generally late inquire about theme. In mist figuring, the haze hubs embedded into the center of cloud and end clients can give different administrations for asset restricted end clients, note that fog nodes are a lot nearer up to end clients compared to thundercloud, and that is appeared in Fig. 1. At the point when delicate information [5], [6], [7] are re-appropriated to fair however inquisitive haze hubs which are like open cloud stage, the information security and protection concerns [8] still block the reception of mist registering as information proprietors put the overall material command over their information in face combinationsorthundercloud.

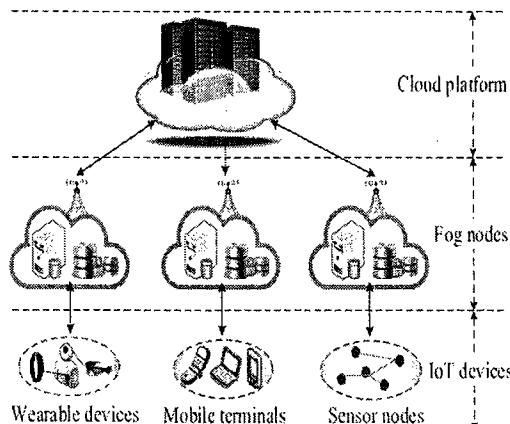


Fig. 1: The infrastructure of fog computing.

To alleviate the information security spillage dangers, information encryption is an effective instrument to ensure information secrecy, yet it makes the data recovery over encoded information incredibly difficult. Also, the encoded information ought to be manageable to access control. case in point, identity-based encryption (IBE) and attribute-based encryption (ABE) can ensure information department via big grainy and fine-grainedfingerprint devices, individually. notwithstanding information section concerns, accomplishing compelling positive identification hunt more than scrambled data 1 also, small-grained fingerprint are likewise the overall indispensable illuminates in real situations. Searchable encryption (SE) innovation which empowers information clients to safely look and specifically recover documents of enthusiasm over encoded information as indicated by client determined key terms may have been broadly investigated. with outfit small-grained fingerprint in very sometime se arrangements, the talented cipher text-policy attribute-based keyword search may have increased much advisement almost all mechanical plus scholarly fields. in plans, a particular end client closet unpicks figure writings going from intrigue if and just if his characteristic set up joins sensational entrance arrangement implanted toward cipher texts plus his analysed side door fits the lists all the while.

Despite the fact that CP-ABKS is a most valuable cryptologic instrument to accomplish each small-grained get entry to control and watchword look interfaces, the overall machine and capacity charges of existing CP-ABKS plans are roughly corresponding to the multifaceted nature going from entryway approach, which very much impede the professional jobs of asset constrained IOT devices. Henceforth, it is basic so keep actionsboth end clientscipher practical.

Revised Manuscript Received on January 15, 2020

PVN Rajeswari, Associate Professor, Dept. of CSE, PBR VITS, Kavali, AP, India.

Chadalawada Lakshmi Janaki, M. Tech, Dept. of CSE, PBR VITS, Kavali, AP, India.

# A Hybrid Secure Storage Scheme to Avoid EDoS Attacks in Cloud Computing

PVN Rajeswari, Golla Vihalya

**Abstract:** In advent of cloud environment, cloud operator is not a completely trusted to put on private information, because of lack of consumer to cloud control. To assurance privacy, documents sharer deploy their encipher documents. Encipher documents dispense to among consumers using CP-ABE scheme. But it is not completely safe in opposition to different assaults. The prior knowledge cannot offer any verification ability to cloud operator whether the user can decipher or not. Various invaders may obtain lot of document by initiate EDoS assaults. The consumer of cloud abides cost. To handle above issues, this article suggests a problem solving plan to safe encipher cloud repository from EDoS assaults and maintain supply utilization. It utilizes CP-ABE tactics in a black-box method furthermore accomplish impulsive entryway contract epithetical CP-ABE. We tend to present 2 mechanisms for various styles, observed via achievement and shield research.

**Keyword:** Access control, Privacy safe, Cloud computing.

## I. INTRODUCTION

Cloud repository has various points of interest, for instance, constantly on the web, a system of meeting cost, and inexpensive [1]. During such senility, more data are reappropriated as far as unseal cloud as enterprise stockpiling, in addition to someone plus occupation reports. Something that leaves a safety issue so document sharer [2]–[4]: unseal cloud isn't creditworthy, plus decentralized tidings shouldn't be lost so cloud provider externally approval relishes intelligence sharer. Numerous capacity systems employ server-governed grante command, take pleasure in undercover phrase founded [5] plus certificate-based-confirmation [6]. They unreasonably believe cloud-provider to substantiate their encrypted. Providers as well as their laborers can examine any record independent of information owners' entrance approach. likewise, the thundercloud provider will distort quality use of report stockpiling plus indictment tax dodgers exhausted bighearted correct archives [2], [7], since we don't have a system for evident calculation assets use. The common server overwhelmed get to control isn't verified. information sharers that one depot records toward cloud-systems yet have to command approval exclusively as well as stay the info made sure toward thundercloud provider and pernicious customers. Encoding isn't decent. up to incorporate the protection affirmation, data proprietors can encode the records plus fix an entrance strategy in order that moderated customers will translate chronicle. In

addition to ciphertext-policy attribute-based cryptography, we tend to will submit to each small-grained grante command and powerful story. Consequently, this entrance control is accessible for information vendors, which is being insufficient. On the fluke that the cloud-provider will not approve customers before booting, from quite a lot of winning CP-ABE distributed storage structures, cloud has got to empower everyone to obtain to ensure openness. That empowers capacity structure powerless across the advantage fatigue blasts. If we settle this issue by having information owners approve the overall sharers in advance inspiring authority so transfer, we tend to misplace the flexibility of fingerprint relishes CP-ABE. Hither record the 2 issues ought to be tended in our own work:

**Problem I:** asset depletion ambush. Whether cloud doesn't perform cloud-side fingerprint, it allows somebody, including pernicious assailants, to transparently download, however just hardly any customers are capable disentangle. The server tends against asset fatigue ambushes. Exactly when noxious customers dispatch the DoS/DDoS ambushes to suffused repositing, the advantage usage will augment. Evaders need in order to pay money for the extended usage amounted instead by attacks, which explains a great plus irrational cash related load. The ambush outmoded introduced given that economic denial of sustainability (EDoS), that alludes to evaders are financially abused over long haul. Moreover, archives are encoded; pirated files will abate scrip via conveying convenience in order to disengaged instigating plus spilled information get pleasure from report wingspread or revise-recurrence.

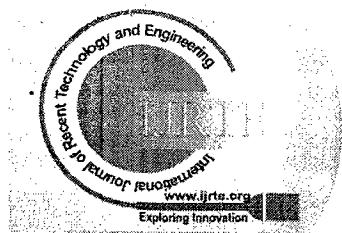
**Problem II:** asset utilization responsibility. in compensation as-you-go plan, customers underpay bread to with the thundercloud supplier for capacity administrations. the cost is chosen through resource use. Along these lines, a CP-ABE based design for distributed storage get to control doesn't bring online insistences to the information slaveholder previous records. it really is asked any cloud specializer organization to exhibit the avoiders just about the certifiableutilization. Else, the overall thundercloud supplier can ready to charge enormous without being found. The following article, we assemble the general cloud-side fingerprint and the present information proprietor slope cpabe supported exercise control, to determine the recently referenced binaries in protection saving distributed warehousing. In our own procedure will turn away the EDoS ambushes via empowering the thundercloud system to check whether customer is affirmed in CP-ABE based arrangement, without discharging different news.

As in our own cloud-side fingerprint, without help use CP-ABE encryption/decoding video game for challenge-response.

Revised Manuscript Received on January 15, 2020.

PVN Rajeswari,<sup>1</sup> Assoc. Professor, Dept. of CSE, PBR VITS, Kavali A.P, India

Golla Vihalya, M.Tech, Dept. of CSE, PBR VITS, Kavali, A.P, India



# International Journal of Recent Technology and Engineering

ISSN: 2277-3878 (Online) • Exploring Innovation • A Key for Dedicated Services  
Published by Blue Eyes Intelligence Engineering & Sciences Publication  
P# G:18-19-20, Block-B, Tirupati Abhimav Homes, Damkheda, Bhopal (Madhya Pradesh)-462037, India  
Website: [www.ijrte.org](http://www.ijrte.org) Email: [submit2@ijrte.org](mailto:submit2@ijrte.org)

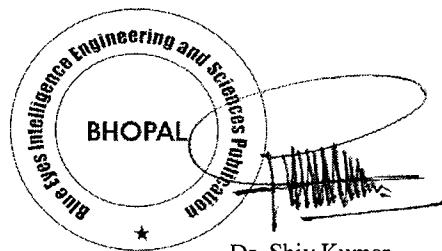
+91-9109122902 | +91-9109122902 | +91-9109122902

## CERTIFICATE

This certifies that the research paper entitled '**Replica Node: Detection of Node Replication in Multidimensional Networks**' authored by '**V. V. Sunil Kumar, B. Chandrasena**' was reviewed by experts in this research area and accepted by the board of 'Blue Eyes Intelligence Engineering and Sciences Publication' which has published in '**International Journal of Recent Technology and Engineering (IJRTE)**', ISSN: 2277-3878 (Online), Volume-8 Issue-5, January 2020. Page No. 2005-2008.

The B Impact Factor of IJRTE is 5.92 for the year 2018. Your published paper and Souvenir are available at: <https://www.ijrte.org/download/volume-8-issue-5/>

Jitendra Kumar Sen  
(Manager)



Dr. Shiv Kumar  
(CEO)



# **RAN METHOD THAT PERFORMS NESTED SCALABLE NO SQL TRANSACTION AND DATA ANALYTICS**

**D.S.C. Reddy**

Professor & HOD, Dept. of CSE,  
PBR Visvodaya Institute of Technology and Science, AP, India.

**Kanamathareddy Reshma Reddy**

M.Tech, Dept. of CSE,  
PBR Visvodaya Institute of Technology and Science, AP, India.

## **ABSTRACT**

*Last decade records a large quantity of data transition occurring web. Today's world is connected by Social Networking sites that have immense size of databases. Currently, there's no utility existing for remodeling SQL databases into NoSQL databases. NoSQL could be a new trend; there's no software system or utilities that are designed for the specified conversion. Most of the utilities developed, were developed for changing one variety of SQL database to a different SQL database. To market Hybrid database design together with an electronic information service and NoSQL database, an information Adapter system is planned. It will affect database transformations employing a database synchronization mechanism. It focuses on sanctioning effective database Analytics on Scaled-out Object Storage Systems. There's implementation of a database. Analytics Layer on associate degree Object-based Storage Cluster to perform in-place Map-Reduce computation on existing data. It keeps the strengths of RDBMS as ACID properties and at an equivalent time by providing the advantages of NoSQL through a middle layer that keeps track of all running transactions and manages with alternative layers with co-occurring transactions. the info Adapter uses a SQL layer acceptive queries from application services, in order that original application remains intact. The info Adapter conjointly controls question flow throughout information transformations. Associate degree approach that performs computation on existing large-scale information in associate degree Object Storage system while not moving information anyplace and outcomes of this approach are analyzed. This define will deliver strict consistency while not poignant measurability and handiness of NoSQL Databases.*

**Keywords:** SQL; NoSQL; data adapter; migration; dataanalytics; SVM

**Cite this Article:** D.S.C. Reddy, Kanamathareddy Reshma Reddy, RAN Method that Performs Nested Scalable no SQL Transaction and Data Analytics, *International Journal of Advanced Research in Engineering and Technology (IJARET)*, 11 (1), 2020, pp 30-37.  
<http://www.iaeme.com/IJARET/issues.asp?JType=IJARET&VType=11&IType=1>

---

## A NO SQL DATABASE MODEL WITH NESTED TRANSACTIONS USING MULTI-TENTANT ARCHITECTURE

D.S.C. REDDY<sup>1</sup>, KANAMATHAREDDY RESHMA REDDY<sup>2</sup>

<sup>1</sup>Professor & HOD, Dept. of CSE, PBR Visvodaya Institute of Technology and Science, AP, India.

<sup>2</sup>M.Tech, Dept. of CSE, PBR Visvodaya Institute of Technology and Science, AP, India.

**Abstract** – As the world is frantically moving towards digitization, handling huge volumes of data is becoming complex and difficult to optimize. This is mainly because of increasing dimensions of data, its unstructuredness and increased need for storage space. To increase the efficiency of the cloud environment, many service providers have moved towards multitenant architecture. In a multi-tenant architecture, a number of individual applications termed as tenants work under a shared environment. In such a scenario, it is imperative that data of one tenant be isolated from that of other tenants. Further, it is also desirable to optimize the use of storage space. With these considerations, this paper proposes multi-tenant database architecture for applications using a column-based NoSQL data store. The architecture has been implemented with the NoSQL database, Cassandra.

**Keywords** – multitenant architecture, Cassandra, Queries Processing.

### I. INTRODUCTION

With overall increase in the measure of data rise, cost of planning the data relies already increased hugely. Considering this, many application services have affected or have strategic now been moving against distributed environment. In the several years the distribution of distributed computing and also the study of distributed systems have magnified gradually. It is also not possible to storage, compute the humungous data on a single machine; thereby leading to the need for distributed and cloud based answers for data storage.

Data being kept in distributed environment [1] or booming a stratus is of large rates and requires storage space to deal with it. It has been observed that triplex customers of cloud based applications, such as certain exploitation software as a service role model; share whatever park data. Storage of the data every application in very cloud ends in data that is typically redundant, because of multiple

## HANDLING GEO TAGGING DATA USING NO SQL DATABASES IN BIG DATA ERA

D.S.C. REDDY<sup>1</sup>, KANAMATHAREDDY RESHMA REDDY<sup>2</sup>

<sup>1</sup>Professor & HOD, Dept. of CSE, PBR Visvodaya Institute of Technology and Science, AP, India.

<sup>2</sup>M.Tech, Dept. of CSE, PBR Visvodaya Institute of Technology and Science, AP, India.

**Abstract** – In modern era usage of smart phones increased drastically and location based services has important role in evolving different people centric services for sustainable improvement of the society such as developing the smart cities, climatic change management services and finding fundamental needs of the people such as hospitals, banks, ATM's. People are generating geo tagged data on various social media websites like face book, twitter etc. which can be considered as big data due to acquiring major three attribute volume, variety and velocity of big data. Managing such a huge amount of data is really challenging. This geo-tagged data needs to be handled using big data management techniques like No SQL rather than traditional Relational Data Base Management System. Selection of appropriate type of No SQL Database is an important activity before developing any Geographical Information System based application. In this paper we tried to find out suitable No SQL data base for GIS application. This paper compares the performance of MongoDB and Neo4j in case of search queries executed on geo-tagged data.

**Keywords** – Geo-tagging, No SQL Database, Neo4j, PostGre SQL.

### I. INTRODUCTION

Geo-tagging, as the name suggests stands for geographical tagging of location or a place. Geotagging is an activity of adding metadata to any form of information, be it a text message, an image or a video. It helps us to visualize the message and understand it in a better way. Latitude and longitude are the two main driving forces of geotagging. Other geo-coordinates may include bearing, place names,

altitudes distance or even a timestamp. This data is mainly generated via crowdsourcing hence there is no control on the data. Such data is heterogenous and large to manage using traditional Relational Data Base Management System. Geo-tagged data plays significant role in developing various citizen centric applications like urban planning, public health, smart city applications, disaster management etc. Hence it is important to

# Cognitive IoT: An Eco friendly Technology

M. Padma, Assistant Professor, CSE Dept., G Pulla Reddy Engineering College, Kurnool, Andhra Pradesh, India.  
padma.gprec@gmail.com

Dr. N. Kasiviswanath, Professor & HOD, CSE Dept., G Pulla Reddy Engineering College, Kurnool, Andhra Pradesh,  
India.hodcse@gprec.ac.in

T. Manjula, Associate Professor,PBR VITS, Kavali,AndhraPradesh,India t\_manjula\_k@yahoo.co.in)

**Article Info****Volume 82****Page Number: 8724 - 8727****Publication Issue:****January-February 2020****Article History****Article Received: 5 April 2019****Revised: 18 Jun 2019****Accepted: 24 October 2019****Publication: 08 February 2020****Abstract:**

Cognitive Technology is a new technology that resulted as an evolution of Internet of things. Internet of things has been already influenced the everyday life of human beings in terms of smart phones, smart watches, smart TVs, Security alert devices. Different sensors used in these devices, use the wireless communication media, some of which are harmful to human life. Artificial Intelligence has brought dramatic changes in the field of Internet of things in terms of automation. Cognitive computation now induces the cognitive capabilities in the field of Internet of Things for better decision making in complex environments. This paper focuses on how the cognitive capabilities are helpful for Internet of things, The resulting technology so called as Cognitive IOT has lead to an eco friendly technology. Thus the major goal of sustainability achieved by the cognitive IOT.

**Keywords:** Cognitive IOT, Internet of Things, Cognitive Computation

## I. INTRODUCTION

The field of computer science has seen so many technological changes over the past decades. Among that the major ones are artificial Intelligence and machine learning is the one that brought automation. Automation lead to the concept of smart devices, which resulted in Internet of things. Cognitive computation has boosted these technologies by helping in taking decisions in dynamic situations.

The use of various automation tools and smart devices has an adverse impact on the environment in terms of radiations. This also has destroyed many living things. Thus the focus is to use technologies that are not only useful but also help in preserving the ecosystem.

The use of cognitive technologies in Internet of thing has lead to a new branch of study known as Cognitive IoT. The focus of Cognitive IoT is to help the smart devices to behave in an eco friendly manner and thus support the concept of sustainability.

## II. WHAT IS IOT

IoT is the shorthand notation for Internet of Things. IoT is inter related collection of digital devices and various sensors that are capable of collecting and exchanging data. The IoT definition has evolved over decades by the invention of new technologies[1]. The major aim of IoT is to use smart devices. IoT has been used in variety of applications ranging from home appliances to large industrial environments[2].Because of its abilities to get the data concerning the physical world, the Internet of Things (IoT) phenomenon is quick picking up force in various handy spaces. Its benefits are not restricted to interfacing things, however incline toward how the gathered data are changed into experiences and interact with Domain Experts for better decision making.[3].

## III. COGNITIVE IOT

In 2002, DARPA characterized as a cognitive system one that can "reason, utilize represent knowledge, gain as a matter of fact, accumulate knowledge, account for itself, acknowledge direction, know about its very own behavior and

## A Review on IoT Devices

A.Prasmitha

*<sup>1</sup>Assistant Professor, CSE Department, PBR Visvodaya Institute of Technology &Science*

### **Abstract**

*In today's world, the Internet of Things plays an important role in human life. Now, most of the electronic devices have been connected with the internet, in fact, they are operated through the internet from anywhere in the world. The basic definition of IoT says that it is a network, which is has been interconnected via various sensors that are used to record the data and it is possible to control the devices. In today's electronic market we have a smart device that comes up with the most advanced sensors. This IoT is majorly used for commercial and industrial purposes. In this paper, some of the popular devices that are being used in IoT are discussed.*

**Key words:** IoT, smart, devices, security, communication.

### **1. Introduction:**

Internet of Things is a system of interconnected devices that capable of exchanging the data in major applications such as in home devices, medical, vehicles, smart cities, wearable fitness devices. Now this IoT has become a technology revolution. People are able to control their smart devices anywhere in the world. This is possible with the help of internet where the protocols are supporting for the control and monitoring of the devices [1-4].

The major features of this IoT are sensors, Artificial Intelligence, connectivity and other devices. Artificial intelligence makes the systems smart and takes its own decision with the help of neural network. It collects the data, processes it and makes the decision. Now most of the electronic gadgets come up with artificial intelligence. It has the power to process at a faster rate than the existing technologies. IoT has the capacity and the capability to work with even small types of networks for communication [2]. With the help of sophisticated sensor equipment, it is possible to integrate with the real world environment.

The advantages of IoT are, it reduces the human intervention, saves money, saves time, processing speed is more, accuracy is more, it supports for automation and control [3]. At the same types it has few drawbacks such as privacy issues, security concern and totally dependent on technology.

Rest of the paper is organized as section 2 covers about the architecture of IoT and section 3 covers about IoT devices used in real time applications, then section 4 covers conclusions.

## CRYPTOGRAPHICALLY ENFORCED DYNAMIC ACCESS CONTROL IN CLOUD COMPUTING

<sup>1</sup>MURALIKRISHNA B, <sup>2</sup>P. SUMASRI, <sup>3</sup>G.MOUNIKA, <sup>4</sup>I.V.S.L.PRASANTI,  
<sup>5</sup>B.VARALAKSHMI

<sup>1</sup>Asst. Professor, Dept. of CSE, PBR VITS, Kavali, A.P, India.

<sup>2, 3, 4, 5</sup>B.Tech, Dept. of CSE, PBR VITS, Kavali, A.P, India.

**Abstract –** Enabling cryptographically enforced access controls for data hosted in untrusted cloud is attractive for many users and organizations. However, designing efficient cryptographically enforced dynamic access control system in the cloud is still challenging. In this paper, we propose Cryptographically enforced access controls, a system that provides practical cryptographic enforcement of dynamic access control. Cryptographically enforced access controls revokes access permissions by delegating the cloud to update encrypted data. In Cryptographically enforced access controls, a file is encrypted by a symmetric key list which records a file key and a sequence of revocation keys. In each revocation, a dedicated administrator uploads a new revocation key to the cloud and requests it to encrypt the file with a new layer of encryption and update the encrypted key list accordingly. Cryptographically enforced access controls propose three key techniques to constrain the size of key list and encryption layers. As a result, Cryptographically enforced access controls enforces dynamic access control that provides efficiency, as it does not require expensive decryption/reencryption and uploading/re-uploading of large data at the administrator side, and security, as it immediately revokes access permissions.

**Index terms –** User Revocation, cloud computing, Access Control.

### I. INTRODUCTION

With the considerable advancements in cloud computing, users and organizations are finding it increasingly appealing to store and share data through cloud services. Cloud service providers (such as Amazon, Microsoft, Apple, etc.) provide abundant cloud based services, ranging from small-scale personal services to large-scale industrial services. However, recent data breaches, such as releases of private photos, have raised concerns regarding the privacy of cloud-

managed data. Actually, a cloud service provider is usually not secure due to design drawbacks of software and system vulnerability. As such, a critical issue is how to enforce data access control on the potentially untrusted cloud.

In response to these security issues, numerous works have been proposed to support access control on untrusted cloud services by leveraging cryptographic primitives. Advanced cryptographic primitives are applied for enforcing many access control paradigms. For example, attribute-based encryption (ABE) is a cryptographic counterpart of attribute-based access control (ABAC) model.

However, previous works mainly consider static scenarios in which access control policies rarely change. The previous works incur high overhead when access control policies need to be changed in practice. At a first glance, the revocation of a user's permission can be done by revoking his access to the keys with which the files are encrypted. This solution, however, is not secure as the user can keep a local copy of the keys before the revocation. To prevent such a problem, files have to be re-encrypted with new keys. This requires the file owner to download the file, re-encrypt the file, and upload it back for the cloud to update the previous encrypted file, incurring prohibitive communication overhead at the file owner side.

Currently, only a few works investigated the problem of dynamic data access control. Garrison et al. proposed two revocation schemes. The first scheme requires an administrator to re-encrypt file with new keys as discussed above. This scheme incurs a considerable communication overhead. Instead, the second scheme delegates users to re-encrypt the file when they need to modify the file, relieving the administrator from re-encrypting file data by itself. This scheme, however, comes with a security penalty as the revocation

# IMPLEMENTATION OF AN EFFICIENT DATA SHARING SCHEME FOR MOBILE CLOUD DATA

<sup>1</sup>MURALIKRISHNA B, <sup>2</sup>CH CHAITANYA

<sup>1</sup>Asst. Professor, Dept. of MCA, PBR VITS, Kavali, A.P, India.

<sup>2</sup>MCA, Dept. of MCA, PBR VITS, Kavali, A.P, India.

**Abstract** – With the popularity of cloud computing, mobile devices can store/retrieve personal data from anywhere at any time. Consequently, the data security problem in mobile cloud becomes more and more severe and prevents further development of mobile cloud. There are substantial studies that have been conducted to improve the cloud security. However, most of them are not applicable for mobile cloud since mobile devices only have limited computing resources and power. Solutions with low computational overhead are in great need for mobile cloud applications. In this paper, we propose a lightweight data sharing scheme (LDSS) for mobile cloud computing. It adopts CP-ABE, an access control technology used in normal cloud environment, but changes the structure of access control tree to make it suitable for mobile cloud environments. LDSS moves a large portion of the computational intensive access control tree transformation in CP-ABE from mobile devices to external proxy servers. Furthermore, to reduce the user revocation cost, it introduces attribute description fields to implement lazy-revocation, which is a thorny issue in program based CP-ABE systems.

**Index terms** – CP-ABE, Data Sharing, Cloud Computing.

## I. INTRODUCTION

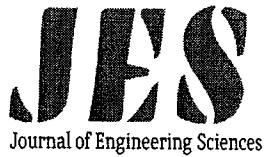
With the development of cloud computing and the popularity of smart mobile devices, people are gradually getting accustomed to a new era of data sharing model in which the data is stored on the cloud and the mobile devices are used to store/retrieve the data from the cloud. Typically, mobile devices only have limited storage space and computing power. On the contrary, the cloud has enormous amount of resources. In such a scenario, to achieve the satisfactory performance, it is essential to use the resources provided by the cloud service provider (CSP) to store and share the data.

Nowadays, various cloud mobile applications have been widely used. In these applications, people (data

owners) can upload their photos, videos, documents and other files to the cloud and share these data with other people (data users) they like to share. CSPs also provide data management functionality for data owners. Since personal data files are sensitive, data owners are allowed to choose whether to make their data files public or can only be shared with specific data users. Clearly, data privacy of the personal sensitive data is a big concern for many data owners.

The state-of-the-art privilege management/access control mechanisms provided by the CSP are either not sufficient or not very convenient. They cannot meet all the requirements of data owners. First, when people upload their data files onto the cloud, they are leaving the data in a place where is out of their control, and the CSP may spy on user data for its commercial interests and/or other reasons. Second, people have to send password to each data user if they only want to share the encrypted data with certain users, which is very cumbersome. To simplify the privilege management, the data owner can divide data users into different groups and send password to the groups which they want to share the data. However, this approach requires fine-grained access control. In both cases, password management is a big issue.

Apparently, to solve the above problems, personal sensitive data should be encrypted before uploaded onto the cloud so that the data is secure against the CSP. However, the data encryption brings new problems. How to provide efficient access control mechanism on ciphertext decryption so that only the authorized users can access the plaintext data is challenging. In addition, system must offer data owners effective user privilege management capability, so they can grant/revoke data access privileges easily on the data users. There have been substantial researches on the issue of data access control over ciphertext. In these researches, they have the following common assumptions. First, the CSP is considered honest and curious. Second, all the sensitive data are encrypted before uploaded to the Cloud. Third, user authorization on certain data is



Journal of Engineering Sciences

# JES Journal of Engineering Sciences

ISSN:0377-9254, Web:[www.jespublisher.com](http://www.jespublisher.com)

UGC CARE APPROVED GROUP 'II' JOURNAL

## CERTIFICATE OF PUBLICATION

This is to certify that the paper entitled

" CLOUD WIZARD "

Authored by

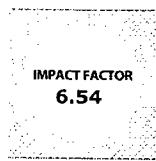
MURALIKRISHNA B, Asst. Professor

From

PBR VITS, Kavali, A.P, India

Has been published in

JES JOURNAL, VOLUME XI, ISSUE VII, JULY - 2020

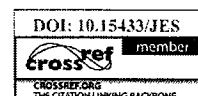


Dr. D.K. Umber

Editors-in-Chief

Dr. D. Karthikaran Umber

JES PUBLICATION



## Cognitive Computing For Sustainable Agriculture

T. Manjula<sup>1</sup> and T. Sudha<sup>2</sup>

<sup>1</sup>Research Scholar, <sup>2</sup>Professor, <sup>1&2</sup>Department of Computer Science and Engineering,  
Sri Padmavati Mahila Visva Vidyalayam, Andhra Pradesh, India  
E-Mail: t\_manjula\_k@yahoo.co.in, thatimakula\_sudha@yahoo.com

**Abstract -** Cognitive computing in agriculture is going to be a big revolution like the green revolution. Agriculture is a big step that accompanied the humanity to evolve from the ancient times to the modern days and has fulfilled the basic need for food supply. Today still remains it's at most importance. Cognitive computing uses cognitive technologies in agriculture that help to understand, learn from experiences and environment, reason, interact and thus increase the efficiency. Civilization has led to more urbanization. There are more people than available food. There is a great necessity to increase the per meter yield. So many techniques have been seen in agriculture in terms of usage of pesticides and fertilizers, use of hybridization and green revolution to increase the production in agriculture. Now the use of modern technologies such as artificial intelligence and cognitive computation is going to bring a new big revolution for sustainable agriculture. The present paper focuses on the problems faced by the modern society in agriculture and how the cognitive computation provides an ultimate solution to the problems. We also discuss some illustrations for the usage of cognitive technologies and machine learning in the field of agriculture.

**Keywords:** Cognitive Computing, Cognitive Technology, Sustainable Agriculture

### I. INTRODUCTION

Agriculture is the industry that followed the evolution of human beings from ancient times to modern times and fulfilled its basic need for food supply [1]. Even today this still remains its primary importance, but it is integrated with more complex mechanisms driven by multiple environmental, economic and sociological forces. This \$5 trillion industry representing 10 percent of global consumer spending, 40 percent of employment and 30 percent of greenhouse gas emissions continues to keep pace with world's evolution, changing tremendously over the past years. Digital and technological advancements are taking over the industry, enhancing food production while adding value to the entire farm-to-fork supply chain and helping it make use of natural resources more efficiently.

Data generated by sensors or agricultural drones collected at farms, on the field or during transportation offer a wealth of information about soil, seeds, livestock, crops, costs, farm equipment or the use of water and fertilizer. Internet of Things technologies and advanced analytics help farmers analyze real time data like weather, temperature, moisture, prices or GPS signals and provide insights on how to optimize and increase yield, improve farm planning, make

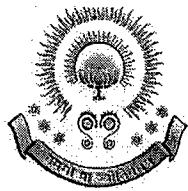
smarter decisions about the level of resources needed, when and where to distribute them in order to prevent waste. Efficiency and productivity will increase in the next years as precision agriculture grows bigger and farms become smarter and more connected. It is estimated that by 2020, over 75 million agricultural IoT devices will be in use, while the average farm is expected to generate an average of 4.1 million data points every day in 2050.

### II. SUSTAINABLE AGRICULTURE

Always people would prefer the natural food that is free of chemicals and artificial enhancements. Unfortunately, the majority of food we consume is produced using industrialized agriculture, which is a type of agriculture where large quantities of crops and livestock are produced through industrial techniques for the purpose of sale. This type of agriculture relies heavily on a variety of chemicals and artificial enhancements, such as pesticides, fertilizers, and genetically modified organisms. This type of agriculture also uses a large amount of fossil fuels and large machines to manage the farm land. Although industrialized agriculture has made it possible to produce large quantities of food, due to the negative aspects of this technique, there has been a shift towards sustainable agriculture.

Sustainable agriculture is a type of agriculture that focuses on producing long-term crops and livestock while having minimal effects on the environment [2]. This type of agriculture tries to find a good balance between the need for food production and the preservation of the ecological system within the environment. In addition to producing food, there are several overall goals associated with sustainable agriculture, including conserving water, reducing the use of fertilizers and pesticides, and promoting biodiversity in crops grown and the ecosystem. Sustainable agriculture also focuses on maintaining economic stability of farms and helping farmers improve their techniques and quality of life.

There are many farming strategies that are used that help make agriculture more sustainable. Some of the most common techniques include growing plants that can create their own nutrients to reduce the use of fertilizers and rotating crops in fields, which minimizes pesticide use because the crops are changing frequently. Another common technique is mixing crops, which reduces the risk of a disease destroying a whole crop and decreases the need



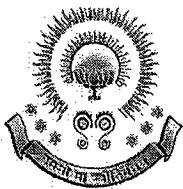
**PARVATHAREDDY BABUL REDDY**  
**VISVODAYA INSTITUTE OF TECHNOLOGY & SCIENCE**  
(Affiliated to J.N.T.U.A, Approved by AICTE and Accredited by NAAC with 'A' Grade)  
**KAVALI – 524201, S.P.S.R Nellore Dist., A.P. India. Ph: 08626-243930**



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

List of Publications of faculty for the academic year 2018-2019

S.No	Name of the Faculty	Title of the Paper	Journal Name and ISBN/ISSN	Vol.No. Issue No. Page No.	Month & Year	Link for relevant document
1	Dr. D.Srujan Chandra Reddy	Secure Access Control Scheme For Data Sharing Using KAE And Attribute Authority Based CP-ABE Schemes	International Journal of Science and Technology ISSN:0974-5645	Vol 11(48),	December 2018	<a href="http://www.indjst.org/index.php/indjst/article/download/138791/99217">www.indjst.org/index.php/indjst/article/download/138791/99217</a>
2	M.Suman	Classification Of Malicious Web Pages In Mobile Environment	Indian journal of Science and Technology ISSN:0974-5645	Vol 11(45),	December 2018	<a href="http://www.indjst.org/index.php/indjst/article/download/137460/98087">www.indjst.org/index.php/indjst/article/download/137460/98087</a>
3	B.Rasagna	An Entity Resolution Using Query Sensible Approach	International Journal of Science and Technology ISSN:0974-5645	Vol 11(48)	December 2018	<a href="https://indjst.org/articles/an-entity-resolution-using-query-sensible-approach">https://indjst.org/articles/an-entity-resolution-using-query-sensible-approach</a>
4	P.V.N.Rajeswari	A Design Approach For Efficient Mining Human Activity Pattern Over Big data	Indian Journal of Science and Technology&ISSN:0974-5645	Vol 12(3)	January 2019	<a href="https://indjst.org/articles/a-design-approach-for-efficient-mining-human-activity-patterns-over-big-data">https://indjst.org/articles/a-design-approach-for-efficient-mining-human-activity-patterns-over-big-data</a>
5	B.Murali Krishna	An Efficient Profit Maximization Scheme in Cloud For Customer Satisfaction	International Journal of Science and Technology ISSN:2249-7455	Vol.No.IX Issue No. 2 Page No. 1606	February 2019	<a href="http://ijamtes.org/gallery/191-feb2019.pdf">http://ijamtes.org/gallery/191-feb2019.pdf</a>
6	D.Srinivasulu Reddy	Data Storage Security In Cloud Computing Using AES Under AKPA	International Journal of Management Technology and Engineering & ISSN :2249-7455	Vol No IX Issue No.II page No.1824	February 2019	<a href="http://www.ijamtes.org/gallery/190-feb2019.pdf">http://www.ijamtes.org/gallery/190-feb2019.pdf</a>
7	D.Srinivasulu Reddy	A Rapid Phrasing Search For Encrypted Cloud Storage	International Journal of Management Technology and Engineering&ISSN :2249-7455	Vol No IX Issue No.III page No.1231	March 2019	<a href="https://app.box.com/s/vwtx06z26hdh38nqvkealgvw9y92177c">https://app.box.com/s/vwtx06z26hdh38nqvkealgvw9y92177c</a>
8	P.Eswaraiah	Providing Security Using CSPTCHS:Captcha as a Graphical Password	International Journal of Research&ISSN:2348-6848	Vol.No.06 Issue No.03 Page No.1	March 2019	<a href="https://journals.pen2print.org/index.php/ijr/article/view/17158/16741">https://journals.pen2print.org/index.php/ijr/article/view/17158/16741</a>
9	P.Eswaraiah	Security Pattern Classification For Adversarial Application	International Journal of Research&ISSN:2348-6848	Vol.No.06 Issue No.03 Page No.963	March 2019	<a href="https://journals.pen2print.org/index.php/ijr/article/view/17342/16939">https://journals.pen2print.org/index.php/ijr/article/view/17342/16939</a>

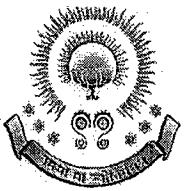


**PARVATHAREDDY BABUL REDDY**  
**VISVODAYA INSTITUTE OF TECHNOLOGY & SCIENCE**  
(Affiliated to J.N.T.U.A, Approved by AICTE and Accredited by NAAC with 'A' Grade)  
**KAVALI – 524201, S.P.S.R Nellore Dist., A.P. India. Ph: 08626-243930**



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

10	Ch.Chandra Sekhar	IOT Based Automatic Smart Agriculture system Using Google Assistant	Journal of Emerging Technologies and Innovative Research&ISSN:2349-5162	Volume 6 Issue 3	March 2019	<a href="http://www.jetir.org/papers/JETIR1903G10.pdf">http://www.jetir.org/papers/JETIR1903G10.pdf</a>
11	P.Feridoz Khan	Secure Location Sharing Using Stamp	International Journal of Research&ISSN:2348-6848	Vol.No.6 Issue No.3	March 2019	<a href="http://journals.pen2print.org/index.php/ijr/">http://journals.pen2print.org/index.php/ijr/</a>
12	Dr.V.V.Sunil Kumar	A privacy preserving approach for secure photo sharing in osn's	JETIR ISSN:2349-5162	VOL-6, ISSUE-4	APRIL 2019	<a href="http://www.jetir.org/papers/JETIR199969.docx">http://www.jetir.org/papers/JETIR199969.docx</a>
13	G.Venkateswarlu	Scalable And Efficient Portable Data Possession in Multi Cloud Environment	International Journal of Scientific Research and Review&ISSN:2279:543 X	Vol No.8 Issue No.2 page No.646	April 2019	<a href="http://www.dynamicpublisher.org/gallery/67-ijsrr-d1482.f.pdf">http://www.dynamicpublisher.org/gallery/67-ijsrr-d1482.f.pdf</a>
14	G.Venkateswarlu	Protecting Cloud Based Multimedia Content Using Signatures	International Journal of Scientific Research and Review&ISSN:2236:6124	Vol NoVIII Issue No.IV page No.2911	April 2019	<a href="http://www.ijsrr.com">www.ijsrr.com</a>
15	M.Suman	Remote PC	International Journal of Emerging Technologies and Innovative Research& ISSN:2349-5162	Vol.No.06 Issue No.4	April 2019	<a href="http://www.ijetir.com">www.ijetir.com</a>
16	P.V.N Rajeswari	A Multi-Tenant Access Control Scheme For Sharing Resources In Cloud Computing Environment	International Journal of Emerging Technologies and Innovative Research& ISSN: 2349-5162	Vol.No.06 Issue No.4	April 2019	<a href="http://www.jetir.org/papers/JETIR1904D40.pdf">http://www.jetir.org/papers/JETIR1904D40.pdf</a>
17	P.V.N Rajeswari	Filter Unwanted Messages From OSN User Wall	International Journal of Research & ISSN: 2236-6124	Vol.No.06 Issue No.4	April 2019	<a href="http://www.ijrpublisher.com">www.ijrpublisher.com</a>
18	K.Sireesha	Confidential Data Sharing In Cloud Computing RS-IBE	International Journal of Research&ISSN:2236-6124	Vol.No.VIII Issue No.IV Page No.1673	April 2019	<a href="http://www.ijr.com">www.ijr.com</a>
19	B.Rasagna	Prediction Based Offloading Strategy In Mobile Cloud Computing	International Journal of Research&ISSN:2236-6124	Vol.No.VIII Issue No.IV Page No.1432	April 2019	<a href="http://www.ijrpublisher.com">www.ijrpublisher.com</a>
20	B.Rasagna	An Efficient Multi Keyword Ranked Search Over Encrypted Cloud Data	International Journal of Research&ISSN:2348-6848	Vol.No.6 Issue No.4	April 2019	<a href="http://www.ijr.com">www.ijr.com</a>



**PARVATHAREDDY BABUL REDDY**  
**VISVODAYA INSTITUTE OF TECHNOLOGY & SCIENCE**  
(Affiliated to J.N.T.U.A, Approved by AICTE and Accredited by NAAC with 'A' Grade)  
**KAVALI – 524201, S.P.S.R Nellore Dist., A.P. India. Ph: 08626-243930**



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

21	G.Venu Gopal	Digital Video Stenography	International Journal of Research&ISSN:2236-6124	Vol.No.VIII Issue No.IV Page No.1848	April 2019	<a href="http://www.ijr.com">www.ijr.com</a>
22	M.Janardhan	An Efficient And Secure Three-Layer Architecture For Cloud Storage Using Intelligence Of FOG Computing	International Journal of Research&ISSN:2236-6124	Vol.No.VIII Issue No.IV	April 2019	<a href="http://www.ijrpublisher.com">www.ijrpublisher.com</a>
23	P.Srinivasulu	Online Location Based Tourist Guide Route recommendation With Place Of Intrest	International Journal of Research&ISSN:2236-6124	Vol.No.8 Issue No.3	April 2019	<a href="http://www.ijr.com">www.ijr.com</a>
24	P.Srinivasulu	A Secure Access Control Schema Using CP-ABE And KAE For Cloud Computing	International Journal of Research&ISSN:2236-6124	Vol.No.VIII Issue No.IV	April 2019	<a href="http://www.ijr.com">www.ijr.com</a>

**Faculty Incharge**

**HOD**

**Head of Department**  
**COMPUTER SCIENCE ENGINEERING**  
**Visvodaya Institute of Technology & Science**  
**KAVALI - 524 201, SPSR, Nellore Dt.**

# Secure Access Control Scheme for Data Sharing Using KAE and Attribute Authority Based CP-ABE Schemes

D.S.C. Reddy and Papietty Saranya\*

Department of CSE, PBR Visvodaya Institute of Technology and Science, Nellore - 524201, Andhra Pradesh, India; saranyacse039@gmail.com, srujand@hotmail.com

## Abstract

**Objective:** To study the access control scheme to protect users' privacy problem in cloud environment is great significance. To overcome the above problem we build a new access control scheme with privilege separation based on privacy protection. **Methods/Statistical Analysis:** Data sharing is one of the key features which change the business/individuals life style in store and share data using clouds. But it also poses data privacy issues. To this effect, in this study we develop a scheme named as PS-ACS (Privacy protection based Access control scheme), which uses cloud servers to store and share the owners' data; for that cloud server divides the users into private and public platforms. And also analyzes the Key Aggregate Encryption (KAE) and Improved Attribute-Based Signature (IABS) to manage the read and write access rights of users in private platform. Also re-evaluates the Hierarchical Attribute-based Encryption which is applied to avoid the bottleneck issue in public platform. **Findings:** Here, we consider the data files of user's private photos, blog data, log files, and business files which required data owners to grant the access rights to read or modify the private data. To protect the data privacy, we use KAE and IABS to build the PS-ACS while sharing the data to the cloud users. In this study, we also show our scheme is protects the data privacy rather than existing techniques. **Applications/Improvements:** We have used different encryption schemes in two different platforms which protect the data privacy efficiently and also we extend our scheme to avoid the single point of failure using HABE efficiently.

**Keywords:** Access Control, Attribute Based Signature Scheme, Data Sharing, Privacy Protection, User Revocation

## 1. Introduction

For users, it is necessary to take full advantage of cloud-based storage service, and conjointly to warrant information privacy. Therefore, we have to ensure a far better access management mechanism<sup>1</sup>. Since, the previous access management techniques cannot provide complete safety to information sharing efficiently. Information security risks brought by data sharing can critically mired in the implementation of cloud computing, many solutions to attain encode and decode of knowledge sharing are projected.

Many authors planned varied techniques to safeguard the privacy of users. In<sup>2</sup> presented the Cipher text-policy Attribute-Based Encryption (CP-ABE), but

which does not assume the revocation of access rights. In<sup>3</sup> presented the most straightforward revocation plan anyway it coordinates to key update issue. In<sup>4</sup> specified Multi-Authority ABE (MA-ABE) to solve key update issue. However, the access rights are not applicable. In<sup>5</sup> introduced information sharing system supported general attributes based cryptography, which offers various access rights to the various users. However, it is inefficient for the complexities.

In<sup>6</sup> presented Key-Aggregate Encryption in which it is difficult to encode the elements of the cipher text and the corresponding key, though exclusively inside the conditions once the information proprietor receptive to the client's attributes. These plans over the sole point on one component of the investigation, and can't offer a

\*Author for correspondence

# Classification of Malicious Webpages in Mobile Environment

Mallu Suman and Sagam Sravanth Kumar\*

Department of CSE, Visvodaya Engineering College, JNTUA, Kavali - 524 201, Andhra Pradesh, India;  
vasanth.sravanth@gmail.com, sumanvec@gmail.com

## Abstract

**Objective:** To study the detection of malicious web page in mobile environment by lowering the false positive rate (FPR) and False Negative Rate (FNR) in real time and also how this CMW blocks the access of malicious webpages to the user are to be studied. **Methods/Statistical Analysis:** Now a days, Mobile devices are progressively being used to access the webpages. Content, Layout size, Functionality have commonly been used to perform the static analysis to check the maliciousness in desktop space. In this paper we have presented a methodology named as CMW (Classification of malicious webpages) which detects the malicious mobile webpages in mobile environment. Here we used static features of mobile webpages derived from the HTML and Javascript content, URL and leading mobile specific capabilities. We then collected over 3500 mobile benign and malicious webpages. **Findings:** We have extracted a feature set consists of 44 features. 11 of which are not previously identified nor used. we then used a binomial classification technique to build a model for CMW to provide 90% accuracy and 89% true positive rate. It also detects a number of malicious webpages which are not accurately detected by existing techniques such as VirusTotal and Google Safe Browsing. **Application/Improvements:** We have used 11 new features in our feature set. Due to these new features, the detection of malicious webpages rate will be increased and false positive and false negative rates are reduced.

**Keywords:** Classification, Features, Machine Learning, Malicious Web Pages, Static Detection

## 1. Introduction

In recent years, Mobile devices are widely used in order to access the web pages. However, despite the considerable advances in processor power and bandwidth, the browsing experience on mobile is significantly different. These variations can mostly be endorsed to the reduction of size of the screen dramatically, which effect's the functionality of the content and layout relating the mobile webpages.

To perform static analysis in order to verify malignancy in the desktop space<sup>1,2</sup> Content, functionality and also layout have often been used. Conventionally, the malicious intent was recognised by the features such as the frequency of iframes and the number of redirections have served. But such affirmations may no longer be true due to the several modifications made to accommodate

mobile devices. To consider mobile specific webpage elements like calls to mobile APIs, several earlier techniques were also failed.

In this paper, we present CMW (Classification of Mobile Webpages), a static analysis technique which is fast and reliable to identify vicious mobile web pages. CMW exploits static features of webpages that are derived from their HTML and JavaScript content, URL and advanced mobile specific abilities. Analytically we have describe the distributions of similar static features when determined from desktop and mobile webpages differ vividly. We then accumulate mobile benign and malicious webpages in the duration of three months. And then exploits a binomial classification technique to extend a model for CMW to provide 90% accuracy and 89% true positive rate. CMW's matches of the performances surpassed that of existing

\*Author for correspondence

# An Entity Resolution using Query Sensible Approach

Bheema Rasagna\* and Kummaragunta Lakshmi Prasanna

Department of CSE, Visvodaya Engineering College, JNTUA, Kavali – 524201, Andhra Pradesh, India:  
rasagnabheema87@gmail.com, lakshmi.kummaragunta@gmail.com

## Abstract:

**Objective:** To study the Entity Resolution (ER) using Qualified Security Assessor (QSA) to minimize the pre-processing steps which are required to fetch the data a given Structured Query Language (SQL)-like selection correctly. **Methods/Statistical Analysis:**

In recent times, the problem of Entity Resolution is carried out in the context of data warehousing as an offline pre-processing step prior to the making data accessible to analysis – an approach that works well under paradigm settings. Such an offline approach, however, is not possible in budding applications that requires analyzing only small portions of the whole dataset and generating answers in (near) real-time. In this we presented an approach named as (QSA) to minimizing the data pre-processing steps in query processing to detect the objects. **Findings:** To test the efficiency of the QSA we collected the bibliographic data from the Google Scholar. This data contained the top 50 computer related researchers each having h-index of 60 or higher. The dataset contained 16, 396 records where 14.3% are duplicates. Then we apply the QSA using two blocking function to group the data records that might be duplicates together. Finally, we ensure pair wise resolve function to detect whether two records represent the same real world entity or not accurately.

**Applications/Improvements:** We have used the semantics of such a collection predicate to decrease pre-processing in the Entity Resolution. The accuracy of the entity resolution using QSA will be increased.

**Keywords:** Data Wareho use, Entity Resolution, Offline Pre-processing, Query Processing, Rudimentary

## 1. Introduction

This study deals with the problem of Entity Resolution (ER) challenge. Predictably, entity resolution brings out in the background of data warehousing as an offline pre-processing step earlier to building data available to analysis – an approach that facilitates well under idea settings. Such an offline approach is not possible in growing applications that need analyzing only tiny portions of the complete data and the producing answers in real-time<sup>1</sup>.

Our approach is stimulated by various key points of view<sup>2</sup>. First, the requirement for current analysis needs modern environments to achieve timely analytical tasks, building it impractical for those environments to utilize detained hypothesis back-end pre-processing technologies. Second, in the context of data analysis task, where

a data analyst may measure and examine data as part of a single step, the method will know “what to clean” only at query time. Last, outlines wherein a little establishment contains an expansive dataset, yet require analyze just small segments of it to answer some efficient inquiries instantly. In such a case, it would be pointless for that organization to use their insufficient accessible assets on pre-handling absolute information, for the most part given that the vast majority of it will be copy.

The earlier methods cannot utilize the rules of such a variety predicate to decrease pre-processing. To deal with these new pre-processing confronts we proposed a QSA to data pre-processing<sup>3,4</sup>. QSA is a fully new balancing model for enhancing the effectiveness: It distinguishes from blocking<sup>5</sup> and is usually additional efficient in collaborating with jamming. QSA measure results are similar

\*Author for correspondence

# A Design Approach for Efficient Mining Human Activity Patterns over Big Data

P. V. N. Rajeswari\* and Kodi Roshan Sai Kumar

Department of CSE, Visvodaya Engineering College, Kavali – 524201, Andhra Pradesh, India; rajivrphd@gmail.com, roshansaikumar24@gmail.com

## Abstract

**Background/Objectives:** In recent times, urban areas are turned to be a smart dwelling spot. In smart cities, most things are done automatically using smart devices such as sensors and smart meters. These smart devices produce large volumes of fine-grained data and stored into servers. To make a study on how to train and detect human health behaviour patterns for healthcare applications from smart meter data. **Methods/Statistical Analysis:** To analyze and detect human activity patterns, we build an Efficient Mining technique using frequent pattern mining and clustering techniques. Here, we consider the UK-Dale dataset incorporates time series information of intensity utilization gathered somewhere in the range of 2012 and 2015. To training and detecting human pattern we build an Efficient Mining technique. **Findings:** The identification of human behaviour patterns for appliance usage using this technique is better than existing techniques with accuracy for short and long term predictions. **Applications/Improvements:** We also extend our work to analyze temporal energy consumption patterns at the appliance level, which is directly related to human activities.

**Keywords:** Behavioural Analysis, Big Data, Data Clustering, Frequent Pattern Mining, Smart Cities

## 1. Introduction

The ongoing overview demonstrates the large portion of the general population indicating enthusiasm to live in urban territories<sup>1</sup>. In reacting to the new needs and difficulties, urban communities are at present grasping monstrous advanced change with an end goal to help manageable urban networks, and give more advantageous condition<sup>2,3</sup>. In such a change, a large number of homes are being furnished with shrewd gadgets, which create enormous volumes of fine-grained and indexical information that can be dissected to help social insurance services.

Progression of big data mining advances, which give methods for handling immense amount of information for noteworthy experiences, can help in seeing how individuals approach their life. For instance, checking the alterations of appliance utilization inside a smart home can be utilized implicitly decide the individual's prosper-

ity depending on authentic information. Since individuals' propensities are for the most part distinguished by ordinary schedules, finding these schedules enables us to perceive odd exercises that may demonstrate individuals' troubles in taking consideration for themselves, for example, not making food or not utilizing shower/shower<sup>4,5</sup>. The fundamental connection between appliance utilization inside the smart home and routine exercises can be utilized by health care applications to identify potential medical issues. This isn't just going to ease the burden on health issues, yet additionally giving 24 hour checking administration that naturally distinguishes typical and anomalous practices for autonomously living patients or those with self-constraining conditions (e.g. elderly and patients with cognitive impairments).

This study proposes the utilization of vital information from smart meters fixed at homes to uncover essential exercises of occupants. Our investigation accepts that there are methods set up to shield individuals' secrecy from being

\*Author for correspondence

# An Efficient Profit Maximization Scheme in Cloud for Customer Satisfaction

First Author: B. Murali Krishna,M.Tech, Assistant Professor in Department of CSE, PBR Visvodaya Institute of Technology and Science, Kavali, Nellore.

Second Author:

P.Madhuri, pursuing B.Tech (CSE) from PBR Visvodaya Institute of Technology and Science, Kavali, Nellore.

G. Kavya, pursuing B.Tech (CSE) from PBR Visvodaya Institute of Technology and Science, Kavali, Nellore.

K. Sowmya, pursuing B.Tech (CSE) from PBR Visvodaya Institute of Technology and Science, Kavali, Nellore.

S. Sravani, pursuing B.Tech (CSE) from PBR Visvodaya Institute of Technology and Science, Kavali, Nellore.

## ABSTRACT

Alongside the advancement of distributed computing, an expanding number of endeavors begin to embrace cloud administration, which advances the development of many cloud specialist co-ops. For cloud specialist organizations, how to arrange their cloud administration stages to acquire the greatest benefit turns out to be progressively the center that they focus on. We think about consumer loyalty to address this issue. Consumer loyalty influences the benefit of cloud specialist organizations in two different ways. On one hand, the cloud arrangement influences the nature of administration which is an essential factor influencing consumer loyalty. Then again, the consumer loyalty influences the demand landing rate of a cloud specialist organization. In any case, few existing works think about consumer loyalty in tackling benefit augmentation issue, or the current works considering consumer loyalty don't give a legitimate formalized definition for it. Subsequently, we initially allude to the meaning of consumer loyalty in financial matters and build up a recipe for estimating consumer loyalty in distributed computing. And after that, an investigation is given in detail on how the consumer loyalty influences the benefit. Finally, mulling over consumer loyalty, administration level understanding, leasing value, vitality utilization, etc, a benefit augmentation issue is planned and illuminated to get the ideal design to such an extent that the benefit is amplified..

## 1. INTRODUCTION

Cloud computing is the delivery of resources and computing as a service rather than a product over the Internet, such that accesses to shared hardware, software, databases, information, and all resources are provided to consumers on-demand. Customers use and pay for services on-demand without considering the upfront infrastructure costs and the subsequent maintenance cost. Due to such advantages, cloud computing is becoming more and more popular and has received considerable attention recently. Nowadays, there have been many cloud service providers, such as Amazon EC2, Microsoft Azure, Salesforce.com, and so forth. As a kind of new IT commercial model, profit is an important concern of cloud service providers. As shown in Fig1, the cloud service providers rent resources from infrastructure providers to configure the service platforms and provide paid services to customers to make profits. For cloud service providers, how to configure their cloud service platforms to obtain the maximal profit becomes increasingly the focus that they pay attention to the optimal configuration problem with profit maximization of cloud service providers has been researched in our previous researches which assumed that the cloud service demand is known in advance and not affected by external factors. However, the request arrival rate of a service provider is affected by many factors in actual, and customer satisfaction is the most important factor.

For example, customers could submit their tasks to a cloud computing platform or execute them on their local computing platforms

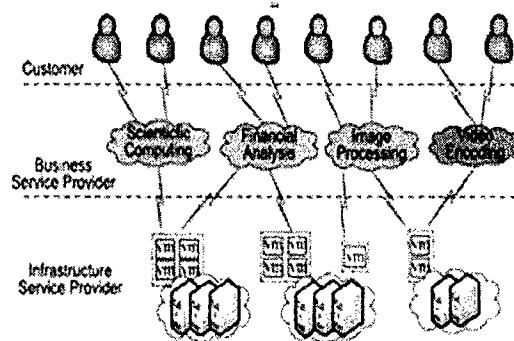


Fig.1. the three tier cloud structure.

The customer behavior depends on if the cloud service is attractive enough to them. To configure a cloud service platform properly, the cloud service provider should know how customer satisfaction affects the service demands. Hence, considering customer satisfaction in profit optimization problem is necessary. However, few existing works take customer satisfaction into consideration in solving profit maximization

# Data Storage Security in Cloud Computing Using AES under AKPA

D. Srinivasulu Reddy<sup>1</sup>, M.Tech, ISTE, Associate Professor in Department of CSE, PBR Visvodaya Institute of Technology and Science, Kavali, Nellore.

Maramreddy Srihari<sup>2</sup>, pursuing Master of Computer Applications (MCA) from PBR Visvodaya Institute of Technology and Science, Kavali, Nellore.

## ABSTRACT

**Distributed computing** is the novel pattern in everywhere throughout the world. Distributed computing gives the capacity to use assets through Internet. As a great deal of specialist organizations of the cloud are accessible in the aggressive PC world. Security in Cloud registering is an essential and basic perspective, and has various issues and issue identified with it. In this we will talk about how to give security to the information from the unapproved clients and give uprightness to the clients. It requires an extremely high level of security and validation. To secure the information in cloud database server, cryptography is one of the imperative strategies. Cryptography gives different symmetric and topsy-turvy calculations to verify the information. This paper shows the symmetric cryptographic calculation named as AES (Advanced Encryption Standard). It depends on a few substitutions, stage and change.

Keywords - Cloud Computing, Cryptography, Security, AES

## 1. INTRODUCTION

Cloud computing is a set of IT Services evolving as the next generation. This service provided to a customer over a network and these services are delivered by third party provider who owns the infrastructure. The data is stored in remote sector. Cloud Computing is the combination of a technology, platform that provides hosting and storage service on the Internet. Cloud computing is sharing of resources on a larger scale which is cost effective and location independent. There are three types of cloud according to their usage. They are private cloud, public cloud and hybrid cloud. The private cloud is owned by a single organization and public clouds are shared on a larger scale. Hybrid cloud is a combination of Private cloud and Public Cloud which is used by most of the industries. Private cloud provides better control and more flexibility. It is provided three levels of "as a service" over the Internet (i) infrastructure as a service (IaaS)- provides hardware and software and equipment to deliver software application environments with a resource usage, (ii)platform as a service (PaaS)-offers an integrated environment to build test and deploy customer applications.,(iii) software as a service (SaaS)- software development model where applications are remotely hosted by an application or service provider and made available to customer via the Internet. Cloud computing is the broader concept of infrastructure convergence. Cloud computing can manage and store all smart phones or tablets apps at one location. So we do not require any memory space at our end. The advantages of cloud computing may be very appealing but nothing is perfect. Cloud got many issues when it comes to security especially on Data theft. Data loss and Privacy. The parameters that affect the security of the cloud and problems faced by cloud service provider and cloud service consumer such as data, privacy, infected application and security issues. This also gives

the security of data and applications in case device is damaged or lost.

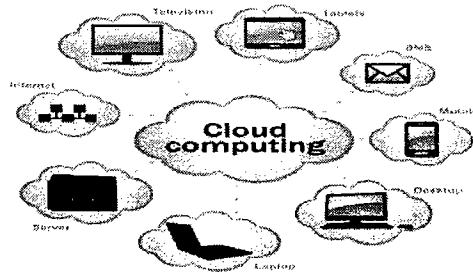


Figure 1: General Structure of Cloud Computing

## 2. CRYPTOGRAPHY

The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography. Security goals of data cover three points namely: Availability, Confidentiality, and Integrity. Cryptography, in modern days is considered grouping of three types of algorithms. They are

### SYMMETRIC-KEY ALGORITHMS

Symmetric algorithms used the same (secret key) key for encryption and decryption. The same key messages are used for encrypted by the sender and decrypted by the receiver. It contains algorithms like Data Encryption Standard (DES), Advanced Encryption Standard (AES), IDEA, Twofish, Ron's Code (RCn), and Triple DES, Blowfish etc.

### ASYMMETRIC-KEY OR PUBLIC KEY ALGORITHMS

Asymmetric algorithms use different keys. One key (public) is used for encryption and other (private key) is used for decryption. It comprises various algorithms like Rivest, Shamir, & Adleman (RSA), Digital

# A Rapid Phrasing Search for Encrypted Cloud storage

1. D. Srinivasulu Reddy, M.Tech, ISTE, Associate Professor in Department of CSE, PBR Visvadaya Institute of Technology and Science, Kavali, Nellore.

K.Sree Keerthi, pursuing B.Tech (CSE) from PBR Visvadaya Institute of Technology and Science, Kavali, Nellore  
S.Devaraj, pursuing B.Tech (CSE) from PBR Visvadaya Institute of Technology and Science, Kavali, Nellore  
Sk. Shahul, pursuing B.Tech (CSE) from PBR Visvadaya Institute of Technology and Science, Kavali, Nellore  
S.Tejeswi, pursuing B.Tech (CSE) from PBR Visvadaya Institute of Technology and Science, Kavali, Nellore

## Abstract:

Cloud computing has generated much interest in the research community in recent years for its many advantages but has also raised security and privacy concerns. The storage and access of confidential documents have been identified as one of the central problems in the area. In particular, many researchers investigated solutions to search over encrypted documents stored on remote cloud servers. Cloud registering is a technology, which gives low cost, scalable computational limit. The capacity and access of report have been significant issue in this area. While, many plans have been proposed to perform conjunctive keyword search, less consideration has been noted. In this paper, we show an expression seek strategy in light of sprout filters, which is speedier than existing framework. Our systems utilize conjunctive catchphrase inquiry to help functionalities. This approach additionally depicted the false positive rate.

## 1.INTRODUCTION

Distributed computing<sup>[1]</sup> has produced much enthusiasm for the examination group in late years. To look over encoded archives put away on cloud numerous plans has been proposed yet less consideration have been noted on more hunt techniques. To conquer the capacity and access of classified reports put away in cloud. We proposed an expression seek utilizing sprout channels which is quicker than existing system. Our procedures utilize a conjunctive watchword which is downside of existing framework to get the put away record speedier and get to secure<sup>[2]</sup>. This approach likewise portrayed the false positive rate for the catchphrase look. Record streams are made and conveyed in different structures on the Internet, for example, news streams, messages, smaller scale blog articles, visiting messages, look into paper documents, web gathering talks, et cetera. The substance of

these records by and large focusses on some disconnected get-togethers and clients' qualities, in actuality. To mine these snippets of data, a great deal of looks into of content mining concentrated on separating themes from report accumulations and archive streams through different probabilistic subject models, for example, established PLSI, LDA and their augmentations. Exploiting these separated themes in report streams, the vast majority of existing works broke down the development of individual subjects to recognize and foresee get-togethers and in addition client practices. In any case, few investigates focused on the relationships among various subjects showing up in progressive records distributed by a particular client, so some covered up yet critical data to uncover customized practices has been ignored. Keeping in mind the end goal to describe client practices in distributed record streams, we ponder on the connections among points

# Providing Security Using CAPTCHA: Captcha as A Graphical Password

Mr. Eswaraiah Puttu & Murahari Bhagyaraj

#1 Associate Professor, Dept of CSE, PBR Visvodaya Institute Of Technology And Science, Kavali, India

#2 Student, Dept of Master of Computer Application (MCA), PBR Visvodaya Institute Of Technology And Science, Kavali, India

**ABSTRACT:** Various security primitives uses hard mathematical problems. Use of hard AI problems for security is emerging and exciting new pattern, but has not yet been explored. In our project, we present a new security primitive based on hard AI problems, this system is named as Captcha as graphical passwords (CaRP). CaRP is Captcha as well as graphical password scheme. CaRP symbolize a number of security problems together, such as online guessing attacks, relay attacks, and shoulder-surfing attacks. Generally, a CaRP password can be found only probabilistically by automatic online guessing attacks even if the password is in the search set. CaRP also offers well approach to address the well-known image hotspot problem in popular graphical password systems, like PassPoints, that generally leads to choices of weak password.

**KEYWORDS:** Imaged based CAPTCHA, Graphical CAPTCHA, Authentication, CAPTCHA, Passwords, Graphical Passwords, Security Attacks, Hard AI problem, Click based CAPTCHA, CaRP, Password Guessing Attacks, Security Primitives, etc.

## I.INTRODUCTION

Graphical passwords are knowledge-based authentication mechanisms where users enter a shared secret as evidence of their identity. However, where text passwords involve alphanumeric and/or special keyboard characters, the idea behind graphical passwords is to leverage human memory for visual information, with the shared secret being related to or composed of images or sketches. Despite the large number of options for authentication, text passwords remain the most common choice for many reasons. Passwords are the most common method of authenticating users, and will most likely continue to be widely used for the foreseeable future, due to their convenience and practicality for service providers and end-users. Although more secure authentication schemes have been suggested in the past. Authentication refers to the process of confirming or denying an individual's claimed identity. Authentication schemes require users to memorize the passwords and recall them during log-in time. Also, adequate authentication is the first line of defence for protecting any resource. Graphical techniques are one of the many alternatives proposed to address the weaknesses in the conventional

## Security Pattern Classifiers for Adversarial Applications

Mr. Eswaraiah Puttu & Ms.Darsi Mounika

#1 Associate Professor,Dept of CSE, PBR Visvodaya Institute Of Technology And Science,Kavali,India  
#2 Studnet,Dept of Master of Computer Application (MCA), PBR Visvodaya Institute Of Technology

And Science ,Kavali,India

**Abstract:** *Pattern classification systems are commonly used in adversarial applications, like biometric authentication, network intrusion detection, and spam filtering, in which data can be purposely manipulated by humans to undermine their operation. As this adversarial scenario is not taken into account by classical design methods, pattern classification systems may exhibit vulnerabilities, whose exploitation may severely affect their performance, and consequently limit their practical utility. In this paper, we address one of the main open issues: evaluating at design phase the security of pattern classifiers, namely, the performance degradation under potential attacks they may incur during operation. We propose a framework for empirical evaluation of classifier security that formalizes and generalizes the main ideas proposed in the literature, and give examples of its use in three real applications. Reported results show that security evaluation can provide a more complete understanding of the classifier's behavior in adversarial environments, and lead to better design choices*

**Keywords:** Data Mining; Java Technology; UML Diagrams; Data Flow Diagram;

### 1.INTRODUCTION:

PATTERN classification systems based on machine learning algorithms are commonly used in security-related applications like biometric authentication, network intrusion detection, and spam filtering, to discriminate

between a “legitimate” and a “malicious” pattern class (e.g., legitimate and spam emails). Contrary to traditional ones, these applications have an intrinsic adversarial nature since the input data can be purposely manipulated by an intelligent and adaptive adversary to undermine classifier operation. This often gives rise to an arms race between the adversary and the classifier designer. Well known examples of attacks against pattern classifiers are submitting a fake biometric trait to a biometric authentication system (spoofing attack) [1], [2]; modifying network packets belonging to intrusive traffic to evade intrusion detection systems (IDSs) [3]; manipulating the content of spam emails to get them past spam filters (e.g., by misspelling common spam words to avoid their detection) [4], [5], [6]. Adversarial scenarios can also occur in intelligent data M analysis [7] and information retrieval [8]; e.g., a malicious webmaster may manipulate search engine rankings to artificially promote her1 website. It is now acknowledged that, since pattern classification systems based on classical theory and design methods [9] do not take into account adversarial settings, they exhibit vulnerabilities to several potential attacks, allowing adversaries to undermine their effectiveness A systematic and unified treatment of this issue is thus needed to allow the trusted adoption of pattern classifiers in adversarial environments, starting from the theoretical foundations up to novel design methods, extending the classical design cycle of [9].

# IoT based Automatic Smart Agriculture System using Google Assistant

<sup>1</sup>Mr.CH.Chandra sekar, <sup>2</sup>P.Yogasindhu, <sup>3</sup>P.Lakshmi Jahnavi, <sup>4</sup>P.Rajitha, <sup>5</sup>N.Lakshmi Priya, <sup>6</sup>P.Mounika

<sup>1</sup> Assistant Professor, <sup>2</sup>Student, <sup>3</sup>Student, <sup>4</sup>Student, <sup>5</sup>Student, <sup>6</sup>Student  
Department of Computer Science, PBR Visvodaya Institute of Technology and Science,  
Kavali, Andhra Pradesh, India

**Abstract :** The paper aims to look at all farmers problems and to find a solution. Since, IOT is an emerging field and its applications are wide, the paper has included the application of IOT in agriculture as well. The paper aims at helping the farmer by providing data such as motor information and soil moisture sensor, through sensors, which is sent on the website, through esp8266 microcontroller which uses esp8266 chip, on which the farmer can easily see. An automatic water pump connected through a relay has been added to water the crops automatically thus reducing the work of the farmer using soil moisture sensor. We can switch on water pump through Google assistant voice input from all over world. Here we are using Adafruit sensor to store data IFTTT is used to link Google assistant.

**Index Terms-** Google assistant, IFTTT, ESP8266, Soil Moisture sensor, Adafruit

## I. INTRODUCTION

India's real wellspring of wage is from agriculture division and 70% of ranchers and general individuals rely upon the agriculture. In India the vast majority of the irrigation frameworks are worked physically. These old fashioned methods are supplanted with semi-robotized and computerized procedures. The accessible conventional procedures resemble jettison irrigation, terraced irrigation, dribble irrigation, sprinkler framework. The worldwide irrigation situation is arranged by expanded interest for higher horticultural efficiency, poor execution and diminished accessibility of water for agriculture. These issues can be suitably amended on the off chance that we utilize computerized framework for irrigation. In Irrigation Control System Using Android and Google Assistant for Efficient Use of Water and Power. Mechanized irrigation framework utilizes Google Assistant to turn engine ON and OFF.

## II. LITERATURE SURVEY

In Google Assistant Based Automated Irrigation Control using IOT based Irrigation System[2].Here its mentioned about using automatic microcontroller based rain gun irrigation system in which the irrigation will take place only when there

will be intense requirement of water that save a large quantity of water. These system brings a change to management of field resources where they developed a software stack called Android is used for mobile devices that include an operating system, middleware and key applications. Mobile phones have almost become an integral part of us serving multiple needs of humans. These system covered lower range of agriculture land and not economically affordable. The System Supports excess Amount of water in the land and uses wifi to send message and an android app is been used they have used a methodology to overcome under irrigation, over irrigation that causes leaching and loss of nutrient content of soil they have also promised that Microcontroller used can increase System Life and lower the power Consumption. There system is just limited to the automation of irrigation system and lacks in extra ordinary features. Automatic Irrigation Control System for Efficient Use of Resources and Crop Planning by Using an Android States and features of their system.

--The system supports water management decision, used for monitoring the whole system with ESP8266-12E WiFi module

## Secure Location Sharing Using STAMP

Mr. P.Feridoz Khan & M.Santhi Priya

#1 Asst. Professor,Dept of CSE, PBR Visvodaya Institute Of Technology And Science,Kavali,India

#2 Studnet,Dept of Master of Computer Application (MCA), PBR Visvodaya Institute Of Technology And Science ,Kavali,India

### ABSTRACT:

*Location-based services square measure quickly changing into vastly in style. Additionally to services supported users' current location, several potential services believe users' location history, or their spatial-temporal place of origin. Malicious users might idle their spatial-temporal place of origin while not a rigorously designed security system for users to prove their past locations. during this paper, we present the SpatialTemporal provenance Assurance with Mutual Proofs (STAMP) scheme. STAMP is designed for ad-hoc mobile users generating location proofs for each other in a distributed setting. However, it can easily accommodate trusted mobile users and wireless access points. STAMP ensures the integrity and nontransferability of the location proofs and protects users' privacy. A semi-trusted Certification Authority is used to distribute cryptographic keys as well as guard users against collusion by a light-weight entropy-based trust evaluation approach. Our prototype implementation on the Android platform shows that STAMP is low-cost in terms of computational and storage resources. Extensive simulation experiments show that our entropy-based trust model is able to achieve high collusion detection accuracy*

**Keywords:** Location Proof, Spatial-Temporal Provenance, Trust, Privacy

### I.INTRODUCTION

With the pervasiveness of smart phones, Location Based Services (LBS) have received considerable attention and become more popular and vital recently. However, the use of LBS also poses a potential threat to user's location privacy. In this project, we present an efficient and privacy-preserving location-based query solution, called APPLAUS and LOCATEme. Specifically, to achieve privacy-preserving spatial range query, we propose the first predicate-only encryption scheme for inner product range (Pseudonym object PO), which can be used to detect whether a position is within a given circular area in a privacy-preserving way. To reduce query latency, we further design a privacy-preserving index structure in LOCATEme. Detailed security analysis confirms the security properties of LOCATEme. In particular, for a mobile LBS user using an Android phone, around 1.9 s is needed to generate a query, and it also only requires a commodity workstation.

Today's location-sensitive service relies on user's mobile device to determine its location and send the location to the application. This approach allows the user to cheat by having his device transmit a fake location, which might enable the user to access a restricted resource erroneously or provide bogus alibis. To address this issue, we propose a privacy preserving location proof updating system (APPLAUS) in



**Journal of Emerging Technologies and Innovative Research**  
An International Open Access Journal  
www.jetir.org | editor@jetir.org

## Certificate of Publication

The Board of

Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162)

Is hereby awarding this certificate to

**Dr. V.V. SUNIL KUMAR**

In recognition of the publication of the paper entitled

**A Privacy Preserving Approach for Secure Photo Sharing in OSNs**

Published In JETIR ( www.JETIR.org ) ISSN UGC Approved & 5.87 Impact Factor

Published in Volume 6 Issue 4 , April-2019

*Pazia P*

EDITOR

JETIR1904D41

*S. Sunil*

EDITOR IN CHIEF

Research Paper Weblink <http://www.jetir.org/view?paper=JETIR1904D41>

Registration ID : 199969



# Scalable and Efficient Provable Data Possession in Multi cloud Environment

**MR. GUNUPATI VENKATESWARLU#1**

**Ms. PABBSETTY RAMYA#2,Ms. DATLA LAKSHMI SOWJANYA#3**

**Ms. INDLA ASWANI#4,Ms. PAMULAPATI SRI PALLAVI#5**

**#1** Asst.Professor,Dept of CSE, PBR Visvodaya Institute Of Technology And Science,Kavali,India

**#2** Studnet,Dept of CSE, PBR Visvodaya Institute Of Technology And Science ,Kavali,India

**#3** Studnet,Dept of CSE, PBR Visvodaya Institute Of Technology And Science ,Kavali,India

**#4** Studnet,Dept of CSE, PBR Visvodaya Institute Of Technology And Science ,Kavali,India

**#5** Studnet,Dept of CSE, PBR Visvodaya Institute Of Technology And Science ,Kavali,India

**Abstract**\_ Cloud is basically a term of virtualiaty in terms of services. In the entire world there are many problem related to cloud security, but here we are going to focused only on our phase and that is user and cloud tenant service provider. Hence distributed cloud environment, multi cloud is used. In the existing system, when client stores his data on single cloud server, the distributed storage and integrity checking are at risk. Provable data possession is a method for ensuring the integrity of data in storage outsourcing. The proposed ID-DPDP protocol able to provide client's identity with his private key and provably secure under the hardness assumption of the standard CDH problem.. It will check clients data kept safely without downloading the whole data. This protocol eliminates certificate management, efficient and flexible.

**Keywords:** Cloud Computing, Multi Cloud, Provable Data Possession, Data Integrity Checking

# Remote PC

Name of 1<sup>st</sup> Author: K.Sowjanya

Name of 2<sup>nd</sup> Author: P.RamyaTeja

Name of 3<sup>rd</sup> Author: v.v. Divya Mrudhula

Name of 4<sup>th</sup> Author: K.Sridhar reddy

Name of Department of Author's: Computer Science Engineering

Guide: MR. M.Suman

**Abstract-** The objective of this project is to control the PC by accessing the desktop remotely. We can work as like as our normal desktop on Java enabled mobile phone. Mobile cloud computing can give mobile device users a number of compensations. Corporation users are able to share resources and applications without a high level of capital expenditure on hardware and software resources. Mobile cloud computing provides an explanation to meet the increasing functionality demands of end-users, as all function logic is executed on distant servers and only user interface functionalities reside on the mobile device. The mobile device acts as a remote show, capturing user input and depiction the show updates received from the distant server. The normal pc desktop can be taken remotely and we can access from any part of the world using internet and wrap support service. The operations such as accessing the internet, sending emails, and also system controls like shutdown, log off, restart through the mobile phone. In our system the remote computer's desktop can be accessed from the normal mobile phone. The remote desktop connection can be made wireless and can be accessed from any part of the world. We can control the remote computer as like our normal local computer by using a java enabled mobile phone.

**Index Terms:** Remote show, capturing user input, depiction the show updates received from the distant server.

## I. INTRODUCTION

### A. Purpose

- To access the remote desktop from mobile phone.
- To see the contents of the file placed on the desktop of the remote computer.
- To reboot a remote server as a manager.

### B. Scope

It is, in spirit, a remote display system which allows you to view a computing 'desktop' environment not only on the machine where it is management, but from anywhere on the Internet and as of a wide variety of machine architectures.

Remote PC based architecture for accessing the desktop of various remote systems (such as MS Windows, Makin-tosh, and UNIX systems) from a cellular handset. It is tacit that the remote computer system is running a REMOTE PC server and that it is attached to a system. The cellular customer can see and maneuver the desktop on the cellular handset. No state is stored at the watcher.

This means you can go away your desk, go to one more machine, whether next door or several hundred miles gone, reconnect to your desktop from there and finish the sentence you be typing. Even the cursor will be in the similar position. With a PC X server, if your PC crashes or is restarted, all the distant applications will expire. With REMOTE PC they go on successively.

It is small and simple. The Win32 watcher, for model, is concerning 150K in size and can be run directly from a soft. There is no setting up wanted. It is truly platform-independent. A desktop management on a Linux mechanism may be displayed on a PC. Or a Solaris machine. Or any numeral of other architectures.

The simplicity of the protocol makes it easy to port to fresh platforms. We have a Java watcher, which will sprint in any Java-capable browser.

In a Windows NT server, allowing you to view the desktop of a remote NT machine on any of these platforms using exactly the same viewer

### C. Suppress Network Traffic

The wireless transmission bandwidth available for a cellular phone is limited. Currently; it is 384k bps, even on IMT-2000 based services (only downstream at this transmission rate).

### D. Recover from an unscheduled disconnection

Because of its wireless nature, stable network connectivity cannot be expected. For example, when the user goes into a tunnel or a building, established connections can be lost. In addition, in order to use the same cellular phone to talk to someone, the user must terminate the network connection.

### E. Suppress computational resource use

CPU performance and memory size are limited on a cellular phone to achieve portability and to lower power consumptions

## II. EXISTING SYSTEM

- In the existing system we make use of **BLUETOOTH** to right to use the organization contents in a mobile.
- In this, only particular application can be accessed.
- The files of the system can be alive accessed just within short distances.

## Protecting Cloud Based Multimedia Content Using Signatures

Mr G. Venkatewarlu #1 Ch.Sindhupriya#2

#1 Assistant Professor,Dept of CSE, PBR Visvodaya Institute Of Technology And Science,Kavali,India

#2Student,Dept of Master of Computer Application (MCA), PBR Visvodaya Institute Of Technology And Science ,Kavali,India

### **ABSTRACT**

Web has million of multimedia contents such as videos and images. It may happen that each and every multimedia content has duplicated copies. There are lots of mechanism available that provides easy way for editing, publishing or uploading multimedia contents so that it may leads to security problem and also reduplicating the identity of content owner and also loss of revenue to the content owner. So that this system can be used to protect the Illegally redistributed multimedia contents such as 3D videos or images. The main goal of this system is to provide cost efficiency ,rapid development ,scalability and elasticity to accommodate varying workloads and improve the accuracy as well as computational efficiency and also the reliability. This system can be deployed on public cloud. And this System show high accuracy for more than 11,000 videos and one million of images.

**KEYWORDS:** Reduplication, Signature, Video Copy Detection, Matching, Public Cloud.

### **1.INTRODUCTION**

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing provides an emerging paradigm where computing resources are made available as a service of the Internet. This paradigm provides facility to Customer to Consumer and businesses without installation of this application and provides access to personal files at any computer with internet access.

Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. This also provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Upon these benefits, there are privacy and security concerns too. For the past few years, cloud-based storage has oscillated somewhere between a

# A Multi-Tenant Access Control Scheme for Sharing Resources in Cloud Computing Environments

Rajeswari P.V.N<sup>1</sup>, <sup>2</sup>T. Sahithi\*

<sup>1</sup>Assoc Professor, Dept. of CSE, Visvodaya Engineering College, AP, India.

<sup>2</sup>M.Tech, Dept. of CSE, Visvodaya Engineering College, AP, India.

## **Abstract:**

**Objective:** This paper is aimed to study sharing of resources on the cloud can be achieved on a large scale since it is cost effective and location independent.

**Methods/Statistical analysis:** Despite of the advantages of cloud computing, organizations are still reluctant to deploy their businesses in the cloud computing environment due to concerns in secure resource sharing. In this paper, we propose a **cloud resource mediation service** offered by cloud service providers, which plays the role of trusted third party among its different tenants. This paper formally specifies the resource sharing mechanism between two different tenants in the presence of our proposed cloud resource mediation service.

**Findings:** To evaluate the our proposed method in terms of security, effectiveness, and efficiency each algorithm was modeled, analyzed, and verified using HLPN, and the Z formal language was used to define transition rules. Finally, the properties of the algorithm were verified using the Z3 solver. The outcomes acquired in the wake of executing the solver exhibited that the asserted algorithm explicit access control properties were fulfilled and permits secure execution of privilege activation on the cloud through the CRMS.

**Applications/Improvements:** we will include a comparative analysis of the proposed CTAC model with other state-of-the-art cross domain access control protocols using real-world evaluations.

**Keywords:** Access Control, Revocation, Cloud Computing.

## **1. Introduction**

While there are various advantages managed by the utilization of cloud computing to encourage coordinated effort among clients and associations, security and protection of cloud services and the client information may discourage a few clients and associations from utilizing cloud and remain points important to analysts<sup>1-4</sup>. Regularly, a cloud service provider (CSP) gives a web interface where a cloud client can oversee assets and settings.

In any case, traditional access control models, for example, role based access control<sup>5</sup>, are commonly unfit to enough manage cross-tenant resource get to demands. Specifically, cross-tenant access request present three key difficulties. First, each occupant must have some earlier understanding and learning about the

## **Online location based tourist guide(Trip Advisor) Route Recommendation with Place Of Interest**

**Mr. SRINIVASULU PATHAKAMURI #1**

**Ms. ALEKHYA #2, Ms. SRAVANI #3**

**Ms. KEDARI MOUNIKA #4, Ms. KANUMARLAPUDI CHATURYA #5**

**#1 Assoc., Professor, Dept of CSE Visvodaya Engineering College, Kavali, India**

**#2 Studnet, Dept of CSE, Visvodaya Engineering College, Kavali, India**

**#3 Studnet, Dept of CSE, Visvodaya Engineering College, Kavali, India**

**#4 Studnet, Dept of CSE, Visvodaya Engineering College, Kavali, India**

**#5 Studnet, Dept of CSE, Visvodaya Engineering College, Kavali, India.**

### **ABSTRACT:**

With the popularity of social media (e.g., Facebook and Flicker), users can easily share their check-in records and photos during their trips. In view of the huge number of user historical mobility records in social media, we aim to discover travel experiences to facilitate trip planning. When planning a trip, users always have specific preferences regarding their trips. Instead of restricting users to limited query options such as locations, activities or time periods, we consider arbitrary text descriptions as keywords about personalized requirements. Moreover, a diverse and representative set of recommended travel routes is needed. Prior works have elaborated on mining and ranking existing routes from check-in data. To meet the need for automatic trip organization, we claim that more features of Places of Interest (POIs) should be extracted. Therefore, in this paper, we propose an efficient Keyword-aware Representative Travel Route framework that uses knowledge extraction from users' historical mobility records and social interactions. Explicitly, we have designed a keyword extraction module to classify the POI-related tags, for effective matching with query keywords. We have further designed a route reconstruction algorithm to construct route candidates that fulfil the requirements. To provide befitting query results, we explore Representative Skyline concepts, that is, the Skyline routes which best describe the trade-offs among different POI features. To evaluate the effectiveness and efficiency of the proposed algorithms, we have conducted extensive experiments on real location-based social network datasets, and the experiment results show that our methods do indeed demonstrate good performance compared to state-of-the-art works.

### **1. INTRODUCTION**

Even though there are numerous tourism websites and travel agencies to provide various travel packages, tourists just become puzzled about how to make a choice and neither could they adjust the travel plan. Besides, if tourists try to arrange the travel route by themselves, tremendous information is easy to exhaust them when considering the location interest, visiting

## A SECURE ACCESS CONTROL SCHEME USING CP- ABE and KAE FOR CLOUD DATA SERVICES

**<sup>1</sup>P. SRINIVASULU, <sup>2</sup>SHAIK SAHEERA, <sup>3</sup>CHAVALA MEGANA,**

**<sup>4</sup>LOKESH, <sup>5</sup>MADDINENI BHAVANI**

<sup>1</sup>Assoc. Professor, Dept. of CSE, Visvodaya Engineering College, Kavali, AP, India.

<sup>2,3,4,5</sup>B.Tech, Dept. of CSE, Visvodaya Engineering College, Kavali, AP, India.

**Abstract** – In this paper we consider the cloud based services is an emerging topic. Cloud services provide great connivance to the users, but also bring security problems such as data privacy and sharing. In this paper, we review privacy protection based Access control scheme. In this scheme we separate the cloud consumers into private and public spaces logically. In private space, to secure the read and write access we use both Key Aggregation crypto system for encryption and signature based access control scheme respectively. In public space, we design and implement the a new CP-ABE scheme called attribute authority based CP-ABE scheme with well-organized decryption to avoid the issues of single point of failure and complicated key distribution, and design an efficient attribute revocation method for it.

**Keywords:** Cloud computing, Key aggregation crypto system, Access control, Attribute based signature scheme, revocation method.

### 1. INTRODUCTION

With the rapid expansion of cloud computing, big data and public cloud services have been extensively used. The user can accumulate his

data in the cloud service. Although cloud computing brings enormous expediency to enterprises and users, the cloud computing security has always been a major peril. For users, it is necessary to take full advantage of cloud storage service, and also to warrant data privacy. Therefore, we need to develop an efficient access control solution. Since the conventional access control approach [1] cannot effectively solve the security problems that exist in data sharing. Data security issues brought by data sharing have critically mired the development of cloud computing, various solutions to achieve encryption and decryption of data sharing have been proposed.

In 2007, Bethencourt et al. [2] first proposed the ciphertext policy attribute-based encryption (CP-ABE). However, this scheme does not consider the revocation of access permissions. In 2011, Hur et al. [3] put forward a fine-grained revocation scheme but it can easily cause key escrow issue. Lewko et al. [4] used multi authority ABE (MA-ABE) to solve key escrow issue. But the access policy is not lithe. Li et al [5] presented data sharing system based on systemic attribute encryption, which endows

# International Journal of Research

An ISO : 7021 - 2008 Certified Journal

ISSN NO: 2236-6124 / web : [www.ijrpublisher.com](http://www.ijrpublisher.com) / e-mail : submitijr@gmail.com

Address : C12/7- U/A, Godhni, Nagpur, Maharashtra - 441111

## CERTIFICATE OF PUBLICATION

This is to certify that the paper entitled

“ FILTER UNWANTED MESSAGES FROM OSN USER WALL ”

Authored by

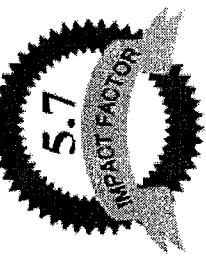
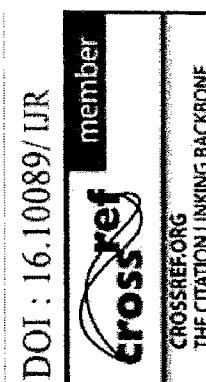
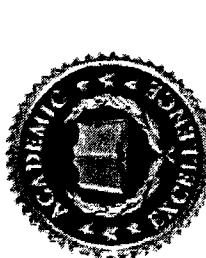
PVN Rajeswari

From

Visvodaya Engineering College ,Kavali,India.

Has been published in

IJR JOURNAL, VOLUME 8, ISSUE 4, APRIL- 2019



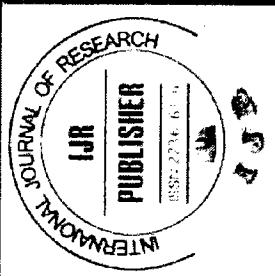
K. V. Kumar S. J.

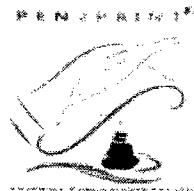
Dr. K. Vikram Kumar Sinha, Ph.D.,

Editor-In-Chief

IJR JOURNAL

[www.ijrpublisher.com](http://www.ijrpublisher.com)





**International Journal of Research (IJR)**

PEN2PRINT®

# **Certificate of Publication**



**Mrs. Bheema Rasagna**

for the paper titled

*An Efficient Multi Keyword Ranked Search over Encrypted Cloud Data*

Published in *International Journal of Research (IJR)*, Vol-06, Issue-04 April 2019

ISSN: 2348-6848

International Refereed and Indexed Journal for Research Publication

With Impact Factor 5.60

Index Copernicus Value (ICV) 100 & Indexed in Thomson Reuters

*S.N. Sharma*

Editor-in-Chief

**International Journal of Research (IJR)**

[www.internationaljournalofresearch.com](http://www.internationaljournalofresearch.com)

Email: [editor@pen2print.org](mailto:editor@pen2print.org)





# Journal of Emerging Technologies and Innovative Research

An International Open Access Journal

www.jetir.org | editor@jetir.org

## Certificate of Publication

The Board of

Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162)

Is hereby awarding this certificate to

**Rajeswari P.V.N**

In recognition of the publication of the paper entitled

**A Multi-Tenant Access Control Scheme for Sharing Resources in Cloud Computing Environments**

Published In JETIR ( www.JETIR.org ) ISSN UGC Approved & 5.87 Impact Factor

Published in Volume 6 Issue 4 , April-2019

*Rajeswari P*

EDITOR

JETIR1904D40

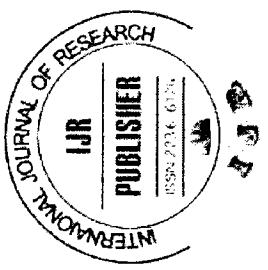
*S. S. S. S. S.*

EDITOR IN CHIEF

Research Paper Weblink <http://www.jetir.org/view?paper=JETIR1904D40>

Registration ID : 199968





# International Journal of Research

An ISO : 7021 - 2008 Certified Journal

ISSN NO: 2236-6124 / web : [www.ijrpublisher.com](http://www.ijrpublisher.com) / e-mail : submitijr@gmail.com

Address : C12/7- UA, Godhni, Nagpur, Maharashtra - 441111

## CERTIFICATE OF PUBLICATION

This is to certify that the paper entitled

“PREDICTION BASED OFFLOADING STRATEGY IN MOBILE CLOUD COMPUTING”

Authored by

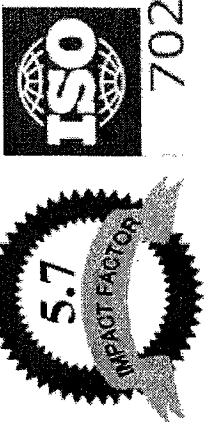
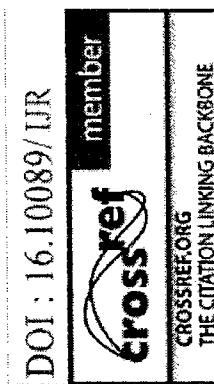
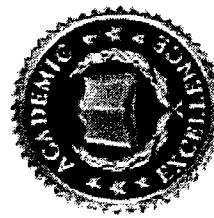
**Mrs. B.Rasagna M.Tech, Assistant Professor**

From

Visvodaya Engineering College, Kavali, Nellore

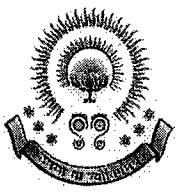
Has been published in

**IJR JOURNAL, VOLUME VIII, ISSUE IV, APRIL- 2019**



International Organization for Standardization  
7021 - 2008

K. V. Kumar,  
Dr. K. Vikram Kumar Sinha, Ph.D.,  
Editor-In-Chief  
IJR JOURNAL  
[www.ijrpublisher.com](http://www.ijrpublisher.com)



**PARVATHAREDDY BABUL REDDY**  
**VISVODAYA INSTITUTE OF TECHNOLOGY & SCIENCE**  
(Affiliated to J.N.T.U.A, Approved by AICTE and Accredited by NAAC with 'A' Grade)  
**KAVALI – 524201, S.P.S.R Nellore Dist., A.P. India. Ph: 08626-243930**



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**List of Publications of faculty for the academic year 2017-2018**

S.No	Name of the Faculty	Title of the Paper	Journal Name and ISBN/ISSN	Vol.No. Issue No./Page No.	Month & Year	Link for relevant document
1	P.V.N.Rajeswari	Context Based Diversification For Keyword Queries Over XML Data	International Journal of Scientific Engineering and Technology Research& ISSN : 2319-8885	Vol.06 Issue.20	June 2017	<a href="http://ijestr.com/uploads/125436IJESTR14847-723.pdf">http://ijestr.com/uploads/125436IJESTR14847-723.pdf</a>
2	P. Eswaraiah	A Novel Approach For NKS Scheme In High Dimensional Data	International Journal of Creative Research Thoughts&ISSN:2320-2882	Vol.No.5 Issue No.4	August 2017	<a href="https://ijcrt.org/papers/IJCRT1704073.pdf">https://ijcrt.org/papers/IJCRT1704073.pdf</a>
3	J. Vamsinath	Extracting Query Facets From Search Results Using QD MINER	International Journal of Creative Research Thoughts&ISSN:2320-2882	Vol.No.05 Issue No.04	August 2017	<a href="https://ijcrt.org/papers/IJCRT1704043.pdf">https://ijcrt.org/papers/IJCRT1704043.pdf</a>
4	Dr.V.V.Sunil Kumar	Rapid Image Searching Approximate Methodology For Large Scale Storage System	International Journal of Creative Research Thoughts&ISSN:2320-2882	Vol.No.5 Issue No.4	August 2017	<a href="https://core.ac.uk/download/pdf/234676962.pdf">https://core.ac.uk/download/pdf/234676962.pdf</a>
5	P.V.N.Rajeswari	Implementing Intrusion Detection System Using Feature Selection And Classification Technique	International Journal Creative Research Thoughts & ISSN :2320-2882	Vol.No.5 Issue No.4	October 2017	<a href="https://ijcrt.org/papers/IJCRT1704075.pdf">https://ijcrt.org/papers/IJCRT1704075.pdf</a>
6	P.V.N.Rajeswari	Improving Efficiency Using Q-Statistics And FS Algorithm In High Dimensional Datasets	International Journal Creative Research Thoughts &ISSN :2320-2882	Vol .No.4 Issue No.3	October 2017	<a href="https://ijcrt.org/viewfull.php?&amp;p_id=IJCRT1704074">https://ijcrt.org/viewfull.php?&amp;p_id=IJCRT1704074</a>
7	R. Konda Reddy	Trust Factor And Fuzzy-Firefly Integrated Particle Swarm Optimization Based Intrusion Detection And Prevention System For Secure Routing Of MANET	International Journal of Computer Networks and Communications &DOI:10.5121	Vol.No.10 Issue No.1	January 2018	<a href="https://core.ac.uk/download/pdf/189124282.pdf">https://core.ac.uk/download/pdf/189124282.pdf</a>
8	P.V.N.Rajeswari	Online Parametric And Non-Parametric Drift Detection Techniques For Streaming	International Journal of Current Engineering and Scientific Research - ISSN : 2394-0697	Vol.No.5 Issue No.3	03&2018	<a href="http://troindia.in/journal/ijcesr/vol5iss3part3/45-53.pdf">http://troindia.in/journal/ijcesr/vol5iss3part3/45-53.pdf</a>
9	R. Konda Reddy	Trust And Fuzzy-Ant Colony Optimization Based Intrusion Detection System For Secure Routing Of manet	International Journal of Computer Science and Mobile Computing&ISSN:2320-088X	Vol.No.7 Issue No.4 Page No.59-75	April 2018	<a href="https://ijcsmc.com/docs/papers/April2018/V7I4201807.pdf">https://ijcsmc.com/docs/papers/April2018/V7I4201807.pdf</a>
10	R. Konda Reddy	Trust Based Genetic Neuro-Fuzzy System For Intrusion Detection And Self Adaptive Swarm Optimization Algorithm For Secure Routing In Manet With Firefly Integrated	International Journal of Applied Engineering Research ISSN:0973-4562	Vol.No.13 Issue No.8 Page No.5722-5735	April 2018	<a href="https://www.ripublication.com/ijaer18/ijaer_v13n8_21.pdf">https://www.ripublication.com/ijaer18/ijaer_v13n8_21.pdf</a>

Faculty Incharge

D  
HOD

Head of Department

COMPUTER SCIENCE ENGINEERING  
 CONVENTIONAL METHODS OF TECHNOLOGY & SCIENCE  
 X AVAIL 1

## Context-Based Diversification for Keyword Queries Over XML Data

K. MANASA<sup>1</sup>, P.V.N. RAJESWARI<sup>2</sup>

<sup>1</sup>PG Scholar, Dept of CSE, Viswodaya Engineering College, Kavali, AP, India, E-mail: chinnimanasa143@gmail.com.

<sup>2</sup>Associate Professor, Dept of CSE, Viswodaya Engineering College, Kavali, AP, India.

**Abstract:** In searching process user enter particular candidate searching keyword and with the help of searching algorithm respective searching query is executed on targeted dataset and result is return as an output of that algorithm. In this case it is expected that meaningful keyword has to be entered by user to get appropriate result set. In case of confusing bunch of keywords or ambiguity in it or short and indistinctness in it causes an irrelevant searching result. Also searching algorithms works on exact result fetching which can be irrelevant in case problem in input query and keyword. This problem statement is focused in this system. By considering the keyword and its relevant context in XML data, searching should be done using automatically diversification process of XML keyword search. In this way system may satisfy user, as user gets the analytical result set based on context of searching keywords. For more efficiency and to deal with big data, HADOOP platform is used. Baseline efficient algorithms are proposed to incrementally compute top-k qualified query candidates as the diversified search intentions. Compare selection criteria are targeted: the k selected query candidates are most relevant to the given query while they have to cover maximal number of distinct results on real and synthetic data sets demonstrates the effectiveness diversification model and the efficiency of algorithms.

**Keywords:** XML Keyword Search, Context-Based Diversification.

### I. INTRODUCTION

Keyword search on structured and semi-structured data has attracted much research interest recently, as it enables common users to retrieve information from such structured data sources without the need to learn sophisticated query languages and database structure. In general, the more keywords a given keyword query contains, the easier the search semantics of the keyword query can be identified. However, when the given keyword query only contains a small number of vague keywords, it will become a very challenging problem to derive the search semantics of the query due to the high ambiguity of this type of keyword queries. Although Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Sometimes user involvement is helpful to identify search semantics of keyword queries, it is not always applicable to rely on users because the keyword queries may also come from system application. In this application case, web or database search engine may need to automatically compute the search semantics of short and frequent keyword queries only based on the data to be searched. The derived search semantics will be maintained and updated in an off-line way. Once a keyword query is issued by the real users, its corresponding search semantics can be directly used to

make an instant response. In this paper, we mainly pay attention to the problem of effectively deriving the search semantics of keyword queries with the consideration of data only, which does not receive much closer attention in the previous works.

**Table 1. Top 10 Selected Feature Terms of q**

keyword	features
database	systems; relational; protein; distributed; oriented; image; sequence; search; model; large.
query	language; expansion; optimization; evaluation; complexity; log; efficient; distributed; semantic; translation.

### II. LITERATURE SURVEY

#### 1. Xrank: Ranked keyword search over xml documents

**AUTHORS:** L.Guo, F. Shao, C. Botev, and J. Shanmugam-sundaram We consider the problem of efficiently producing ranked results for keyword search queries over hyperlinked XML documents. Evaluating keyword search queries over hierarchical XML documents, as opposed to (conceptually) flat HTML documents, introduces many new challenges. First, XML keyword search queries do not always return entire documents, but can return deeply nested XML elements that contain the desired keywords. Second, the nested structure of XML implies that the notion of ranking is no longer at the granularity of a document, but at the granularity of an XML element. Finally, the notion of

# A NOVEL APPROACH FOR NKS SCHEME IN HIGH DIMENSIONAL DATA

<sup>1</sup>Eswaraiah Puttu, <sup>2</sup>Shaik Shameer

<sup>1</sup>Asso. Professor in Dept. of CSE, PBR Visvodaya Institute of Technology & Science, Kavali, and Andhra Pradesh, India.

<sup>2</sup>M.Tech, Dept. of CSE, PBR Visvodaya Institute of Technology & Science, Kavali, and Andhra Pradesh, India.

**Abstract** – Consider objects that are tagged with keywords and are embedded in a vector space. The presence of keywords in feature space allows for the development of new tools to query and explore these multi-dimensional datasets. We propose a method called Projection and Multi Scale Hashing that uses random projection and hash-based index structures, and achieves high scalability and speedup. In multi-dimensional spaces, it is difficult for users to provide meaningful coordinates, and our work deals with another type of queries where users can only provide keywords as input. Images are represented using color feature vectors, and usually have descriptive text information (e.g., tags or keywords) associated with them. Our system is based on real datasets shows that we can show the efficient searching of keywords in multidimensional datasets.

**Key Words:** Querying, Multi-dimensional Data, Indexing, Hashing.

## I. INTRODUCTION

In today's digital world the amount of data which is developed is increasing day by day. There is different multimedia in which data is saved. It's very difficult to search the large dataset for a given query as well to archive more accuracy on user

query. In the same time query will search on dataset for exact keyword match and it will not find the nearest keyword for accuracy. Ex: Flickr.

The amount of data which is developed is increasing day by day, thus it is very difficult to search large dataset for a given query as well to achieve more accuracy on user query. So we have implemented a method of efficient search in multidimensional dataset. This is associated with images as an input. Images are often characterized by a collection of relevant features, and are commonly represented as points in a multi-dimensional feature space. For example, images are represented using colour feature vectors, and usually have descriptive text information (e.g., tags or keywords) associated with them. We consider multi-dimensional datasets where each data point has a set of keywords. The presence of keywords in feature space allows for the development of new tools to query and explore these multi-dimensional datasets.

Our main contributions are summarized as follows.

- (1) We propose a novel multi-scale index for exact and approximate NKS query processing.

# Extracting Query Facets from Search Results Using QD Miner

J. Vamsinath, D.Bhavana

Associate Professor, Dept. of CSE, PBRVITS, Kavali, India  
M.Tech Student 2nd year, Dept. of CSE, PBR VITS, Kavali, India

**ABSTRACT:** Now A days we are facing one problem that is data extraction from large amount of data set. for that problem here I am providing one solution ie query facets As an example, for the question "stuff remittance", these gatherings may be diverse aircrafts, distinctive flight sorts (local, global), or distinctive travel classes (in the first place, business, economy). I name these gatherings inquiry aspects and the terms in these gatherings feature terms. I build up a directed approach in view of a graphical model to perceive inquiry aspects from the uproarious hopefuls found. The graphical model figures out how likely a competitor term is to be an aspect term and additionally how likely two terms is to be assembled together in an inquiry feature, and catches the conditions between the two components. An inquiry aspect can be gotten by totaling the noteworthy records. The question aspect motor will consequently get the features related with an inquiry. Seeking will be less demanding with the assistance of aspects .It likewise includes the idea of regular thing mining. The features are allocated weightage esteem. Keeping in mind the end goal to show the features in need savvy way utility mining idea is additionally incorporated with it. It enhances the looking

## INTRODUCTION

Here I am tackle the problem of finding query facets. A query facet is a set of items which explain and summarize one significant aspect of a query. Here a facet item is typically a word or a phrase. A query may have various facets that summarize the information about the query from different perspectives. Table 1 shows sample facets for some queries. Facets for the query —watches— cover the information about watches in five distinctive aspects, as well as brands, gender categories, sustaining features, styles, and colors. The query —visit Beijing— has a query facet about trendy resorts in Beijing (Tiananmen square, forbidden city, summer palace, ...) and a facet on tour related topics (attractions, shopping, dining, ...). Query facets provide remarkable and useful information about a query and thus can be used to get better search experiences in many ways. First, we can present query facets together with the original search results in a suitable way. Thus, users can understand some significant aspects of a query without browsing tens of pages. For example, a user could study different brands and categories of watches. We can also apply a faceted search based on the mined query facets. User can make clear their specific intent by selecting facet items. Then search outcome could

# Rapid Image Search Using Approximate Methodology for Large-Scale Storage Systems

V.V.Sunilkumar, Nunna Sai Sindhura

Associate Professor, Dept. of CSE, PBRVITS, Kavali, India

M.Tech Student 2<sup>nd</sup> year, Dept. of CSE, PBR VITS, Kavali, India

**Abstract** In this paper I propose a near-real-time and cost-effective semantic queries based methodology, called FAST. The thought behind FAST is to investigate and misuse the semantic connection inside and among datasets through relationship mindful hashing and sensible level organized tending to altogether decrease the preparing inertness, while acquiring acceptably little loss of information look exactness. The close continuous property of FAST enables quick ID of corresponded records and the critical narrowing of the extent of information to be prepared. FAST supports a few sorts of information examination, which can be executed in existing accessible stockpiling frameworks. We direct a certifiable utilize case in which youngsters detailed missing in a to a great degree swarmed condition (e.g., a very well known beautiful spot on a pinnacle traveler day) are recognized in a convenient mold by breaking down 60 million pictures utilizing FAST. Quick is additionally enhanced by utilizing semantic-mindful namespace to give

dynamic and versatile namespace administration for ultra-huge capacity frameworks. Broad trial comes about exhibit the productivity and adequacy of FAST in the execution upgrades.

**Index Terms**—Cloud storage, data analytics, real-time performance, semantic correlation

## 1. Introduction

Storage frameworks are confronting extraordinary difficulties in dealing with the records from numerous information escalated application, for example, business exchanges, logical registering, and interpersonal organization networks, portable applications, data perception, and distributed computing. Roughly 800 Exabyte of information were made in 2009 alone. As indicated by a current study, 1,780 server farm in 26 nations. The progressive catalog tree based metadata administration conspire utilized as a part of all record frameworks today. The most imperative elements of namespace administration are document ID and query File framework namespace as a data

# Implementing Intrusion Detection System Using Feature Selection and Classification Technique

<sup>1</sup>P.V.N Rajeswari, <sup>2</sup>Nataraja Sirisha

<sup>1</sup>Assoc. Professor in Dept. of CSE, Visvodaya Engineering College, Kavali, and Andhra Pradesh, India.

<sup>2</sup>M.Tech, Dept. of CSE, Visvodaya Engineering College, Kavali, and Andhra Pradesh, India.

**Abstract** – With the growth of Internet, there has been a tremendous increase in the number of attacks and therefore Intrusion Detection Systems (IDS's) has become a main stream of information security. The purpose of IDS is to help the computer systems to deal with attacks. This anomaly detection system creates a database of normal behaviour and deviations from the normal behaviour to trigger during the occurrence of intrusions. Based on the source of data, IDS is classified into Host based IDS and Network based IDS. In network based IDS, the individual packets flowing through the network are analyzed where as in host based IDS the activities on the single computer or host are analyzed. The feature selection used in IDS helps to reduce the classification time. In this paper, the IDS for detecting the attacks effectively has been proposed and implemented. For this purpose, a new feature selection algorithm called Optimal Feature Selection algorithm based on Information Gain Ratio has been proposed and implemented. This feature selection algorithm selects optimal number of features from KDD Cup dataset. In addition,

two classification techniques namely Support Vector Machine and Rule Based Classification have been used for effective classification of the data set. This system is very efficient in detecting DoS attacks and effectively reduces the false alarm rate. The proposed feature selection and classification algorithms enhance the performance of the IDS in detecting the attacks.

**Keywords :** Intrusion Detection; Information Gain; Support Vector Machine; Feature Selection Technique and Classification

## I. INTRODUCTION

Computers have been networked together with very large user source and so security has been a vital concern in many areas. With the rapid growth of internet communication and availability of tools to intrude the network, security for network has become indispensable. Current security policies do not sufficiently guard the data stored in the databases. Many other technologies like firewalls, encryption and authorization mechanisms can offer security, but they are

# Improving Efficiency Using Q-Statistics and FS Algorithm in High Dimensional Datasets

<sup>1</sup>P.V.N Rajeswari, <sup>2</sup>Nataraja Priyanka

<sup>1</sup>Assoc. Prof in Dept. of CSE, PBR Visvodaya Institute of Technology & Science, Kavali, AP, India.

<sup>2</sup>M.Tech, Dept. of CSE, PBR Visvodaya Institute of Technology & Science, Kavali, AP, India.

**Abstract –** Classification problems in high dimensional data with small number of observations are becoming more common especially in microarray data. The increasing amount of text information on the Internet web pages affects the clustering analysis [1]. The text clustering is a favorable analysis technique used for partitioning a massive amount of information into clusters. Hence, the major problem that affects the text clustering technique is the presence uninformative and sparse features in text documents. A broad class of boosting algorithms can be interpreted as performing coordinate-wise gradient descent to minimize some potential function of the margins of a data set [1]. This paper proposes a new evaluation measure Q-statistic that incorporates the stability of the selected feature subset in addition to the prediction accuracy. Then we propose the Booster of an FS algorithm that boosts the value of the Q statistic of the algorithm applied.

**Keywords:** High dimensional data classification; feature selection; stability; Q-statistic; Booster;

## I. INTRODUCTION

The presence of high dimensional data is becoming more common in much practical application such as data mining, machine learning and micro array gene expression data analysis. Typical publicly available microarray data has tens of thousands of features with small sample size and the size of the features considered in microarray data analysis is growing[1][2]. Recently, after the increasing amount of digital text on the Internet web pages, the text clustering (TC) has become a hard technique used to clustering a massive amount of documents into a subset of clusters. It is used in the area of the text mining, pattern recognition and others. Vector Space Model (VSM) is a common model used in the text mining area to represents document components. Hence, each document is represented as a vector of terms weight, each term weight value is represented as a one dimension space. Usually, text documents contain informative and Uninformative features, where an uninformative is as irrelevant, redundant, and uniform distribute features. Unsupervised feature section (FS) is an important task used to find a new subset of informative features to improve the TC algorithm.

# TRUST FACTOR AND FUZZY-FIREFLY INTEGRATED PARTICLE SWARM OPTIMIZATION BASED INTRUSION DETECTION AND PREVENTION SYSTEM FOR SECURE ROUTING OF MANET

Ramireddy Kondaiah<sup>1</sup> and Bachala Sathyanarayana<sup>2</sup>

<sup>1</sup>Research Scholar, Department of Computer Science, Rayalaseema University, Kurnool ,A.P,India.& Associate Professor, Dept of CSE, PBRVITS, Kavali, Andhra Pradesh , India.

<sup>2</sup>Professor in Computer Science &Technology ,Sri Krishnadevaraya University, Anantapur, A.P, India.

## ABSTRACT

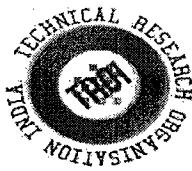
*Mobile Ad hoc Networks (MANET) is one of the rapidly emanating technologies, which has gained attention in a wide range of applications in the fields of military, private sectors, commercials and natural calamities. Securing MANET is a dominant responsibility, and hence, a trust factor and fuzzy based intrusion detection and prevention system is proposed for routing in this paper. Based on the trust values of the nodes, the fuzzy system identifies the intruder, such that the path generated in the MANET is secured. Moreover, an optimization algorithm, entitled Fuzzy integrated Particle Swarm Optimization (Fuzzy-FPSO), is proposed by the concatenation of the Firefly Algorithm (FA) and Particle Swarm Optimization (PSO) for the optimal path selection in order to provide secure routing. The simulation of the proposed methodology is NS2 simulator and analysis is carried out considering four cases, like without attack, flooding attacks, black hole attack and selective packet drop attack concerning throughput, delay and detection rate. The remarkable evaluation measures of the proposed Fuzzy-FPSO are the maximal throughput of 0.634, minimal delay of 0.044 , maximal detection rate of 0.697 and minimal routing overhead of 0.24550 And the evaluation measure for the case without any attacks are the maximal throughput of 0.762, minimal delay of 0.029 ,maximal detection rate of 0.805 and minimal routing overhead of 0.11511.*

## KEYWORDS

*MANET, Routing, Trust, Fuzzy system, Firefly Algorithm, Particle Swarm Optimization.*

## 1. INTRODUCTION

The wireless communication network is available in many modes with the hasty technology evolution. Because of the omnipresent existence of remarkable factors, like scalability and mobility, the wireless networks [1] are preferred compared to the wired network. One of the crucial applications of the wireless network is the Mobile Ad-hoc Network (MANET), which has uninterrupted self-configuration, self-maintenance and framework-less network for mobile gadgets interlinked without wires [2]. A MANET is a collection of heterogeneous, self-organized and battery powered mobile nodes with varying availability of resources and computation capacity [5]. The communication of data between these nodes is established with the help of neighbors either directly or indirectly without utilizing the support of any central coordinator or permanent framework [6]. MANET is extensively used when the components or mobile nodes are not within the similar transmission range. Single-hop network and multi-hop network are the two types of networks; A network which provides direct communication between nodes existing within the same range is named single-hop network. It doesn't require any intermediate node,



## ONLINE PARAMETRIC AND NON PARAMETRIC DRIFT DETECTION TECHNIQUES FOR STREAMING DATA IN MACHINE LEARNING: A REVIEW

P.V.N. Rajeswari<sup>1</sup>, Dr. M. Shashi<sup>2</sup>

<sup>1</sup>Assoc. Professor, Dept of Comp. Sc. & Engg., Visvodaya Engineering College, Kavali, AP, India

<sup>2</sup>Professor, Dept of Comp. Sc. & System Engg, Andhra University, Visakhapatnam, AP, India

### Abstract

Enormous amount of data streams are generated by large number of real time applications with the stupendous advancement in technology. Incremental and online - offline learning algorithms are more relevant to process the data streams in the data mining context. Detecting the changes and reacting against them is an interesting research area in current era in knowledge discovery process, in Machine Learning. The target function also is changed frequently, due to the occurrence of changes in data streams. This is an intrinsic problem of online learning, popularly known as Concept Drift. To handle the problem despite of the learning model, novel methods are needed to examine the performance metrics. This examination will be done during the learning process and prompt drift signals whenever a significant variation has been detected. The Concept Drift problem can be detected using various techniques. This paper focuses on reviewing on existing Parametric and non-Parametric techniques Online for drift detection.

**Keywords:** Stream mining; Concept drift; Parametric; Non-parametric; Machine Learning;

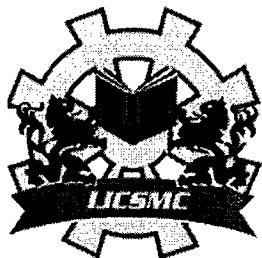
### I. INTRODUCTION

Adaptation of science and technological outcomes including computerization in every walk of life leads to accumulation of voluminous amount of data that need to be processed by machines for pattern extraction for its effective usage. Machine Learning algorithms are widely

applied in the areas like, image processing, data mining, medical diagnosis, search engines, etc. Machine learning categorized into two types namely Batch learning and Online learning based on representation and presentation of training samples. Batch learning systems accept a large number of examples and learn to build a model from all of them at once. In contrast, Online learning systems are given examples sequentially as streaming data [1] from which learning happens incrementally.

Learning from data streams aims to capture the target concept as it changes over time, and it is a current research area of growing interest. For instance, changes can emerge due to changing interests of people towards news topics, shopping preferences, energy consumption, etc. (e.g. influenced by seasonal changes). Spam filtering [2] is another example, wherein spammers try to elude filters by disguising their emails as genuine with newer tricks challenging spam filters to continuously enhance their capability to successfully identify spam over time. So it is possible that a learning model previously induced may be incompatible with the present data, making an update mandatory. This type of problem is commonly known as Concept Drift. Many online learning algorithms[18], which are variants of the base models such as Rule-based systems, Decision Trees, Naive Bayes, Support Vector Machines, Instance based learning, and ensemble of classifiers [3] [4], have been implemented for handling Concept Drift.

## **International Journal of Computer Science and Mobile Computing**



A Monthly Journal of Computer Science and Information Technology

**ISSN 2320-088X**

**IMPACT FACTOR: 6.017**

*IJCSMC, Vol. 7, Issue. 4, April 2018, pg.59 – 75*

# **Trust and Fuzzy- Ant Colony Optimization based Intrusion Detection System for Secure Routing of MANET**

**Ramireddy Kondaiah<sup>1</sup>, Dr. Bachala Sathyanarayana<sup>2</sup>**

<sup>1</sup>Research Scholar (PP COMP.SCI-053), Department of Computer Science, Rayalaseema University, Kurnool, Andhra Pradesh, India, E-Mail: [rkondareddy75@gmail.com](mailto:rkondareddy75@gmail.com)

<sup>2</sup>Professor in Computer Science & Technology, Sri Krishnadevaraya University, Anantapur, Andhra Pradesh, India, E-Mail: [bachalasatya@yahoo.com](mailto:bachalasatya@yahoo.com)

---

**Abstract:** *Mobile Ad-Hoc Network (MANET) is a specific type of wireless network that is infrastructure less, dynamic and self-organizing and self-configuring multi-hop wireless network. Nodes are mobile and therefore nodes can join or leave the network at any time. Routing in Ad-hoc networks is a challenging task due to mobility of nodes. Security in Mobile Ad hoc Network (MANET) is one of the key challenges due to its special features e.g. hop-by-hop communications, dynamic topology, and open network boundary that received tremendous attention by researchers. Traditional security methods are not applicable in MANET due to its special properties. Mobile Ad hoc Networks (MANETs) are vulnerable to various kinds of attacks due to their dynamic nature and lack of a central point of control. In this paper, we propose a hybrid approach named as Trust and Fuzzy -Ant Colony Optimization(TFACOIDS) based Intrusion Detection System for secure routing of MANET. This technique involves the detection of attacker level of the nodes in the network layers such as MAC layer, physical layer and routing layer using fuzzy logic technique. Based on the detected attacker level, the trust value of each node is updated. When source node wants to transmit a data packet to the destination, the route with trustworthy nodes is selected using swarm based ant colony optimization (ACO) technique. By simulation results, we show that proposed technique enhances the secured data communication.*

**Keywords:** *MANET, Ant Colony Optimization, Fuzzy, Trust*

---

# Trust based Genetic Neuro-Fuzzy System for Intrusion Detection and Self Adaptive Firefly integrated Particle Swarm Optimization Algorithm for Secure Routing in MANET

Ramireddy Kondaiah<sup>1</sup> and Dr. Bachala Sathyanarayana<sup>2</sup>

<sup>1</sup>Research Scholar ((PP COMP.SCI-053), Department of Computer Science, Rayalaseema University, Kurnool, Andhra Pradesh, India.

<sup>2</sup>Professor in Computer Science & Technology, Sri Krishnadevaraya University, Anantapur, Andhra Pradesh, India.

## Abstract

Mobile Ad hoc Network (MANET), which is comprised of a number of self-organized and battery equipped mobile nodes, is used widely in various applications, including military and private sectors. However, security is a major issue in MANET routing, as the network is prone to attacks. This paper introduces the intrusion detection scheme for establishing the secured path in MANET. Here, the presence of intruder in network is identified with the use of genetic neuro-fuzzy system, and various trust factors. Then, the possible paths between the source and the destination through the trust nodes are generated. The work aims to identify the secured paths from the possible paths through the proposed Self Adaptive Firefly based Particle Swarm Optimization (SA-FPSO) Algorithm. Finally, the secured paths are generated between the source and the destination for data communication. Simulation environment for implementing the proposed scheme is developed with the NS2 simulator, and evaluated by introducing network attacks, such as black hole, flooding, and selective packet drop attack. Simulation results reveal that the proposed SA-FPSO scheme outclassed existing works with the values of 0.04319 sec, 0.691, and 0.769 for delay, detection rate, and throughput, respectively, while the MANET is under black hole attack.

## INTRODUCTION

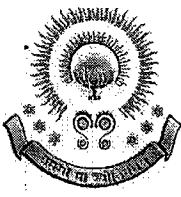
MANET has the dynamic topology and the nodes present in the network do not provide proper structure to the network, and thus, it may suffer from various network attacks [1]. MANET contains several nodes freely distributed over the wireless medium. The data is passed from the source node to the destination node through various set of intermediate nodes, and the communication between the nodes can be referred as hopping. Based on the communication, the MANET comes under two categories; they are single hop network, and multi hop network [3]. Various routing algorithms come in handy for establishing the routing path between the source and the destination for data transmission.

The MANET nodes have large separation distance and limited battery life. Thus, establishing the routing path helps in improving the speed and efficiency of communication. One of the major factors affecting the path establishment is the network attacks [4]. Network attacks affect both the routing

mechanism and the security mechanism. Further, it comes under the category of passive attack and active attack. Passive attack does not pose a greater threat to the network, whereas the active attacks change the data transfer [10]. Handling the security threats occurring in MANET can be done through Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). IDS identify the malicious nodes in network, whereas the IPS prevents the system from security threats and allows secured data transmission [1]. Formerly, IDS detects the malicious activity in the node through anomaly detection and misuse detection. IDS can be defined as the reactive defence mechanism, which offers defence to MANET through early detection of network attacks [15] [16]. IDS helps in providing secured nodes for routing protocol and thereby, establish a secured path between the source and the destination [11].

IDS design parameters, such as routing nature of the protocols, mobility of the nodes, lack of centralized control and limited bandwidth act as factors for the presence of malicious nodes in MANET [1]. DoS attack specifies the isolation of node from the network, which results in packet dropping, by modifying the data packets transferred between source and destination. DoS attacks result in route disruption, data rejection, and data depletion. DoS attacks in the MANET come under different categories, namely wormhole attack, blackhole attack, and greyhole attack, respectively [13] [14]. Wormhole attack happens when two or more malicious nodes establish a private channel between them [4]. The black hole attack [17] attracts the traffic by providing false routing information, and upon data reception, it drops the data packets. The black hole attack drops most of data and hence, referred as full data dropping attack. The greyhole attack [18] is similar to the black hole attack, but drops partial data. Greyhole attack is also referred as partial data dropping attack [12]. Sybil attacks create identity of physical device to launch a coordinate attack on the network, and this weakens the detection process [10].

In several literature schemes, both the qualities of IDS and IPS are utilized, to develop the Intrusion Detection and Prevention Scheme (IDPS) [1]. Recently, developed routing algorithms have neglected the IDS and thus, failed to provide secured routing path. As the security is one of the important design parameters, inclusion of IDS scheme along with the routing algorithm improves the overall efficiency of the MANET [2]. Several works used the classification scheme for classifying the normal nodes from the malicious nodes. In [6], SVM scheme



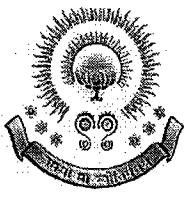
**PARVATHAREDDY BABUL REDDY**  
**VISVODAYA INSTITUTE OF TECHNOLOGY & SCIENCE**  
(Affiliated to J.N.T.U.A, Approved by AICTE and Accredited by NAAC with 'A' Grade)  
**KAVALI – 524201, S.P.S.R Nellore Dist., A.P. India. Ph: 08626-243930**



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**List of Publications of faculty for the academic year 2016-2017**

S.No	Name of the Faculty	Title of the Paper	Journal Name and ISBN/ISSN	Vol.No. Issue No. Page No.	Month & Year	Website link
1	Dr.V V Sunil kumar	A Real Time Prototype For Vehicle Tracking And Alerting System	International Journal of Innovative Technology And Research&ISSN:2319-1058	Vol.No.7 Issue No.1 Page No.	June 2016	<a href="http://www.ijatir.org/uploads/326514IJATIR9248-104.pdf">http://www.ijatir.org/uploads/326514IJATIR9248-104.pdf</a>
2	G.Venu Gopal	Fast Mining Approach For Automatic Recognition Of Rare Raga Swaram Notes	International Journal of Innovative Technology And Research&ISSN:2319-1058	Vol.No.7 Issue No.1 Page No.	June 2016	<a href="http://ijiet.com/wp-content/uploads/2016/07/89.pdf">http://ijiet.com/wp-content/uploads/2016/07/89.pdf</a>
3	J. Vamsinath	Efficient Mining of Top-K High Utility Itemsets From Uncertain Databases	International Journal of Computer science and Information Security&ISSN:1947-5500	Vol.No.14 Issue No. Page No.	Oct 2016	<a href="https://www.academia.edu/29176545/Efficient_Mining_Of_Top_K_High_Utility_Itemsets_From_Uncertain_Databases">https://www.academia.edu/29176545/Efficient_Mining_Of_Top_K_High_Utility_Itemsets_From_Uncertain_Databases</a>
4	P.V.N. Rajeswari	iOVDFT for Concept Drift problem in Big Data	A National Conference in Advanced Trends in Computer Science and Information	Vol.No.4 Issue No.8 Page No.	Oct 2016	<a href="http://www.ijcstjournal.org/volume-4/issue-5/IJCST-V4I5P47.pdf">http://www.ijcstjournal.org/volume-4/issue-5/IJCST-V4I5P47.pdf</a>
5	K.Sireesha	Neighbouring Active Virus Triage By Software Facts Discount Methods	International Journal of Advanced Technology and Innovative Research&ISSN:2320-5547	Vol.No.05 Issue No.1 Page No.5374-5376	Jan 2017	<a href="https://www.ijitr.com/index.php/ojs/article/view/1501/pdf">https://www.ijitr.com/index.php/ojs/article/view/1501/pdf</a>
6	M.Vijaya Bhaskar	Endangered Information Combination Technique For Wireless Sensor Networks In The Occurrence Of Collusion Attacks	International Journal of Innovative Technology And Research&ISSN:2320-5547	Vol.No.05 Issue No.1 Page No.5368-5370	Jan 2017	<a href="http://www.ijitr.com/index.php/ojs/article&gt;download&gt;pdf">www.ijitr.com&gt;index.php&gt;ojs&gt;article&gt;download&gt;pdf</a>
7	SK.Shabbir Basha	Confidentiality Destructive And Dishonest Discovery Of Packet Falling Assaults In Wireless AD HOC Networks	International Journal of Innovative Technology And Research&ISSN:2320-5547	Vol.No.05 Issue No.1 Page No.5471-5473	Jan 2017	<a href="http://www.ijitr.com/index.php/ojs/article&gt;view">www.ijitr.com&gt;index.php&gt;ojs&gt;article&gt;view</a>
8	M.Janardhan	Protected Spatial Best-Key Request Handling Via Confidential Location-Based Service Sources	International Journal of Advanced Technology and Innovative Research&ISSN:2320-5574	Vol.No.05 Issue No.01 Page No.5371-5373	Jan 2017	<a href="https://www.ijitr.com/index.php/ojs/article/view/1500/pdf">https://www.ijitr.com/index.php/ojs/article/view/1500/pdf</a>



**PARVATHAREDDY BABUL REDDY**  
**VISVODAYA INSTITUTE OF TECHNOLOGY & SCIENCE**  
(Affiliated to J.N.T.U.A, Approved by AICTE and Accredited by NAAC with 'A' Grade)  
KAVALI – 524201, S.P.S.R Nellore Dist., A.P. India. Ph: 08626-243930



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

9	J. Vamsinath	Secure Data Integrity in Privacy Preserving Mobile Health Monitoring using Cost Efficient Clouds	International Journal of Advanced Technology and Innovative Research&ISSN:2348-2370	Vol.No.09 Issue No.01 Page No.0023-0025	Jan 2017	<a href="http://www.ijatir.org/uploads/145326IJATIR13420-04.pdf">http://www.ijatir.org/uploads/145326IJATIR13420-04.pdf</a>
10	Dr.V.V.Sunil Kumar	Improving Routing Performance In Manets Using Proactive Route Maintaintance	International Journal of Advanced Research in Computer Science and Software Engineering	Vol.No.III Issue No.3	Mar 2017	<a href="https://www.worldwidejournals.com/indian-journal-of-applied-research(IJAR)/fileview/March 2017 1491813244_152.pdf">https://www.worldwidejournals.com/indian-journal-of-applied-research(IJAR)/fileview/March 2017 1491813244_152.pdf</a>

Faculty Incharge

  
HOD

Head of Department  
**COMPUTER SCIENCE ENGINEER**  
Visvodaya Institute of Technology & Science  
KAVALI - 524 201, S.P.S.R. Nellore |

## **A Real Time Prototype for Vehicle Tracking and Alerting System**

**V. V. SUNIL KUMAR**

Dept of CSE, PBR Visvodaya Institute of Technology and Science, Kavali, Nellore, AP, India,  
E-mail: sunil.vemula1981@gmail.com.

**Abstract:** A vehicle tracking system is an electronic device installed in a vehicle to enable the owner or a third party to track the vehicle's location. This paper proposed to design a vehicle tracking system that works using GPS and GSM technology, which would be the cheapest source of vehicle tracking and it would work as anti-theft system. For doing so an ARM7/89C52 microcontroller is interfaced serially to a GSM Modem and GPS Receiver. A GSM modem is used to send the position (Latitude and Longitude) of the vehicle from a remote place. The GPS modem will continuously give the data i.e. the latitude and longitude indicating position of the vehicle. When the request by user is sent to the number at the GSM modem, the system automatically sends a return reply to that mobile. Here piezo electric buzzer is used to detect the vibrations that are occurred in case of any accidents and it sends signal to microcontroller to send latitude and longitude information to the number stored in microcontroller. Also a SOS Button is used in case of any emergencies. When the button is pressed, the system automatically sends a message to the number stored in the microcontroller.

**Keywords:** GPS, GSM SIM300, Microcontroller 89C52 ARM7, Sensors.

### **I. INTRODUCTION**

Nowadays Embedded Systems are plays a major role in our daily life to fulfill the daily needs of a human being with less effort even to do the complex and specific tasks instead off a human being. The embedded systems are well popular in all sectors utilizations like home appliances, mobile communication, office automation devices and so on. Each and every application will have a special purpose processor and special purpose hardware to satisfy the user specific requirements with the help of a embedded software called as ERTOS-Embedded Real Time Operating System to execute the user specific applications. The ERTOS is also referred as "firm ware". The Embedded systems are designed to do a specific task that is defined by the user based on user requirements. The limitation of any Embedded System is they have not sufficient resources like memory and they don't have CDROM memory. The Embedded systems are always counter to some deadlines in work. The basic characteristic of an Embedded System is, it has to complete a specific task with a specified given time period. In Real Time Embedded Systems the targets are tough, if any system

is failure to meet the requirements that may cause the smash the system like Air Traffic Control Management System. Another limitation of Embedded Systems Power, All the Embedded Systems are battery based systems, so the power consumption is low.

The proposed VTS -Vehicle Tracking System model is used to describe the locality of a vehicle through GPS technology. The GPS is used to establish the communication path between satellites and ground stations and identify the exact location of a vehicle by using triangulation approaches. With the help of VTS now it is very easy to trace our high expensive vehicles with accurate location and time on the earth. The VTS also provides the details about vehicle accidents and sends the emergency alert message to our registered mobile Number. The VTS consists of transmitting unit at vehicle side and monitoring unit at user side. The Vehicle Unit consists of a circuit which is designed with GPS and GSM modem hardware parts and is constructed with the primary functions of a modem that keep tracking the vehicle by getting the information through GPS receiver from GPS satellites. The GSM modem sends the vehicle location data to the base station. The microcontroller is the heart of this device. It is the interface between the GSM module and the GPS receiver. A microcontroller is a small computer on a single integrated circuit containing a processor core, data memory, A/D converter and programmable input/output peripherals. In this device the microcontroller is programmed in such a way that it stimulates the GSM modem in message forwarding when a request is send by the user. Microcontrollers contains a Piezo electric buzzer which detects vibrations when any accident occurs and to report occurrences of accident automatically via GSM communication platform using SMS messaging. This unit also contains a SOS Button which is useful in emergency situation.

Nowadays the major challenging issue for all users and researchers is how best they are providing the security for their Vehicles is considering the primary goal. The researchers develop one best model to provide security for the vehicle with the help of GPS systems. Now the user can closely monitor the vehicle locations from time to time and easy to track their vehicle locations. This model is well popular and referred as Vehicle Tracking System. The VTS

# Fast Mining Approach for Automatic Recognition of Rare Raga Swaram Notes

T.V.Mahendra

*Associate Professor*

*Dept.of CSE*

*NBKIRST,Vidyanagar*

G.Venugopal

*Associate Professor*

*Dept.of CSE*

*VITS,Kavali*

**Abstract - Data Mining** is a powerful technology to discover and analyze large data sets. It has its applications in various fields of Arts, Science and Engineering. One such field is Music. Music is a form of arts which comes under fine arts category. Carnatic music is a form of south Indian classical music which comprises of swarams (7 notes) to evolve music. This research work deals with automatic identification of rare Carnatic raga Swaram notes through Data Mining algorithms. The training sets considered for the work are Aavarohanam notes of 72 melakartha raga and 212 Janya raga. C4.5 decision tree algorithm, Random Tree and Rule Induction algorithm were utilized to classify the Melakartha raga and the Janya raga. However the Janya raga swaram notes were also investigated through the use of appropriate feature relevance algorithms namely Feature ranking, Correlation based Feature Selection (CFS) filtering, and Fast Correlation based Filter (FCBF) filtering. The Melakartha raga data set was accurately classified with 100% accuracy by all the aforementioned classification techniques while predictor attributes selected through feature ranking algorithm produced nearly 90% accurate classification with Rule Induction algorithm on the Janya raga data.

**Keywords - Carnatic raga swarams, Classification, Feature Selection, Rule Induction.**

## I. INTRODUCTION

Data Mining [1], an analysis part of knowledge discovery with immense potential helps to classify and access hidden details from a database. Data mining [2] helps in finding predictive information that experts may miss because it lies outside their expectations. Data Mining [1-2] detects patterns based on user queries with Classes, Clusters, Association, Sequential Patterns and Feature Selection. Feature selection [3] in supervised learning attempts to find a feature subset that produces higher classification accuracy. Classification [3] is the task of generalizing known structure, to apply to new data. Classification, a data mining technique is used to predict group membership for data instances. The above said data mining techniques can be applied to various fields viz. medical, business, arts etc.

One such field in arts is Music. Music can be classified as Western Music and Indian Classical Music [4]. The Indian classical music can be further viewed as Hindustani Music and Carnatic Music. Carnatic music is a South Indian Classical music which consists of Raga (melody), seven Swaras (note with pitch), and Thalas (rhythmic beat) to produce a musical concert note [5-6]. Each Raga consists of template Arohana and Aavarohana from which notes (Swaras) are produced. It consists of 72 main Melakartha raga from which many combinations of Janya raga can be formed.

In this paper we apply Feature Selection and Classification methods to raga swara notes to automatically recognize raga and we perform a comparative analysis on the performance of classification and feature selection algorithms.

The rest of the paper is organized as follows. Section 2 discusses the Literature survey on classification of music and raga identification. Section 3 gives the description on Carnatic Music. Section 4 narrates the Data Mining methods utilized to recognize Carnatic Music Swaras, while Section 5 presents the Experimental Results. Section 6 concludes the paper with a view on possible extensions to this research.

## II. LITERATURE SURVEY

# Efficient Mining Of Top-K High Utility Itemsets From Uncertain Databases

Vamsinath Javangula<sup>1</sup>, Suvarna Vani Koneru<sup>2</sup>, Haritha Dasari<sup>3</sup>

<sup>1</sup>Cse Department, P.B.R VITS, Kavali, Andhra Pradesh, India

vamsi.img@gmail.com

<sup>2</sup>Cse Department, Velagapudi Ramakrishna Siddhartha Engineering College, Kanuru, Andhra Pradesh, India

suvarnavanik@gmail.com

<sup>3</sup>Cse Department, University College of Engineering College, Kakinada, JNTUK, Andhra Pradesh, India

harithadasari9@yahoo.com

## Abstract—

Mining High-utility itemsets is vital issue in data mining research. Utility Mining have various Applications in cross-marketing retail stores, website click stream analysis and biomedical applications. The algorithms currently proposed for mining on data which defined exactly. Normally when big data received through various sensor networks due to noise presence it deviate from original values and data becomes uncertain. High utility itemsets are identified in uncertain data by setting proper minimum utility, minimum potential probability thresholds. Normally algorithms generate large number of high utility itemsets and lot time is consumed if proper threshold are not identified. In this paper, both of this problems addressed in an efficient framework to mine Top-K Uncertain High-Utility Itemsets (TKUHUI), is proposed, where k is the required high utility itemsets. Extensive experimental results on real and synthetic datasets show that TKUHUI is both efficient and scalable.

## I. INTRODUCTION

Data Mining is popularly referred as information Discovery in knowledge (KDD). Data Mining projected varied techniques like Classification, Clustering, Association Rule Mining, Frequent Pattern Mining, and outlier analysis. In e-commerce, inventory management data processing play a significant role. In these areas frequent pattern mining terribly helpful.

Frequent pattern Mining is employed to catch the frequent patterns from transaction databases. Association rules mining (ARM) [2] model works based on the if an item is exist in the transaction or not by examining the all database items equally important. Frequent itemsets known by ARM will

provide little profit among the overall profit, but non-frequent items can provide highest amount of profit..

In reality, a retail business could also be curious about distinguishing its most precious customers (customers who contribute a large amount of the profits to the company). These are the shoppers, who could purchase full priced things, high margin things, which can be absent from an most of the transactions as a result of most customers don't obtain these things. During a Association Rule Mining, these transactions representing extremely profitable customers could also be omitted. Utility mining is probably going to be helpful during a wide selection of sensible applications.

Recently, a utility mining model was outlined [2]. Utility could be a parameter of however "useful" an itemset is. The goal of utility mining is to spot high utility itemsets that drive an major portion of the total utility. Historical ARM drawback could be a special case of utility mining, wherever the utility of every item is often one and also the sales amount is either zero or one.

There is no efficient strategy to find all the high utility itemsets due to the nonexistence of "downward closure property" (anti-monotone property) in the utility mining model. A heuristics [2] is used to predict whether an itemset should be added to the candidate set

In MEU (Mining using Expected Utility) the prediction usually overestimates, particularly at the starting stages, wherever the no.of candidates approaches the quantity of all the mixtures of items. Such needs will simply overwhelm the memory area available and computation power of most of the machines. Additionally, MEU might miss some high utility itemsets once the variance of the itemset supports is more.

The challenge of utility mining is in limiting the scale of the candidate set and simplifying the computation for hard the utility. so as to tackle this

## iOVFDT for Concept-drift Problem in Big Data

Rajeswari P. V. N [1], Radhika P. [2]

Assoc. Professor [1], Dept of CSE, Visvodaya Engineering College, Kavali

Asst. Professor [2], Dept of CSE, Geethanjali Institute of Science & Technology, Nellore  
AP – India.

### ABSTRACT

The problem of How to efficiently uncover the knowledge hidden within massive and big data remains an open problem. It is one of the challenges is the issue of ‘concept drift’ in streaming data flows. Concept drift is a well-known problem in data analytics, in which the statistical properties of the attributes and their target classes shift over time, making the trained model less accurate. Many methods have been proposed for data mining in batch mode. Stream mining represents a new generation of data mining techniques, in which the model is updated in one pass whenever new data arrive. This one-pass mechanism is inherently adaptive and hence potentially more robust than its predecessors in handling concept drift in data streams. In this paper, we evaluate the performance of a family of decision-tree-based data stream mining algorithms. The advantage of incremental decision tree learning is the set of rules that can be extracted from the induced model. The extracted rules, in the form of predicate logics, can be used subsequently in many decision-support applications. However, the induced decision tree must be both accurate and compact, even in the presence of concept drift. We compare the performance of three typical incremental decision tree algorithms (VFDT [2], ADWIN [3], iOVFDT [4]) in dealing with concept-drift data. Both synthetic and real-world drift data are used in the experiment. iOVFDT is found to produce superior results.

**Keywords:-** Data Stream Mining; Concept Drift; Incremental Decision Tree; Classification.

### I. INTRODUCTION

Big data has become a hot research topic, and how to mine valuable information from such huge volumes of data remains an open problem. Many research institutes worldwide have dedicated themselves to solving this problem. The solutions differ from traditional data mining methods, where the mining process must be efficient and incremental.

Processing big data presents a challenge to existing computation platforms and hardware. However, according to Moore’s Law, CPU hardware may no longer present a bottleneck in mining big data due to the rapid development of integrated circuit industry. A well-designed algorithm is crucial in solving problems associated with big data.

A data stream model is usually defined as a model in which data move continuously at high-speed. Most big data can be considered as data streams, in which new data are generated continuously. Data streams contain very large volumes of data, which cannot be stored in either internal or external memory. A one-pass algorithm therefore forms the basis of data stream mining, which briefly stores a sufficient statistical matrix when new data passes, but does

not require the full dataset to be scanned repeatedly.

A data stream also depicts an infinite big data scenario in which the underlying data distribution of newly arriving data may differ from older data in the real world: the so-called concept-drift problem. For example, click-streams of users’ navigation patterns on an e-commerce website may reflect their purchase preferences as analyzed by the system. However, as people’s preferences for products change over time, the old model is no longer applicable, resulting in concept drift.

Decision trees are one of the most important data classification techniques. These techniques are widely used because of their ability to interpret knowledge in different domains and present it as a tree-like graph. Decision trees can be distinguished into two categories according to their components: single-tree algorithms and multi-tree algorithms. A single-tree algorithm is lightweight and easy to implement and thus favored for data stream environments, although in some cases, a multi-tree algorithm may achieve slightly higher accuracy.

### DATA STREAMS MINING PROBLEMS

# Neighboring Active Virus Triage By Software Facts Discount Methods

KALAPATI.SIREESHA

Assistant Professor, Dept Of CSE  
P.B.R Visvodaya Institute of Technology and  
Science(PBRVITS), Kavali, A.P, India

SUDEEPTHI CHAKRAM

M.Tech Student, Dept Of CSE  
P.B.R Visvodaya Institute of Technology and  
Science(PBRVITS), Kavali, A.P, India

**Abstract:** Mining of understanding has switched right into a competent approach to manage software data. By leveraging means of data mining, mining manner of software repositories can expose interesting data within software repositories and resolve actual software problems. Within our work we manage impracticality of information reduction for bug triage that's decrease in bug data in order to save work price of developers and get better the traditional to create easy the whole process of bug triage. A lengthy move of managing of software bugs is bug triage, which assign a precise developer to repair a totally new bug. To influence obvious of costly price of manual bug triage, existing work has forecasted an analog means of bug triage, involving the techniques of text classification can be expected developers for bug reports. Data decrease in aid of bug triage aims to place up somewhat-scale furthermore to expert quantity of bug data by way of elimination of bug reports furthermore to words which are redundant otherwise non-informative.

**Keywords:** Software Repositories; Bug Triage; Data Mining; Text Classification; Bug Data;

## I. INTRODUCTION

Existed means of software analysis aren't totally suitable for important and hard data within software repositories. Bug repository, plays a substantial role in managing of software bugs that are foreseeable and fixing of bugs is pricey within software development. Huge software projects organize bug repositories to cope with selection of data that assist developers to carry bugs [1]. Within the bug repository, an insect is managed as being a bug believe that records textual description of bug reproducing increase with regards to status of bug fixing. An insect repository offer data platform to cope with several types of tasks above bugs. Within our work, bug reports within the bug repository are known as bug data. As software bug details have the freedom-form text information, you need to produce well-processed bug data to create easy application. Within our work we handle the problem of understanding reduction for bug triage that's decrease in bug data in order to save work price of developers and get better the traditional to create easy the whole process of bug triage. Data reduction for bug triage aims to place up somewhat-scale furthermore to expert quantity of bug data by way of elimination of bug reports furthermore to words which are redundant otherwise non-informative. Instance selection with feature selection was combined to concurrently decrease data scale on bug dimension furthermore to word dimension [2]. For exercising order of applying instance selection furthermore to feature selection, we remove attributes inside the historic bug data sets and produce a predictive representation for almost any novel bug data set.

## II. METHODOLOGY

Inside the latest methods for software development, software repositories are major databases for storing from the development of software development. Software companies consume cost in handling of software bugs. An unavoidable move of fixing bugs is bug triage, which assign a developer perfectly right into a new bug. Vast software projects organize bug repositories to deal with range of data that really help developers to hold bugs. Data reduction for bug triage aims to put up just a little-scale additionally to expert number of bug data by means of removal of bug reports additionally to words that are redundant otherwise non-informative. To reduce time cost within manual work, text classification methods are functional to deal with automatic bug triage. There are 2 challenges that are connected towards bug data that could influence effective utilization of bug repositories within the tasks of software development. Due to daily-reported bugs, large figures of latest bugs is stored up within bug repositories is challenge to look at such important bug data within software development. In contrast software techniques experience from poor of bug data. Two distinctive characteristics of substandard bugs are noise additionally to redundancy. We handle the issue of knowledge reduction for bug triage that's reduction in bug data to save work cost of developers and acquire better the conventional to produce easy the entire process of bug triage. Noisy bugs might misinform connected developers whereas redundant bugs waste restricted time period of bug handling [3]. A period of time-consuming move of managing of software bugs is bug triage, which assign an exact developer to fix a completely new bug. In conventional software

# Endangered Information Combination Technique For Wireless Sensor Networks In The Occurrence Of Collusion Attacks

MENTA VIJAYA BHASKAR

Assistant Professor, Dept Of CSE

P.B.R Visvodaya Institute of Technology and  
Science(PBRVITS), Kavali, A.P, India

PANDITI SRAVAN KUMAR

M.Tech Student, Dept Of CSE

P.B.R Visvodaya Institute of Technology and  
Science(PBRVITS), Kavali, A.P, India

**Abstract:** Iterative filtering algorithms hold great promise for this sort of purpose. Because of limited computational power and sources, aggregation of understanding from multiple sensor nodes finished in the aggregating node is generally accomplished by simple way of example averaging. During this paper we show several existing iterative filtering algorithms, while considerably greater quality against collusion attacks in comparison with simple averaging methods, are nonetheless susceptible having a novel sophisticated collusion attack we introduce. However such aggregation is called highly vulnerable to node compromising attacks. Because the performance of small power processors dramatically improves, future aggregator nodes will have a way to performing modern-day data aggregation algorithms, thus making WSN less vulnerable. Thus, ascertaining standing of knowledge and standing of sensor nodes is important for WSN. Such algorithms concurrently aggregate data from multiple sources and provide trust assessment of people sources, usually in a kind of corresponding weight factors utilized on data supplied by each source. To handle this security issue, we advise an apparent difference for iterative filtering techniques by providing a preliminary approximation for such algorithms which makes them not just collusion robust, but in addition better and faster converging.

**Keywords:** Wireless Sensor Networks; Robust Data Aggregation; Collusion Attacks;

## I. INTRODUCTION

At the moment, because of limitations from the computing power and resource of sensor nodes, information is aggregated by very simple algorithms for example averaging. However, such aggregation is proven to be very susceptible to problems, and most importantly, malicious attacks. Data from multiple sensors is aggregated in an aggregator node which in turn forwards towards the base station just the aggregate values [1]. Thus, better, modern-day algorithms are essential for data aggregation later on WSN. This kind of formula must have two features: In the existence of stochastic errors such formula should produce estimates that are near to the optimal ones in information theoretic sense. The formula ought to be robust in the existence of non-stochastic errors, for example problems and malicious attacks, and, besides aggregating data, such formula also needs to offer an assessment from the reliability and standing of the information caused by each sensor node. A trustworthiness assessment at a moment represents an aggregate from the conduct from the participants as much as that moment and needs to be robust in the existence of various problems and malicious conduct. There are a variety of incentives for attackers to control the trust and status lots of participants inside a distributed system, and the like manipulation can seriously impair the performance of these a method. The primary target of malicious attackers is aggregation algorithms of trust and

status systems. Trust and status happen to be lately recommended as a good security mechanism for Wireless Sensor Systems. Sensors deployed in hostile environments might be susceptible to node compromising attacks by adversaries who plan to inject false data in to the system. Within this context, assessing the standing of the collected data turns into a challenging task. Because the computational power really low power processors dramatically increases, mostly driven by demands of traveling with a laptop, and because the price of such technology drops, WSNs can afford hardware which could implement modern-day data aggregation and trust assessment algorithms. Iterative Filtering (IF) algorithms are a beautiful choice for WSNs simply because they solve both problems-data aggregation and knowledge trustworthiness assessment-utilizing a single iterative procedure. This paper presents a brand new sophisticated collusion attack scenario against numerous existing IF algorithms in line with the false data injection. Such a panic attack scenario, colluders make an effort to skew the aggregate value by forcing such IF algorithms to converge to skewed values supplied by among the attackers. Although such suggested attack is relevant to some wide range of distributed systems, it's particularly harmful once launched against WSNs for 2 reasons [2]. First, trust and status systems play critical role in WSNs as a technique of resolving numerous important problems, for example secure routing, fault tolerance, false data recognition,

# Confidentiality-Destructive And Dishonest Discovery Of Packet Falling Assaults In Wireless Ad Hoc Networks

**SHAIK SHABBIR BASHA**

Associate Professor, Dept Of CSE

P.B.R Visvodaya Institute of Technology and  
Science(PBRVITS)  
Kavali, A.P, India

**V. VENKATESWARLU**

Mtech Student, Dept Of CSE

P.B.R Visvodaya Institute of Technology and  
Science(PBRVITS)  
Kavali, A.P, India

**Abstract:** In broad wireless means, link errors are relatively important, and may not be significantly lesser than packet shedding rate of insider attacker hence insider attacker can hide in backdrop of harsh funnel conditions. We're concerned in combating an insider attack and thinking about complexity to discover happening of selective packet drops and recognize malicious node that handle such drops. Within our work during study of packet sequence losses inside the network, we're concerned in exercising whether losses result from approach to link errors simply, otherwise by collective after effect of link errors in addition to malicious drop. We develop accurate formula for recognition of selective packet drops which are produced by insider attackers. To create apparent on computation of correlations, we create a homomorphic straight line authenticator that's on public auditing design basis that enables the detector to make sure honesty of packet loss information that's as outlined above by nodes. This arrangement is privacy preserving, and sustains low communication in addition to storage spending. Our formula additionally provides honest in addition to freely verifiable decision statistics as proof to keep recognition decision.

**Keywords:** Insider Attacker; Malicious Node; Selective Packet; Homomorphic Linear Authenticator; Privacy Preserving; Public Auditing;

## I. INTRODUCTION

Recognition of selective attacks of packet shedding is especially difficult in very active wireless setting. The complexity arises from necessity we must differentiate where packet is dropped, and recognize whether drop is planned otherwise unplanned. Due to broad nature of wireless means, packet drop within network might result from approach to harsh funnel conditions [1]. Within our work we're concerned in combating an insider attack and thinking about complexity to discover happening of selective packet drops and recognize malicious node which lead to such drops. Within our work during observation of packet sequence losses inside the network, we're concerned in exercising whether losses be a consequence of approach to link errors simply, otherwise by collective after effect of link errors additionally to malicious drop. We're concerned in insider-attack situation, where malicious nodes utilize their information of communication circumstance to reduce minute packets which are important towards network performance. Because the packet shedding rate during this situation is the same as funnel error rate, usual algorithms which are on packet loss rate recognition cannot achieve acceptable recognition precision progress recognition accurateness, we advise using correlations among lost packets [2]. To create apparent on open calculation of correlations, we improve your homomorphic

straight line authenticator that's based on public auditing design that enables the detector to make sure honesty of packet loss information that's as outlined above by nodes. This structure is privacy preserving, and sustains low communication additionally to storage spending. Our structure in addition provides privacy-preserving and incurs small communication additionally to storage overheads.

## II. METHODOLOGY

In systems of multi-hop, nodes help in relaying traffic. An foe may use supportive nature to commence attacks. After being incorporated within route, foe commences shedding packets. In severe form, malevolent node simply stops forwarding each packet that's introduced on by upstream nodes, disrupting path between source additionally to destination. Such denial-of-service attack can paralyze network by way of partitioning its topology. Within our work we develop accurate formula for recognition of selective packet drops which are produced by insider attackers. We're concerned in combating an insider attack and anxious in complexity to discover happening of selective packet drops and recognize malicious node which lead to such drops. During observation of packet sequence losses inside the network, we're concerned in exercising whether losses be a consequence of approach to link errors simply, otherwise by collective aftereffect of link errors

# Protected Spatial Best-Key Request Handling Via Unconfidential Location-Based Service Sources

**M. JANARDHAN**

Assistant Professor, Dept Of CSE  
P.B.R Visvodaya Institute of Technology and  
Science(PBRVITS), Kavali, A.P, India

**PRANAY GANGAVARAPU**

M.Tech Student, Dept Of CSE  
P.B.R Visvodaya Institute of Technology and  
Science(PBRVITS), Kavali, A.P, India

**Abstract:** Additionally owing towards rising recognition of social systems, it's more and more appropriate for mobile users to distribute with other people while using the entire types of points of interests. We consider novel distributed system meant for collaborative location-based data making furthermore to discussing which become increasingly popular due to elevated growth and development of Internet-capable furthermore to location-aware cell phones. Our objective should be to facilitate user to make sure authenticity and precision of query result came back using the location-based providers. During this paper, we introduce three novel schemes for fostering realistic deployment and extensive using envisioned system and the need for our schemes is the fact data collector pre-computes and validates some auxiliary more understanding about its data set, which exist all which is data set to location-based providers. The information collector will collect reviews regarding points-of-interest from data contributors, while location-based providers purchase points-of-interest data many techniques from data collector and let users to cope with spatial queries which request points-of-curiosity about a assured region with maximum k ratings by having an interested points-of-interest attribute.

**Keywords:** Location-Aware Mobile Devices; Social Networks; Mobile Users; Collaborative Location-Based Data; Location-Based Service Providers; Points-Of-Interest;

## I. INTRODUCTION

The unpredictable expansion of and location aware mobile devices is fostering collaborative information production and sharing over extraordinary size. Two drawbacks with existing top-k query services were observed such as: individual location-based service providers contain extremely small data sets comprising points-of-interest reviews which affect usefulness as well as eventually hinder prevalent usage of spatial top-k query services. Secondly location-based service providers might modify their data sets by means of deletion of several reviews or else addition of fake reviews and provides tailored query results for the restaurants that pay or else against those that say no to pay [1]. While location-based service providers are not malicious, they might return false query results in the influence of a variety of attacks in which same attacker can submit numerous fake reviews for the similar points-of-interest. A promising solution to the above issues is to set up several trusted data collectors as central hubs for collection of points-of-interest reviews. Data collectors will offer various incentives, for stimulation of review submissions and subsequently profit by means of selling the review information towards individual location-based service providers. Our intention is to facilitate user to confirm authenticity and accuracy of query result returned by the location-based service providers. Our work will consider a new distributed scheme

for collaborative location-based data making and sharing which become more and more popular because of increased expansion of Internet-capable as well as location-aware mobile devices.

## II. METHODOLOGY

It becomes routine for people to carry out a variety of spatial points-of-interest queries at online providers of location-based service. We consider a new distributed scheme for collaborative location-based data making and sharing which become more and more popular because of increased expansion of location-aware mobile devices [2]. The proposed system includes data collector, data contributors, location-based service providers, as well as system users. The data collector will gather reviews regarding points-of-interest from data contributors, while location-based service providers purchase points-of-interest data sets from data collector and permit users to carry out spatial top-k queries which request for points-of-interest within an assured region and with maximum k ratings for an interested points-of-interest attribute. A location-based service provider requires return accurate points-of-interest data records in addition to proper authenticity as well as accuracy proofs constructed from genuine hints. We introduce three novel schemes for fostering realistic deployment and extensive usage of envisioned system. The key proposal of our schemes is that data collector pre-computes and validates some auxiliary information regarding its data set, which are sold all along with

## Secure Data Integrity in Privacy Preserving Mobile Health Monitoring Using Cost Efficient Clouds

J. VAMSI NATH<sup>1</sup>, MYLA KODANDA<sup>2</sup>

<sup>1</sup>Associate Professor, Dept of CSE, PBR VITS College, Nellore, AP, India.

<sup>2</sup>PG Scholar, Dept of CSE, PBR VITS College, Nellore, AP, India.

**Abstract:** This cloud assisted mobile health monitoring includes mobile communication as well as cloud computing technologies to provide various services especially feedback decision support using information communication Technologies (ICT's) and mobile healthcare applications for the both parties involved in this mechanism for better security with extended privacy and data integrity by applying techniques. This system is to provide the simple user interface which can be easily understandable. It incorporated the hash based message authentication code (MAC) and MD-5 algorithm technique which can protect data integrity. This system also uses AES algorithm and outsourcing decryption technique for better privacy and security. Proposed design demonstrates mobile healthcare applications with simple user interface and protection to integrity of data in cloud-assisted privacy preserving mobile health monitoring. This system provides useful mobile healthcare applications with good results and it is very useful to remote area peoples where hospitals not easily accessible.

**Keywords:** Data Integrity, Mobile Healthcare Applications, hash based Message authentication code, MD-5, ICT's, Cloud Security, Cloud Efficiency, Trust Authority (TA).

### I. INTRODUCTION

Use of low cost sensors for mobile devices improves the service provider's quality while lowering the cost. Mobile health applications are designed for remote monitoring on health status. Medinet project of Microsoft is a mobile health application for diabetes and cardiovascular disease patients in remote areas. In Medinet project all respective details of patients could then be sent to a central server which could then run various web medical applications on these data to return timely advice to the client. Drawback includes cloud-assisted mHealth monitoring could offer a great opportunity to improve the quality of healthcare services and potentially reduce healthcare costs, there is some existing issues in reality. Without properly addressing the data management in this system, clients' privacy may be severely breached during the collection, storage, diagnosis, and Communications and computing. A recent study shows that most of peoples consider the privacy of their health information very important [1]. There is also need of data integrity in overall system which measures accuracy of data

flow in system. So systems data integrity concern is at high priority which comprises also security of system. However, how to achieve this effectively without compromising data integrity, privacy and security becomes a great challenge, which should be carefully investigated [2].

### II. BACKGROUND

In old CAM there is need to persist accuracy in overall process of system, because in the old model, if wrong input goes to doctors then it could result in wrong prescription of suggestion from the system. The basic CAM has the security enervation such as the identity representation set for a client's attribute vector  $v$  is known to trust authority and hence trust authority can easily infer the clients private attribute vector. Also if the client cannot protect his privacy from the cloud either because the cloud can easily find out the identity representation for the private key  $pkv_i$ ,  $i \in [1, n]$  by running identity test in MDRQ. [1, 3, 4]. Modified system uses AES algorithm with hash functions which incorporate message authentication code (MAC). It also comprises the various modules which communicate with each other for better integrity and uses simple user interface.

### III. SYSTEM MODEL

System uses four modules as follows:

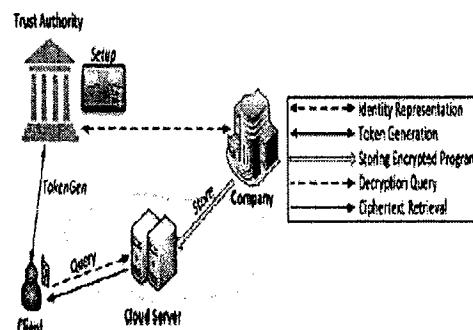


Fig. 1 System Architecture for CAM.

#### A. Cloud Server

Cloud server working mechanism includes following steps: Cloud Server act as offline storage. All data are saved in encrypted format even passwords of users. Ages, gender, emails of user are not encrypted.



## Improving Routing Performance in MANETS using Proactive Route Maintenance

### KEYWORDS

Ad-Hoc Networks, Wireless Mobile, Dynamic Source Routing, Proactive.

D.Likhith Reddy

Dep. of ECE, PBRVITS,kavali

V.V.Sunil kumar

Associate Professor, Dept. of CSE, PBR visvodaya institute of technology and science, kavali, AP

**ABSTRACT** Dynamic Source Routing (DSR) algorithm is simple and best suited for high mobility nodes in wireless ad hoc networks. Due to high mobility in ad-hoc network, route may not exist for long time. Hence DSR algorithm finds an alternative route when the existing communicating route goes down. It becomes a time consuming process if the communicating route fails frequently. In order to avoid this, we propose a modification to the existing DSR protocol. In this paper, we add a link breakage prediction algorithm to the Dynamic Source Routing (DSR) protocol. The mobile node uses signal power strength from the received packets to predict the link breakage time, and sends a warning to the source node of the packet if the link is soon-to-be-broken. The source node can perform a pro-active route rebuild to avoid disconnection. Intermediate nodes in the route continuously monitor the signal strength at the time of communication, based on a predefined threshold signal value. Intermediate node sends a message to the source node that the route is likely to be disconnected; if signal strength falls below the threshold value. If source receive this message it starts using backup route and if back route also fails then it finds alternative route. The backup route will minimize the time consuming process of finding an alternative route to some extent. Experiments demonstrate that adding link breakage prediction to DSR can significantly reduce the total number of dropped data packets (by at least 25%). Simulation results show that the probability of the communication breakage decreases when parallel routes are used.

### 1. INTRODUCTION

There are currently two variations of mobile wireless networks. The first is known as infrastructure network. The bridges for these networks are known as base stations. A mobile unit within these networks connects to and communicates with, the nearest base station that is within its communication radius. As the mobile unit travels out of range of one base station into the range of another, a "handoff" occurs from the old base station to the new, allowing the mobile to be able to continue communication seamlessly throughout the network. Typical applications of this type of network include office wireless local area networks (WLANs). The second type of mobile wireless network is the mobile ad-hoc network or MANET. Unlike infrastructure network, this type of network needs no base station. Mobile nodes communicate to each other by either directly or through intermediate nodes. Ad-hoc network becomes popular since it can be applied in many situations, such as emergency search-and-rescue operations, classroom, meetings or conference and many more. To facilitate communication within the network, a routing protocols used to discover routes between nodes. Building a MANET routing protocol is not an easy job, since efficiency and correctness becomes the main concern. Some approach had been proposed to make routing protocol becomes efficient and correct. Routing protocols in MANET, generally, can be categorized as table-driven and on-demand. In table-driven (also called proactive protocol), like in most routing protocol for wired network, each node is required to maintain routing table keep updated whether there is or not a request for routes. In on-demand (also called as reactive protocol), each node seeks for routes only when there is need to do so.[1]

### 2. Dynamic Source Routing Protocol (DSR)

The Dynamic Source Routing (DSR) protocol is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. It is based on the concept of source routing, a routing technique in which the sender of the packet determines the complete sequence of the nodes through which to forward the packet. The sender explicitly lists this route in the packet's header, identifying each forwarding "hop" by the address of the next node to which to transmit the packet on its way to the destination host.

The DSR protocol consists of two mechanisms: Route Discovery and

Route Maintenance. When a mobile node wants to send a packet to some destination, it first checks its route cache to determine whether it already has a route to the destination. If it has one, it will use this route to send the packet. Otherwise, it will initiate route discovery by broadcasting a route request packet. When receiving a request packet, a node appends its own address to the route record in the route request packet if it did not receive this request message before, and re-broadcasts the query to its neighbors. Alternatively, it will send a reply packet to the source without propagating the query packet further if it can complete the query from its route cache. Furthermore, any node participating in route discovery can learn routes from passing packets and gather this routing information into its route cache.

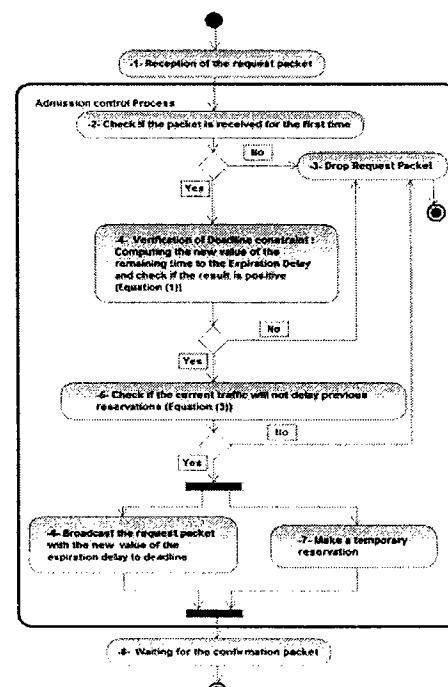


Fig 2: Activity diagram of intermediate node behavior in real time route request phase



# PARVATHAREDDY BABUL REDDY

## VISVODAYA INSTITUTE OF TECHNOLOGY & SCIENCE

(Affiliated to J.N.T.U.A, Approved by AICTE and Accredited by NAAC with 'A' Grade)

KAVALI – 524201, S.P.S.R Nellore Dist., A.P. India. Ph: 08626-243930

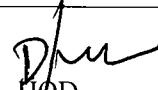


### DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

**List of Publications of faculty for the academic year 2015-16**

S.No	Name of the Faculty	Title of the Paper	Journal Name and ISBN/ISSN	Vol.No. Issue No. Page No.	Month & Year	Link for relevant document
1	P.Eswaraiah	Secure Data Storage in Clouds by Decentralized Access Control Scheme	International journal of Advance Research in Computer Science and Management Studies&ISSN:2321-7782	Vol.No.5 Issue No.3 Page No.4476	June 2015	<a href="https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1085.9000&amp;rep=rep1&amp;type=pdf">https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1085.9000&amp;rep=rep1&amp;type=pdf</a>
2	J. Vamsinath	Optimizing Energy Consumption of Mobile Relay Nodes in WSN's Networks	International Journal of Advanced Technology and Innovative Research&ISSN:2348-2370	Vol.No.4 Issue No.9 Page No.1636-1639	Aug 2015	<a href="http://www.ijatir.org/uploads/562341IJATIR6096-282.pdf">http://www.ijatir.org/uploads/562341IJATIR6096-282.pdf</a>
3	J. Vamsinath	Dynamic Shortest Path Computation using LTI-TD Framework in Road Networks	International Journal of Advanced Technology and Innovative Research&ISSN:2348-2370	Vol.No.4 Issue No.9 Page No.1629-1631	Aug 2015	<a href="http://www.ijatir.org/uploads/543621IJATIR6094-280.pdf">http://www.ijatir.org/uploads/543621IJATIR6094-280.pdf</a>
4	K.Sireesha	The Quality Demonstration projected in Cloud supervisions	International Journal of Science Engineering and Advance Technology&ISSN:2321-6905	Vol.No.3 Issue No.9 Page No.537-541	Sept 2015	<a href="http://www.ijseat.com/index.php/ijseat/article/view/438/pdf">http://www.ijseat.com/index.php/ijseat/article/view/438/pdf</a>
5	Dr.D. Srujan Chandra Reddy	Protection Assement of Design Classifiers under Assault	International Journal of Science Engineering and Advance Technology&ISSN:2321-6905	Vol.No.3 Issue No.9 Page No.527-531	Sept 2015	<a href="https://1library.net/document/download/yer8mnrq#">https://1library.net/document/download/yer8mnrq#</a>
6	D.Anil	Advanced Quering and Information Retrieval	International Journal of Recent Trends in Engineering And Research&ISSN:2455-1437	Vol.No.2 Issue No.03	Mar 2016	<a href="https://www.ijrter.com/papers/volume-2/issue-3/advanced-querying-and-information-retrieval.pdf">https://www.ijrter.com/papers/volume-2/issue-3/advanced-querying-and-information-retrieval.pdf</a>
7	B.Rasagna	Embedded Extended Visual Cryptography Schemes	Institute for Engineering Research And Publication	Vol.No.2 Issue No.8	Mar 2016	<a href="https://www.academia.edu/31565119/Detecting_Malicious_Entities_in_Wireless_Mesh_pdf">https://www.academia.edu/31565119/Detecting_Malicious_Entities_in_Wireless_Mesh_pdf</a>
8	B.Rasagna	Detecting Malicious Entities In Wireless Mesh Network	Institute for Engineering Research And Publication	Vol.No.2 Issue No.8	Mar 2016	<a href="https://www.academia.edu/31565119/Detecting_Malicious_Entities_in_Wireless_Mesh_pdf">https://www.academia.edu/31565119/Detecting_Malicious_Entities_in_Wireless_Mesh_pdf</a>
9	B.Rasagna	Information Retrieval By Keyword	Institute for Engineering Research And Publication	Vol.No.2 Issue No.8	Mar 2016	<a href="https://www.academia.edu/31565129/Information_Retrieval_by_Keyword_Query_pdf?auto=download">https://www.academia.edu/31565129/Information_Retrieval_by_Keyword_Query_pdf?auto=download</a>

  
Faculty in charge

  
HOD  
Head of Department  
**COMPUTER SCIENCE ENGINEERING**  
Visvodaya Institute of Technology & Science

# International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: [www.ijarcsms.com](http://www.ijarcsms.com)

## *Secure Data Storage in Clouds by Using Decentralized Access Control Scheme*

**P. Eswaraiah<sup>1</sup>**

Computer Science and Engineering  
PBR Visvodaya Institute of Technology & Science  
Kavali

**M. Mallika<sup>2</sup>**

Computer Science and Engineering  
Shree Institute of Technical Education  
Tirupati

**Abstract:** This paper focuses on real-world applications of a new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the series without knowing the user's identity before storing data. Decentralized access control scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. The scheme also address user revocation. Moreover, authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches.

**Key words:** Access control, Authentication, Attribute-based signatures, Attribute-based encryption, Cloud storage

### I. INTRODUCTION

#### **Cloud computing:**

Cloud computing is receiving a lot of attention from both academic and industrial worlds. In cloud computing, users can outsource their computation and storage to servers (also called clouds) using Internet. These free users from the hassles of maintaining resources on-site. Clouds can provide several types of services like applications (e.g., Google Apps, Microsoft online), infra- structures (e.g., Amazon's EC2, Eucalyptus, Nimbus). and platforms to help developers write applications (e.g., Amazon's S3, Windows Azure).

Much of the data stored in clouds is highly sensitive, for example, medical records and social networks. Security and privacy are, thus, very important issues in cloud computing. In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced. User privacy is also required so that the cloud or other users do not know the identity of the user. The cloud can hold the user accountable for the data it outsources, and likewise, the cloud is itself accountable for the services it provides. The validity of the user who stores the data is also verified. Apart from the technical solutions to ensure security and privacy, there is also a need for law enforcement.

Access control in clouds is gaining attention because it is important that only authorized users have access to valid service. A huge amount of information is being stored in the cloud, and much of this is sensitive information. Care should be taken to ensure access control of this sensitive information which can often be related to health, important documents (as in Google Docs or Drop box) or even personal information (as in social networking). There are broadly three types of access control: user-based access control (UBAC), role-based access control (RBAC), and attribute-based access control (ABAC). In UBAC, the access control list contains the list of users who are authorized to access data. This is not feasible in clouds where there are many users. In RBAC users are classified based on their individual roles. Data can be accessed by users who have matching roles. The roles

## Optimizing Energy Consumption of Mobile Relay Nodes in WSN's Networks

J. VAMSINATH<sup>1</sup>, P. KHELA TEJASWI<sup>2</sup>

<sup>1</sup>Associate Professor, Dept of CSE, PBR Visvodaya Institute of Technology & Science, Kavali, AP, India.

<sup>2</sup>PG Scholar, Dept of CSE, PBR Visvodaya Institute of Technology & Science, Kavali, AP, India.

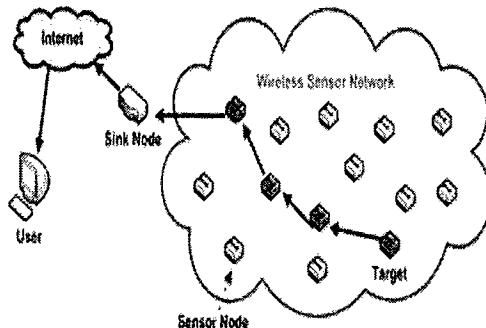
**Abstract:** Now a days, Wireless detector Networks (WSNs) are progressively employed in data-intensive applications like micro climate monitoring, exactitude agriculture, and audio/video police work. A key challenge visage by data-intensive WSNs is to transmit all the info generated among associate application's period of time to the bottom station despite the very fact that detector nodes have restricted power supplies. We tend to propose mistreatment inexpensive disposable mobile relays to scale back the energy consumption of data-intensive WSNs. Our approach differs from previous add two main aspects. First, it doesn't need advanced motion coming up with of mobile nodes, so it can be enforced on variety of inexpensive mobile detector platforms. Second, we tend to integrate the energy consumption thanks to each mobility and wireless transmissions into a holistic optimization framework. Our framework consists of 3 main algorithms. The first algorithmic program computes associate optimum routing tree presumptuous no nodes will move. The second algorithmic program improves the topology of the routing tree by avariciously adding new nodes exploiting quality of the new additional nodes. The third algorithmic program improves the routing tree by relocating its nodes while not dynamic its topology. This repetitive algorithmic program converges on the optimum position for every node given the constraint that the routing tree topology doesn't amendment. We tend to gift economical distributed implementations for each algorithmic program that need solely restricted, localized synchronization. as a result of we tend to don't essentially reckon associate optimum topology, our final routing tree isn't essentially optimum. However, our simulation results show that our algorithms considerably beat out the best existing solutions.

**Keywords:** Optimization, Wireless Sensor Networks, Tree Construction.

### I. INTRODUCTION

A wireless detector network (WSN) may be a wireless network consisting of spatially distributed autonomous devices that use sensors to observe physical or environmental conditions. Fig.1 show that Wireless detector networks are expected to be deployed inaccessible and hostile environments like environs observation applications, battlefields for enemy movement observation, etc. Although, it faces the matter to send all the information

detected by the detector nodes to the bottom station inside associate application's period of time because of the restricted power provides. These WSNs are must maintain adequate energy of the detector nodes to transmit all the information generated inside the period of time of the applications to the bottom station. Many alternative approaches are projected to considerably cut back the energy price of WSNs by exploitation the quality of nodes.



**Fig. 1. System Overview.**

The inexpensive disposable mobile relays are wont to cut back the entire energy consumption of data-intensive WSNs. totally different from information mules or mobile base station, the mobile relays don't transport data; instead, they move to totally different locations then stay stationary to forward information on the methods from the sources to the bottom station. Thus, the communication delays will be considerably reduced compared with exploitation mobile sinks or information mules.

### II. EXISTING SYSTEM

In wireless sensor networks the data collected by sensor nodes are transmitted to the sink node and then to the base station. All these nodes depends on the battery for transmitting data. So there is a need to reduce the battery consumption. Several different approaches have been proposed to significantly reduce the energy cost of WSNs by using the mobility of nodes. Some of them are

- Data mules
- Mobile sink nodes

A data mule is a vehicle that physically carries a computer with storage between remote locations to effectively create a

## Dynamic Shortest Path Computation using LTI-TD Framework in Road Networks

J. VAMSINATH<sup>2</sup>, D. KALPANA<sup>1</sup>

<sup>1</sup>Associate Professor, Dept of CSE, PBR Visvadaya Institute of Technology & Science, Kavali, AP, India.

<sup>2</sup>PG Scholar, Dept of CSE, PBR Visvadaya Institute of Technology & Science, Kavali, AP, India.

**Abstract:** Nowadays, several online services provide live traffic data such as Google-Map, Navteq, INRIX Traffic Information Provider, and TomTom NV. But still computing the shortest path on live traffic is big problem. This is important for car navigation as it helps drivers to make decisions. In presented approach server will collect live traffic information and then announce them over wireless network. With this approach any number of clients can be added. This new approach called live traffic index-time dependant (LTI-TD) enables drivers to update their shortest path result by receiving only a small fraction of the index. The existing systems were infeasible to solve the problem due to their prohibitive maintenance time and large transmission overhead. LTI-TD is a novel solution for Online Shortest Path Computation on Time Dependent Network.

**Keywords:** LTI-TD, Shortest Path, Transmission Overhead.

### I. INTRODUCTION

With the popularity of online map applications and their wide deployment in mobile devices and car-navigation systems, an increasing number of users search for point-to-point fastest paths and the corresponding travel-times [3]. This problem has been extensively studied on static road networks where edge costs are constant. Many efficient speed-up techniques have been developed to compute the fastest path in a matter of milliseconds. The quickest path approaches make the assumption that the travel-time for each edge of the road network is constant. In real-world the actual travel-time on a road heavily depends on the traffic congestion and, therefore, it is time-dependent. One can observe that the time-dependent travel-times yield a change in the actual quickest path between any pair of places throughout the day. Specifically, the quickest path from one place to another varies depending on the departure-time from the source.

### II. EXISTING SYSTEM

Nowadays, several online services provide live traffic data such as Google-Map, Navteq, INRIX Traffic Information Provider, and TomTom NV. Online services analyzed collected data from road sensors, traffic cameras. These systems are able to compute shortest path based on

current live traffic data. But they do not provide routes to drivers. Traffic data provides information about speeds on specific road changing over time. It is important in network analysis. Traffic affects travel times, which in turn affect results hence network analysis is important. If you are planning a route from one place to another and without considering traffic, expected travel and arrival times could not be accurate. You may miss routes that save time by avoiding the slower and congested roads. The following two diagrams show that the quickest route can change at different times of the day due to traffic as shown in Figs.1 and 2.

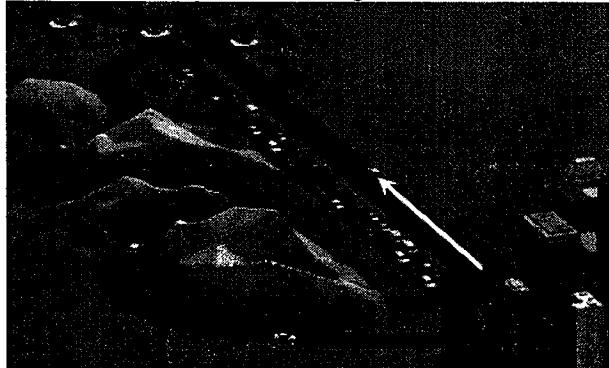


Fig.1. Traveler traffic is heavy, but traffic to the suburbs is light; therefore, the quickest route from the city to the suburbs at this time is along the divided highway.

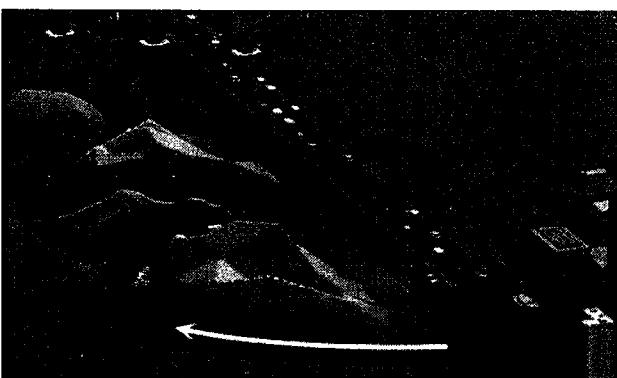


Fig. 2. Travelers are driving home, which increases the travel time in that direction. Travel has become slow



## The Quality Demonstration projected in Cloud supervisions

Mrs. K. Sireesha #1, Ms. M. Radhika #2

Assistant Professor, Dept. of CSE, VEC, Kavali, India,

M.Tech 2<sup>nd</sup> year, Dept. of CSE, PBR VITS, Kavali, India,

Email:kalapati.sireesha85@gmail.com,monabotiradhika@gmail.com

### Abstract—

A defender amongst the preeminent vital current examinations inside of the Cloud Computing provisioning is that the Service Level Agreement and its application in ensuring the gave appropriated figuring organizations. The strategy for giving appropriated organizations has been reconsidered as partner result of using dispersed figuring that as a region of flip has well known new challenges with every suppliers and customers. Estimation the character of circulated processing procural from the client's point of view is basic accordingly on surety that the organization fits in with the sum decided inside of the understanding; this is regularly typically implied as Quality of skill. There has been some work in estimation the standard of Service as a strategy for ensuring the organization level in dispersed processing. One in everything about troubles with estimation the standard of aptitude parameters is that gigantic quantities of the parameters are subjective, and thusly makes it challenging to portray a deliberate metric to be utilized for instrumenting the gave organization. This paper depicts a working - headway investigate that attempts to portray partner assessed metric that may be utilized as partner execution live to benchmark SaaS applications in appropriated processing. Such a metric are significant to cloud suppliers and also buyers for ensuring that the sent organizations meet the shopper wants. The conveyed registering applications brings another course of action of data security issues. The cloud security model see capable of SLA (Service Level Agreement) was centered on. From the assurance troubles of conveyed figuring , appropriated registering security risks was compound widely, the organization level understandings was augmented, the CSLA (Cloud Service Level Agreement) structure was anticipated, the cloud security course of action was arranged, the cloud security level auxiliary designing and cloud organizations evaluating and charging models was anticipated.

### I. Introduction:

As a result of the fundamental imagined by dispersed registering as the overwhelming model for the acquisition of IT organizations later on, it has been routinely implied as the fifth utility close by force, gas, water and telephony. Purchasers of

the cloud search for courses for ensuring that the cloud gives a predictable and reliable organization. Disregarding the cloud's attempts suppliers to ensure high availability of organizations, customers search for protections to ensure their rights if there ought to emerge an event of break the understanding [1]. Circulated processing can be described as the acquirement of organizations by setting up the information's benefits advancement through the web [2]. It is a massive aggregate of conceivable resources, for instance, hardware or stages, which may be considered as another to set up resources, since they are supplied on requesting, toward the day's end pay as you go resources [3]. Circulated figuring focal points both the customers and designers. From the creator's perspective, it expands the enrolling force furthermore stockpiling capacity to manage their applications, while for the customers it promises the openness of their knick-knacks paying little personality to the status of their machines [4]. Circulated figuring is a creating advancement that unravels the passageway to the enrolling resources which are widely scattered over the Internet. Disseminated processing grants computations to be performed through shared resources instead of using resources available on one site. This suggests for a dispersed figuring application, there will be one presented and kept up event for the whole cloud instead of presenting the item for each purchaser [5]. Three standard organizations have been used to portray the disseminated registering, these organizations are: firstly, Software as a Service (SaaS), which insinuates the applications gave on the cloud to the end customer freeing the buyer from the heaviness of keeping up these applications, these applications considering the web programs; likewise, Platform as a Service (PaaS), which is regularly used by the architects to gather and run their applications; and thirdly, Infrastructure as a Service (IaaS), which supplies the base resources as an organization like limit and handling to ensure the benefits' adaptability as demonstrated by the customer's necessities [6-8]. The appropriated processing model for giving IT organizations suggests that purchasers have partial control over the organization's workplace. In light of this, it is not satisfactory to center the obliged organizations and possible suppliers. It is furthermore basic to focus



## Protection Assessment of Design Classifiers under Assault

Dr. D. Srujan Chandra Reddy<sup>1</sup>, S. Ajay Kumar<sup>2</sup>

#1 Assoc. Professor, Department of CSE, PBR Visvodaya Institute of Technology & Science, Kavali.

#2 student, M.Tech (C.S) and Department of CS, PBR Visvodaya Institute of Technology & Science, Kavali.

### Abstract—

Design arrangement frameworks area unit usually utilized as an area of antagonistic applications, as biometric confirmation, system interruption location, and spam separating, within which info are often deliberately controlled by individuals to undermine their operation. As this ill-disposed scenario isn't thought of by ancient configuration techniques, style grouping frameworks could show vulnerabilities, whose abuse may seriously influence their execution, and thence confine their handy utility. Many works have attended the problem of outlining vigorous classifiers against these dangers, albeit basically concentrating on explicit applications and kinds of assaults. During this paper, we have a tendency to address one in every of the first open issues: assessing at define stage the safety of example classifiers, specifically, the execution debasement beneath potential assaults they will create amid operation. We have a tendency to propose a system for Experimental assessment of classifier security that formalizes and sums up the principle thoughts projected within the writing. System Security carries with it the procurements and techniques received by a system chairman to forestall and screen unapproved access. Email is that the principle correspondence interface currently every day everyone uses/have mail get to all or any authorities' organization sent on by a mail correspondence. During this mail correspondence we are going to have a spam sends. Spam Emails/numerous E-sends contains URL's to a sites or Webpages prompts infection or hacking. Thus we have a tendency to as of currently have a system for characteristic the spam sends but it will not acknowledge the total spam sends. Spamming is that the utilization of Electronic messages to send/get spontaneous mass messages significantly promoting erratically. Wherever as during this strategy we have a tendency to area unit planning to distinguish the total spam via email examining before it browse by the purchasers, impeding the area freelance of the purchasers E-mail ID, essential word primarily based obstructing by checking the themes, dominant the excellence within the middle of open and personal space before obstruction, watchword security by biometric, identity verification, pattern identification (face filtering) associated acknowledgment is an one in every of a form technique to acknowledge

all and sundry. We have a tendency to utilize savage power string match calculation. It demonstrates the somebody footage of face filtering acknowledgment framework may be perceived proficiently utilizing bury reliance of pixels rising from facial codes of images.

### I. Introduction:

In Pattern order frameworks machine learning calculations are utilized to perform security-related applications like biometric validation, system interruption location, and spam sifting, to recognize an "authentic" and a "malevolent" example class. The info information can be deliberately controlled by an enemy to make classifiers to deliver false negative. In spite of customary ones, these Applications have a natural antagonistic nature since the data information can be intentionally controlled by a smart and versatile enemy to undermine classifier operation. This frequently offers ascend to a weapons contest between the foe and the classifier planner. No doubt understood samples of assaults against example classifiers are: presenting a fake biometric characteristic to a biometric confirmation framework (mocking assault) [1], [2]; Well known cases of assaults are: Spoofing assaults where one individual or program intentionally misrepresenting information and subsequently picking up an illegitimate point of preference [1][2], modifying system bundles fitting in with meddlesome movement controlling substance of emails[3], modifying system parcels having a place with nosy activity. Ill-disposed machine learning is an examination field that lies at the convergence of machine learning and PC security. It expects to empower the sheltered selection of machine learning procedures in ill-disposed settings like spam sifting, malware identification and biometric acknowledgment. Samples include: assaults in spam separating, where spam messages are muddled through incorrect spelling of awful words or insertion of good words; assaults in PC security, e.g., to jumble malware code inside of system bundles or delude signature recognition; assaults in biometric acknowledgment, where fake biometric characteristics may be abused to mimic an authentic client (biometric satirizing) or to trade off clients' format exhibitions that are adaptively upgraded over time.[16] To comprehend the security properties of learning calculations in



## Advanced Querying And Information Retrieval

Ms. M.SANDHYAI<sup>1</sup>, Mr. D.ANIL<sup>2</sup>,

<sup>1</sup>M.tech 2<sup>nd</sup> year, Dept. of CSE, VEC, Kavali, India

<sup>2</sup>Associate professor, Dept. of CSE, VEC, Kavali, India

**ABSTRACT-** The most challenging research works in computing is privacy and protection. it provides an innovative business model for organizations with minimal investment. security is one of the major issues in cloud computing. currently huge researches is taking place on cloud computing. this is a survey paper on query services in cost efficient clouds .generally user expects immediate result for any query .but it is a cost efficient even we may adjust with the delay in query services .this survey presents description and comparison of Ostrovsky, COPS, and EIRQ protocols. EIRQ protocol is the latest among these protocols and it address the issues of privacy, aggregation, CPU consumption and network bandwidth usage.

### I. INTRODUCTION

Cloud computing is the internet based storage method. It is mainly used for storing the files and applications infrastructures .Peoples uses the cloud because of its attractive features like secure service, infinite of storage, it will satisfy the user experience, low cost multiple user can access the files and applications. In cloud, the query service process are frequently used because, the user can save their cost. The owners in the cloud will pay the amount only for their using time of server. This is an important feature because; the working time of query service in cloud is very high and more expensive. Cloud application, an organization subscribes the cloud services and authorizes its staff to share files in the cloud. Each file is described by a set of keywords, and the staff, as authorized users, can retrieve files of their interests by querying the cloud with certain keywords. In such an environment, how to protect user privacy from the cloud, which is a third party outside the security boundary of the organization, becomes a key problem. Private searching was proposed by Ostrovsky .which allows a user to retrieve files of interest from an untrusted server without leaking any information. However, the Ostrovsky scheme has a high computational cost, since it requires the cloud to process the query on every file in a collection. Otherwise, the cloud will learn that certain files, without processing, are of no interest to the user. It will quickly become a performance bottleneck when the cloud needs to process thousands of queries over a collection of hundreds of thousands of files.

We argue that subsequently proposed Commercial clouds follow a pay-as-you-go model, where the customer is billed for different operations such as bandwidth, CPU time, and so on. Solutions that incur excessive computation and communication costs are unacceptable to customers. To make private searching applicable in a cloud environment, our previous work designed a cooperative private searching protocol (COPS), where a proxy server, called the aggregation and distribution layer (ADL), is introduced between the users and the cloud. The ADL deployed inside an organization has two main functionalities: aggregating user queries and distributing search results. Under the ADL, the computation cost incurred on the cloud can be largely reduced, since the cloud only needs to execute a combined query once, no matter how many users are executing queries.

# Embedded Extended Visual Cryptography Schemes

[<sup>1</sup>] S. Meghana Reddy, [<sup>2</sup>] B Rasagna, [<sup>3</sup>] Prasad B  
[<sup>1</sup>] II/IV, [<sup>2</sup>][<sup>3</sup>] Associate Professor

[<sup>1</sup>][<sup>2</sup>][<sup>3</sup>] Department of CSE, Marri Laxman Reddy Institute of Technology and Management (MLRITM)  
Hyderabad

[<sup>1</sup>] meghana1995reddy@gmail.com [<sup>2</sup>] bheemarasagna@gmail.com [<sup>3</sup>] bprasad@gmail.com

**Abstract** A visual cryptography scheme (VCS) is a kind of secret sharing scheme which allows the encoding of a secret image into shares distributed to participants. The beauty of such a scheme is that a set of qualified participants is able to recover the secret image without any cryptographic knowledge and computation devices. An extended visual cryptography scheme (EVCS) is a kind of VCS which consists of meaningful shares (compared to the random shares of traditional VCS). In this paper, we propose a construction of EVCS which is realized by embedding random shares into meaningful covering shares, and we call it the embedded EVCS. Experimental results compare some of the well-known EVCSs proposed in recent years systematically, and show that the proposed embedded EVCS has competitive visual quality compared with many of the well-known EVCSs in the literature. In addition, it has many specific advantages against these well-known EVCSs, respectively.

**Keywords:** Visual Cryptography Scheme, Data Compression Algorithm, Encoding Algorithm

## I. INTRODUCTION

The basic principle of the visual cryptography scheme (VCS) was first introduced by Naor and Shamir. VCS is a kind of secret sharing scheme that focuses on sharing secret images. The idea of the visual cryptography model proposed in is to split a secret image into two random shares (printed on transparencies) which separately reveals no information about the secret image other than the size of the secret image. The secret image can be reconstructed by stacking the two shares. The underlying operation of this scheme is logical operation OR.

### a. Project purpose:

Purpose of a VCS with random shares the traditional VCS or simply the VCS. In general, a traditional VCS takes a secret image as input, and outputs shares that satisfy two conditions: 1) any qualified subset of shares can recover the secret image; 2) any forbidden subset of shares cannot obtain any information of the secret image other than the size of the secret image.

### b. Project Scope:

System provides a friendly environment to deal with images. Generally tools supports only one kind of image formats. Our application supports .gif and .png (portable network graphics) formatted images and our application has been developed using swing and applet technologies, hence provides a friendly environment to users. Vcs of an evcs, we mean a traditional vcs that have the same access structure with the evcs. Generally, an evcs takes a secret image and original share images as inputs, and outputs shares that satisfy the given three option: any qualified subset of shares can recover the secret image, any forbidden subset of shares cannot obtain any

information of the secret image other than the size of the secret image and all the shares are meaningful images.

### c. Product Features:

EVCS is flexible in the sense that there exist two trade-offs between the share pixel expansion and the visual quality of the shares and between the secret image pixel expansion and the visual quality of the shares. This flexibility allows the dealer to choose the proper parameters for different applications. Comparisons on the experimental results show that the visual quality of the share of the proposed embedded EVCS is competitive with that of many of the well-known EVCSs in the literature.

## II. SYSTEM ANALYSIS

### a. Problem definition:

Whenever we transmit the data (image) in the network, any unauthenticated person can read our data (image). In order to provide security to data (image) generally sender will encrypt the data (image) and send it the intended person and the receiver will decrypt the encrypted data(image) and uses it.

### b. Existing System:

Visual cryptography is the art and science of encrypting the image in such a way that no-one apart from the sender and intended recipient even realizes the original image, a form of security through obscurity. By contrast, cryptography obscures the original image, but it does not conceal the fact that it is not the actual image.

### c. Limitations of Existing System:

The existing system does not provide a friendly environment to encrypt or decrypt the data (images).

# Detecting Malicious Entities in Wireless Mesh Networks

[<sup>1</sup>] K Vijay Kumar, [<sup>2</sup>] B Rasagna, [<sup>3</sup>] Prasad B  
[<sup>1</sup>] II/IV, [<sup>2</sup>][<sup>3</sup>] Associate Professor

[<sup>1</sup>][<sup>2</sup>][<sup>3</sup>] Department of CSE, Marri Laxman Reddy Institute of Technology and Management (MLRITM)  
Hyderabad

[<sup>1</sup>] kudurutakavijay123@gmail.com [<sup>2</sup>] bheemarasagna@gmail.com [<sup>3</sup>] bprasad@gmail.com

**Abstract:** Multi-hop wireless mesh networks provide a community with a communication infrastructure which gives the ability to have a single or few connections to the internet along with each other. The core philosophy is that each node in the network would route each other packets for the benefit of everyone in the mesh network. This can give rise to a malicious node taking advantage of the forwarding nature in the network. A malicious node can drop the packets that should be forwarded and only forward its own packets therefore decreasing the benefits of the network for nodes upstream from the "bad" node. We present a Random Tester Detection Protocol (RTDP) that will detect the malicious node. The protocol leverages the broadcast nature of wireless networks along with anonymous messages to detect the free riding nodes. The protocol is evaluated in a network simulator created using Java.

**Keywords:** Random Tester Detection Protocol, Multi-hop wireless mesh networks, Dissemination.

## I. INTRODUCTION

Cheating in multi-hop wireless mesh networks can have very negative effects on users of the network. Multi-hop wireless networks allow neighbors to connect their home networks together. There are many advantages to enabling such connectivity and forming a community mesh network. For example, when enough neighbors cooperate and forward each others packets, they do not need to individually install an Internet gateway but instead can share faster, cost-effective Internet access via gateways that are distributed in their neighborhood. Packets dynamically find a route, hopping from one neighbor's node to another to reach the Internet through one of these gateways. Another advantage is that neighbors can cooperatively deploy backup technology and never have to worry about losing information due to a catastrophic disk failure. A third advantage is that this technology allows bits created locally to be used locally without having to go through a service provider and the Internet. Neighborhood community networks allow faster and easier dissemination of cached information that is relevant to the local community [1]. In this network the internet access is not controlled by a central entity but by everyone in the neighborhood.

### a. Cheaters

The multi-hop wireless mesh networks rely on the cooperation and interconnection of nodes to accomplish the common goal of internet access and communication. This

requirement of cooperation can give rise to individual cheaters in the network. Examples where individual behavior can be in conflict with the system goal include free-riding in peer-to-peer file sharing networks [3], cheating in online games [4], ISP competition in Internet routing [6], and network congestion control [8]. These cheater nodes will behave selfishly even to the detriment of the other nodes in the network.

### b. Routing

The lack of infrastructure and organizational environment of mobile ad-hoc networks gives special opportunities to attackers. The opportunities we focus on in this paper deal with the routing aspect of malicious behavior. Routing attacks such as [7]:

- ❖ No forwarding of control messages or data. (Gray hole problem)
- ❖ Route salvaging through rerouting to avoid a broken link, although no error has been observed.
- ❖ Lack of error messages, although an error has been observed.
- ❖ Unusually frequent route updates.
- ❖ Silent route change

### c. Problem

We will refer to cheating in a multi-hop network as failure to forward packets for other nodes. Those nodes are consuming global resources, as bandwidth and energy, to

# Information Retrieval by Keyword Query Routing

[<sup>1</sup>] G.Prasanna [<sup>2</sup>] B Rasagna, [<sup>3</sup>] Prasad B  
[<sup>1</sup>] II/IV, [<sup>2</sup>][<sup>3</sup>] Associate Professor

[<sup>1</sup>][<sup>2</sup>][<sup>3</sup>] Department of CSE, Marri Laxman Reddy Institute of Technology and Management  
(MLRITM) Hyderabad

[<sup>1</sup>] prasannaguduri19@gmail.com [<sup>2</sup>] bheemarasagna@gmail.com [<sup>3</sup>] bprasad@gmail.com

**Abstract:** Keyword search is an intuitive paradigm for searching linked data sources on the web. We propose to route keywords only to relevant sources to reduce the high cost of processing keyword search queries over all sources. We propose a novel method for computing top-k routing plans based on their potentials to contain results for a given keyword query. We employ a keyword-element relationship summary that compactly represents relationships between keywords and the data elements mentioning them. A multilevel scoring mechanism is proposed for computing the relevance of routing plans based on scores at the level of keywords, data elements, element sets, and subgraphs that connect these elements. Experiments carried out using 150 publicly available sources on the web showed that valid plans (precision@1 of 0.92) that are highly relevant (mean reciprocal rank of 0.89) can be computed in 1 second on average on a single PC. Further, we show routing greatly helps to improve the performance of keyword search, without compromising its result quality.

**Keywords:** Keyword Query Routing, Linked Data Sources, Processing Keyword, Queries

## I. INTRODUCTION

In recent years the Web has evolved from a global information space of linked documents to one where both documents and data are linked. Underpinning this evolution is a set of best practices for publishing and connecting structured data on the Web known as Linked Data. The adoption of the Linked Data best practices has lead to the extension of the Web with a global data space connecting data from diverse domains such as people, companies, books, scientific publications, films, music, television and radio programmes, genes, proteins, drugs and clinical trials, online communities, statistical and scientific data, and reviews. This Web of Data enables new types of applications. There are generic Linked Data browsers which allow users to start browsing in one data source and then navigate along links into related data sources. There are Linked Data search engines that crawl the Web of Data by following links between data sources and provide expressive query capabilities over aggregated data, similar to how a local database is queried today. The Web of Data also opens up new possibilities for domain-specific applications. Unlike Web 2.0 mashes which work against a fixed set of data sources, Linked Data applications operate on top of an unbound, global data space. This enables them to deliver more complete answers as new data sources appear on the Web. We propose to investigate the problem of keyword query routing for keyword search over a large number of

structured and Linked Data sources. Routing keywords only to relevant sources can reduce the high cost of searching for structured results that span multiple sources. To the best of our knowledge, the work presented in this paper represents the first attempt to address this problem. We use a graph-based data model to characterize individual data sources. In that model, we distinguish between an element-level data graph representing relationships between individual data elements, and a set-level data graph, which captures information about group of elements. This set-level graph essentially captures a part of the Linked Data schema on the web that is represented in RDFS, i.e., relations between classes. Often, a schema might be incomplete or simply does not exist for RDF data on the web. In such a case, a pseudo schema can be obtained by computing a structural summary such as a data guide.

### 1.2 Motivation

In today's world we access the Web for many needs. The Web is a collection of Linked data spread over different sources. If a user searches the Web with a simple keyword, it searches for the same across different sources and produces a large number of suggestions, of which many are not relevant to the users need. This process also implies a lot of cost in terms of time and searching. If we build a proper keyword query routing mechanism, we can improve the response time of the query and eliminate most of the suggestions that are not relevant to the keyword. shows the survey on information level required for

# Reduction Of Switching Activity In Noc By Using Data Encoding Schemes

**Y.Supraba, R.S.Pratap Singh**

P.b.r visvodaya institute of technology and science

Kavali, s.p.sr.nellore, india

[Ysupraba4@gmail.com](mailto:Ysupraba4@gmail.com)

P.b.r visvodaya institute of technology and science

Kavali, s.p.sr.nellore, india

[rpsvits@rediffmail.com](mailto:rpsvits@rediffmail.com)

**Abstract:** As technology shrinks, the power dissipated by the links of a network-on-chip (NOC) starts to compete with the power dissipated by the other elements of the communication subsystem, namely, the routers and the network interfaces (NIs). In this paper we present a reduction of switching activity in network on chip (NOC) by using data encoding schemes. In proposed schemes there is no need to change link architecture and it will reduce transitions (i.e. nothing but switching activity contains both switching transitions and coupling transitions). due to these transitions lot of power consumption is presented at the network on chip and routers so that by using data encoding schemes we can save consumption of energy and dissipation of power without any degradation of performance .

**Keywords:** Coupling switching activity, data encoding, low power, network-on-chip (NoC), power analysis.

## 1. INTRODUCTION:

Global interconnect length does not scale with smaller transistors and local wires. Chip size remains relatively constant because the chip function continues to increase and RC delay increases exponentially. At 32/28 nm, for instance, the RC delay in a 1-mm global wire at the minimum pitch is 25× higher than the intrinsic delay of a two-input NAND fan out of 5 [1]. If the raw computation horsepower seems to be unlimited, thanks to the ability of instancing more and more cores in a single silicon die, scalability issues, due to the need of making efficient and reliable communication between the increasing number of cores, become the real problem [3]. The network on- chip (NOC) design paradigm [4] is recognized as the most viable way to tackle with scalability and variability issues that characterize the ultra deep sub micron meter era. Nowadays, the on-chip communication issues are as relevant as, and in some cases more relevant than, the computation related issues [4]. In fact, the communication subsystem increasingly impacts the traditional design objectives, including cost (i.e., silicon area), performance, power dissipation, energy consumption, reliability, etc. As technology shrinks, an ever more significant fraction of the total power budget of a complex many-core system-on-chip (SOC) is due to the communication subsystem.

In this paper, we focus on techniques aimed at reducing the power dissipated by the network links. In fact, the power dissipated by the network links is as relevant as that dissipated by routers and network interfaces (NIs) and their contribution is expected to increase as technology scales [5]. In particular, we present a set of data encoding schemes operating at flit level and on an end-to-end basis, which allows us to minimize both the switching activity and

the coupling switching activity on links of the routing paths traversed by the packets.

The proposed encoding schemes, which are transparent with respect to the router implementation, are presented and discussed at both the algorithmic level and the architectural level, and assessed by means of simulation on synthetic and real traffic scenarios. The analysis takes into account several aspects and metrics of the design, including silicon area, power dissipation, and energy consumption. The results show that by using the proposed encoding schemes power and energy can be saved without any significant degradation in performance and with area overhead in the NI.

## II. OVERVIEW OF THE PROPOSAL

The basic idea of the proposed approach is encoding the flits before they are injected into the network with the goal of minimizing the self-switching activity and the coupling switching activity in the links traversed by the flits. In fact self-switching activity and coupling switching activity are responsible for link power dissipation. In this paper, we refer to the end-to-end scheme. This end-to-end encoding technique takes advantage of the pipeline nature of the wormhole switching technique [4]. Note that since the same sequence of flits passes through all the links of the routing path, the encoding decision taken at the NI may provide the same power saving for all the links. For the proposed scheme, an encoder and a decoder block are added to the NI. Except for the header flit, the encoder encodes the outgoing flits of the packet such that the power dissipated by the inter-router point-to-point link is minimized.

## III. PROPOSED ENCODING SCHEMES

## Recognition of License Plate for Straight and Inclined -Number Plates

J. SANKEERTHA<sup>1</sup>, V. PHANIBHUSHAN<sup>2</sup>

<sup>1</sup>PG Scholar, Dept of ECE, PBRVITS, JNTUA, Kavali, AP, India, E-mail: sankeerta.j@gmail.com.

<sup>2</sup>Associate Professor, Dept of ECE, PBRVITS, JNTUA, Kavali, AP, India.

**Abstract:** In this project, for detection of the inclined number plates Hough transform is used .The tilted number plate is converted into straight one which is analyzed by threshold methods to convert image into binary. Connected component analysis method (CCAT) is used to detect candidate objects inside the unknown image. Genetic algorithm (GA) plays a significant role here. Crossover operator which sorts the genes according to X and Y coordinates one at a time is used. The analysis is carried out using basic Image processing formulae and matlab.

**Keywords:** Image processing, Genetic Algorithms.

### I. INTRODUCTION

Analyzing the number plate is the most critical step in vehicle identification systems. There were many previously developed techniques like color based techniques, external shape based, edge based techniques. Out of which none proved to be efficiently working for detection .The main drawback of these techniques was their intensive computational demand and deviation in output characteristics when bumper stickers and model identification symbols are present.

### II. SYSTEM OVERVIEW

The proposed system has two sections of analysis. One section analyses the process of differentiating straight and angular images. The conversion of angular image into straight one is done .Straight ones are analysed by GA(Genetic Algorithm) phase. The optimum LP system locations depending on GRM(Geometric Relationship Matrix) is obtained. The proposed Flowchart is as shown in Fig.1.

### III. CHECKING IMAGE ANGLE

Image angle is checked if it is in inclined mode modification is done and made into position for easy detection of LP. This uses Hough transform technique. The implementation part deals with short line coding and quick computation.

#### A. Color to Gray Image

RGB to gray is performed by standard NTSC method by eliminating hue and saturation information while retaining the luminance as follows:

$$G_s = 0.299 * R + 0.587 * G + 0.114 * B. \quad (1)$$

#### B. Gray to Binary using Dynamic Threshold Method

Sensitive stage of analysis of LP detection is this one. The global threshold method is not suitable .Simple process of differentiating foreground and background is done. If pixel

intensity is higher than 90% of local mean, it is background and otherwise it is foreground. The 10% offset below the mean is chosen.

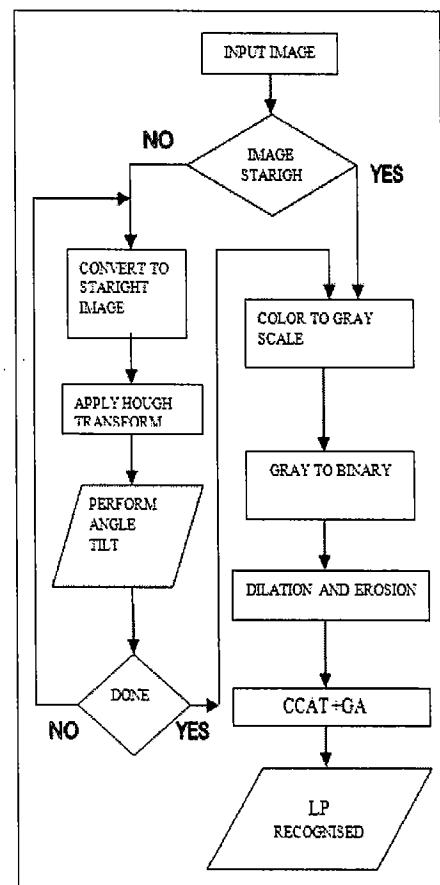


Fig.1. Flowchart.

## **Robust Document Image Binarization Technique for Degraded Document Images**

**Subba Rao Nasina**

M.tech Student,  
PBR VITS,  
Kavali, Nellore(D.t), A.P

**A Suman Kumar Reddy**

Associate Professor,  
PBR VITS,  
Kavali, Nellore(D.t), A.P

---

**Abstract:** Libraries and archives around the world store an abundance of old and historically important documents and manuscripts. These documents accumulate a significant amount of human heritage over time. Segmentation of text from badly degraded document images is a very challenging task due to the high inters/intravariation between the document background and the foreground text of different document images. In this paper, we propose a novel document image binarization technique that addresses these issues by using adaptive image contrast. The adaptive image contrast is a combination of the local image contrast and the local image gradient that is tolerant to text and background variation caused by different types of document degradations. In the proposed technique, an adaptive contrast map is first constructed for an input degraded document image. The contrast map is then binarized and combined with Canny's edge map to identify the text stroke edge pixels. The document text is further segmented by a local threshold that is estimated based on the intensities of detected text stroke edge pixels within a local window. The proposed method is simple, robust, and involves minimum parameter tuning. It has been tested on three public datasets that are used in the recent document image binarization contest (DIBCO) 2009 & 2011 and handwritten-DIBCO 2010 and achieves accuracies of 93.5%, 87.8%, and 92.03%, respectively that are significantly higher than or close to that of the best performing methods reported in the three contests. Experiments on the Bickley diary dataset that consists of several challenging bad quality document images also show the superior performance of our proposed method, compared with other techniques.

**Keywords:** optical character recognition (OCR), document analysis, document image processing, post processing, degraded document image binarization and pixel classification.

---

### **1. INTRODUCTION**

Documents image binarization is performed in the preprocessing stage for document analysis and it aims to segment the foreground text from the document background. A fast and accurate document image binarization technique is important for the ensuing document image processing tasks such as optical character recognition (OCR). Though document image binarization has been studied for many years, the thresholding of degraded document images is still an unsolved problem due to the high inter/intra variation between the text stroke and document background across different document images. Many environmental factors, improper handling, and the poor quality of the materials used in their creation cause them to suffer a high degree of degradation of various types. Today, there is a strong move toward digitization of these manuscripts to preserve their content for future generations. The huge amount of digital data produced requires automatic processing, enhancement, and recognition. A key step in all document image processing workflows is binarization, but this is not a very sophisticated process, which is unfortunate, as its performance has a significant influence on the quality of OCR results. Many research studies have been carried out to solve the problems that arise in the binarization of old document images characterized by many types of degradation including faded ink, bleed-through, show-through, uneven illumination, variations in image contrast, and deterioration of the cellulose structure. There are also differences in patterns of hand-written and machine-printed documents, which add to the difficulties associated with the binarization of old document images.

As illustrated, the handwritten text within the degraded documents often shows a certain amount of variation in terms of the stroke width, stroke brightness, stroke connection, and document background. In addition, historical documents are often degraded by the bleedthrough where the ink

**Automatic Number Plate Recognition System using an Improved Segmentation****P. SOWMYA<sup>1</sup>, N.KRISHNA CHAITANYA<sup>2</sup>**<sup>1</sup>PG Scholar, Dept of ECE, PBR Visvadaya Institute of Technology & Science, Kavali, A.P, India.<sup>2</sup>Associate Professor, Dept of ECE, PBR Visvadaya Institute of Technology & Science, Kavali, A.P, India.

**Abstract:** Automatic Number Plate Recognition (ANPR) is an active area of research. It is a real time embedded system which identifies the characters directly from the image of the license plate. ANPR system eliminates the use of radio frequency identification are very useful to the law enforcement agencies and similar equipments are minimized. Since number plate guidelines are not strictly practiced everywhere, it often becomes difficult to correctly identify the non-standard number plate characters. In this paper we try to address this problem of ANPR by using a pixel based segmentation algorithm of the alphanumeric characters in the license plate. The non-adherence of the system to any particular country-specific standard & fonts effectively means that this system can be used in many different countries a feature which can be especially useful for trans-border traffic e.g. use in country borders etc. Additionally, there is an option available to the end-user for retraining the Artificial Neural Network (ANN) by building a new sample font database. This can improve the system performance and make the system more efficient by taking relevant samples.

**Keywords:** ANPR, Artificial Neural Network, license plate, region growing, Component tag.

**I. INTRODUCTION**

The automatic number plate recognition systems(ANPR) exist for a long time, but only in the late 90s it became an important application because of the large increase in the number of vehicles. The information extracted from the license plates is mainly used for traffic monitoring, access control, parking, motorway road tolling, and border control, making car logs for parking systems, journey time measurement etc. by the law enforcement agencies. The recognition problem is generally sub-divided into 5 parts: (1) image acquisition i.e. capturing the image of the license plate (2) pre-processing the image i.e. normalization, adjusting the brightness, skewness and contrast of the image (3) localizing the license plate (4) character segmentation i.e. locating and identifying the individual symbol images on the plate, (5) optical character recognition. There may be further refinements over these (like matching the vehicle license number with a particular database to track suspected vehicles etc.) but the basic structure remains the same. A guiding parameter in this regard is country-specific traffic norms and standards. This helps to fine tune the system i.e. number of

characters in the license plate, text luminance level (relative index i.e. dark text on light background or light text on dark back ground) etc. So the problem can then be narrowed down for application in a particular country. For example, in India the norm is printing the license plate numbers in black colour on a white background for private vehicles and on a yellow background for commercial vehicles. The general format for the license plate is two letters (for state code) followed by district code, then a four digit code specific to a particular vehicle. In U.S.A no strict guidelines have been set regarding the fonts that can be used for this purpose.

**A. Related Works**

Such has been the impact of the ANPR systems that the scientific community started to take immense interest in this field since its introduction and today many commercial systems. They used a black pixel projection based image segmentation scheme to recognize Turkish number plates in the binary domain. They tried to localize the number plate in the image by using a smearing technique. Vertical and horizontal runs of the binarized image were taken. This was followed by segmentation of the plate from the rest of the image based on a particular threshold number of pixels. A similar algorithm was used to segment the component characters from the plate after the image was filtered and dilated. Cross correlation coefficient technique have been used to classify the text.



Fig1. Singapore number plate

Hough transform is another approach by which the boundary lines and eventually shapes are detected. The lines are first changed into parameter space of slope and intersect. Two parallel lines are then searched and the region in between the lines is passed as a potential plate region. Tran Duc Duan, Tran Le Hong Du, Tran Vinh Phuoc, and Nguyen Viet Hoang tried to use a contour based algorithm in association with the Hough transform to bring down the computational overhead. This contour algorithm narrows down the sample points on which the Hough transformation is to be applied. This is followed by a projection based

## **Implementation of Asymptotic Capacity of Large Relay Networks for Cooperative Communication**

**GORIPATHI SEENAIAH<sup>1</sup>, N.KRISHNA CHAITANYA<sup>2</sup>**

<sup>1</sup>PG Scholar, PBR Visvodaya Institute of Technology & Science, Kavali, Andhra Pradesh, India.

<sup>2</sup>Assistant Professor, PBR Visvodaya Institute of Technology & Science, Kavali, Andhra Pradesh, India.

**Abstract:** This paper analyzes the capacity of a wireless relay network composed of a large number of nodes that operate in an amplify-and-forward mode and that divide into a fixed number of levels. The capacity computation relies on the study of products of large random matrices, whose limiting Eigen value distribution is computed via a set of recursive equations. Using free probability theory and assuming that the noise power at relays but not at destination is negligible, the closed-form expression of the asymptotic instantaneous end-to-end mutual information is derived as the number of antennas at all levels grows large. The so-obtained deterministic expression is independent from the channel realizations while depending only on channel statistics. This expression is also shown to be equal to the asymptotic average end-to-end mutual information. The singular vectors of the optimal pre-coding matrices, maximizing the average mutual information with finite number of antennas at all levels, are also obtained. It turns out that these vectors are aligned to the eigenvectors of the channel correlation matrices. Thus they can be determined using only the channel statistics. As the structure of the singular vectors of the optimal pre-coders is independent from the system size, it is also optimal in the asymptotic regime.

**Keywords:** Large Relay Networks, Conferencing, Asymptotic, Decode-and-Forward, Amplify-and-Forward.

### **I. INTRODUCTION**

Many cooperation strategies have been proposed in the literature based on different relaying techniques, such as amplify and forward (AF), decode and forward (DF) and coded cooperation, compress and forward (CF) etc. when these schemes are employed in a pair-wise cooperating system as shown in the below figure. We can assume that, at each instant in time, only one user acts as the source while the other user serves as the relay that forwards the source's message to the destination. The role between the source and the relay can be interchanged at any instant in time. If the DF scheme is employed the relay will decode and regenerate a new message to the destination in the subsequent time slot. At provide better detection performance. As an extension to the DF scheme, the message generated by the relay can be re-encoded to provide addition error protection, and such a scheme can also be referred to as coded cooperation. If the AF scheme is employed, the relay simply amplifies the received signal and forwards it directly to the destination without explicitly decoding the message. The SR scheme, on the other hand, is a dynamic scheme where relays are selected to retransmit the source message only if the relay path is sufficiently reliable.

This scheme can be applied on the top of both AF and DF schemes to improve cooperation efficiency. Among the many cooperation schemes proposed in the literature, DF, AF, and SR schemes are the most basic and widely adopted. More

sophisticated schemes, such as the CF scheme can also be devised by exploiting the statistical dependencies between the messages received at the relay and destination but require higher implementation complexity. Most cooperation strategies involve two phases of transmission: the coordination phase and the cooperative transmission phase. Coordination is especially required in cooperative transmission phase. Coordination is especially required in cooperative systems since the antennas are distributed among different terminals, as opposed to that in centralized MIMO systems. Although extra coordination may reduce bandwidth inefficiency, the cost is often compensated for by the large diversity gains experienced at high SNR. Specifically coordination can be achieved either by direct inter-user communication or by the use of feedback from the destination. Based on the information obtained through coordination, cooperating partners will compute and transmit messages so as to reduce the transmission cost or enhance the detection performance at the receiver. The rest of the paper is organized as follows. In Section II, we introduce the Methodology. In Section III, we discuss the Cooperation in relay channels. In Section IV, we present some simulation and numerical results. Finally, the paper is concluded in Section V.

### **II. METHODOLOGY**

In this literature we introduce a conferencing link technique to increase the achievable rate of the system that is used for long transmission. For simplicity, the  $p$ -portion deterministic

# An Implementation of Adaptive Multipath Routing Algorithm for congestion control

**N.Krishna Chaitanya**

Research Scholar, ECE Department, JNTUCE,  
KAKINADA

**S.Varadarajan**

Professor, ECE Department, S V University College of  
Engineering TIRUPATI

## Abstract

This paper proposes a better adaptive multi path routing technique for routing the data packets effectively from source to destination under congestion at a router. In traditional adaptive multi path routing techniques, if congestion occurred at a router then the route is changed from source to destination. In a single path routing algorithm, all the data packets transmitted through a single path, where the time taken to transmit the packets is more. This drawback is eliminated by using multi path routing technique, where the packets are transmitted through different paths. The proposed method provides a better solution for minimizing the congestion by rerouting the data packets over other paths, which are not utilized by the same in multi-path routing. This method avoids the unnecessary dropping of packets at a congested router and improves the network performance.

## Keywords

Congestion, multi-path routing, Packets, router

## 1. Introduction

Most of the routing techniques in a network are based on a single path. As the number of data packets transferring increases, the data traffic increases in the network, as a result congestion will occur. To avoid this, multi-path routing [5] is preferred. In multi-path routing, the total available data is split and transferred among several paths. Many multi-path routing protocol techniques have been proposed in networks. Some of the multi path routing techniques are Simultaneous Multi Path Communication (SMPC) [1], and Distribution and Congestion Minimized Multipath (DCMM) routing [2]. The existing methods are used to reduce the congestion in multipath routing.

In multi-path routing, still there is possibility of occurrence of congestion. This paper proposes a method to avoid the congestion occurring in multipath routing. It reduces the unnecessary retransmissions and delay for data packets, which will affect the performance of the network. In order to avoid congestion, multi path routing along with load balancing is used [3, 4].

The rest of the paper organized as follows. Section 2 provides the overview on the existing multipath routing techniques. In Section 3, we introduce the proposed Adaptive Multipath Routing for Congestion Control (AMR-CC). The Section 4 discusses the flow chart used in

this method. Section 5 presents the simulation results, and section 6 concludes the paper.

## 2. Existing Methods

One of the multipath routing techniques is Simultaneous Multi-Path Communication [3]. There are two types of SMPC's available; they are (i) SMPC-I & (ii) SMPC-P. Here both the techniques are based on bandwidth control. In SPMC-I [1], all paths for communication are treated equally. The bandwidths of each path are controlled independently. In this technique, it is possible to control the bandwidth for each path with no information of any other path.

In SMPC-P [1], the priority will be given to the paths that are used for data transfer. If the total communication bandwidth used for data transfer is greater than the available bandwidth, it uses priority control scheme. In this, the communication bandwidth is controlled by decreasing the bandwidth of one of the paths in ascending order of priority level among the paths having a lower priority.

In these methods, still there exists a problem because of reducing the transmission bandwidth in the network, which will increase the data transmission delay and reduces the network performance.

Another existing method is Distribution and Congestion Minimized Multipath (DCMM) routing. Here, in this method, the routing decisions minimize network congestion, routing decisions address link congestion avoidance topology and maximum flow optimization. Here, number of paths in multi path routing is reduced, and as a result, it is unable to minimize the congestion [5]. Because of the limitations in the available techniques, a new technique has been proposed to minimize the network congestion and to improve network performance.

## 3. Proposed Method

A method was proposed with an algorithm, flow chart and presented by Chaitanya, N. Krishna, S. Varadarajan, and P.

## **Wireless Communication and GPRS Based Irrigation System**

**N. KRISHNA CHAITANYA<sup>1</sup>, D. SHILPA<sup>2</sup>**

<sup>1</sup>Assoc Prof, Dept of ECE, PBR Visvadaya Institute of Technology & Science, Kavali, Andhra Pradesh, India.

<sup>2</sup>PG Scholar, Dept of ECE, PBR Visvadaya Institute of Technology & Science, Kavali, Andhra Pradesh, India.

**Abstract:** To optimize water use for agricultural crops an automated irrigation system was developed. The system has a distributed wireless network of soil-moisture and temperature sensors placed in the root zone of the plants. Besides, a Gate way unit handles sensor information, triggers actuators, and transmits data to a web application. An algorithm was developed with threshold values of temperature and soil moisture that was programmed into a microcontroller-based gateway to control water quantity. The system was powered by photovoltaic panels and had a duplex communication link based on a cellular-Internet interface that allowed for data inspection and irrigation scheduling to be programmed through a web page. The automated system was tested in a sage crop field for 136 days and water savings of up to 90% compared with traditional irrigation practices of the agricultural zone were achieved. Three replicas of the automated system have been used successfully in other places for 18 months. Because of its energy autonomy and low cost, the system has the potential to be useful in water limited geographically isolated areas.

**Keywords:** Cellular Networks, Measurement, Automation, Internet, Wireless Sensor Networks (WSNs), Irrigation, Water Resources.

### **I. INTRODUCTION**

Agriculture utilizes 85% of available freshwater resources worldwide, and this percentage will continue to be dominant in water consumption because of population growth and increased food demand. There is an urgent need to create strategies based on science and technology for sustainable use of water, including technical, agronomic, managerial, and institutional improvements. There are different systems to achieve water savings in various crops, from basic ones to more technologically advanced ones. For instance, in one system plant water status was monitored and irrigation scheduled based on canopy temperature distribution of the plant, which was acquired with thermal imaging. Besides, other systems have been developed to schedule irrigation of crops and optimize water use by means of a crop water stress index (CWSI). The empirical CWSI was first defined over 30 years ago. This index was later calculated using measurements of infrared canopy temperatures, ambient air temperatures, and atmospheric vapor pressure deficit values to determine when to irrigate broccoli using drip irrigation. Irrigation systems can also be automated through information on volumetric water content of soil, using dielectric moisture sensors to control actuators and save water, instead of a predetermined irrigation schedule at a particular time of the day and with a specific duration.

An irrigation controller is used to open a solenoid valve and apply watering to bedding plants (*impatiens*, *petunia*, *salvia*, and *vinca*) when the volumetric water content of the substrate drops below a set point. An alternative parameter to

determine crop irrigation needs is estimating plant evapotranspiration (ET). ET is affected by weather parameters, including solar radiation, temperature, relative humidity, wind speed, and crop factors, such as stage of growth, variety and plant density, management elements, soil properties, pest, and disease control. Systems based on ET have been developed that allow water savings of up to 42% on time-based irrigation schedule. In Florida, automated switching tensiometers have been used in combination with ET calculated from historic weather data to control automatic irrigation schemes for papaya plants instead of using fixed scheduled ones. Soil water status and ET-based irrigation methods resulted in more sustainable practices compared with set schedule irrigation because of the lower water volumes applied. A system developed for malting barley cultivations in large areas of land allowed for the optimizing of irrigation through decision support software and its integration with an infiel wireless sensor network (WSN) driving an irrigation machine converted to make sprinkler nozzles controllable.

The network consisted of five sensing stations and a weather station. Each of the sensing stations contained a data logger with two soil water reflectometers, a soil temperature sensor, and Bluetooth communication. Using the network information and the irrigation machine positions through a differential GPS, the software controlled the sprinkler with application of the appropriate amount of water. Software dedicated to sprinkler control has been variously discussed. A data acquisition system was deployed for monitoring crop

## Melanoma Early Detection using Dual Classifier

N. KRISHNA CHAITANYA<sup>1</sup>, I. PAVANI<sup>2</sup>

<sup>1</sup>Associate Professor, Dept of ECE, PBR VITS, Kavali, AP, India.

<sup>2</sup>PG Scholar, Dept of ECE- VLSI, PBR VITS, Kavali, AP, India.

**Abstract:** Melanoma spreads through metastasis, and therefore it has been proved to be very fatal. A system to prevent this type of skin cancer is being awaited and is highly in-demand. It is important to highlight that excess exposure to radiations from the sun gradually erode melanin in the skin. Moreover, such radiations penetrate into the skin thereby destroying the melanocyte cells. Melanomas are asymmetrical and have irregular borders, notched edges, and color variations, so analyzing the shape, color, and texture of the skin lesion is important for melanoma early detection and prevention. In this work, the components of a portable real-time noninvasive skin lesion analysis system to assist in the melanoma prevention and early detection are proposed. The first component is a real-time alert to help users to prevent skin burn caused by sunlight; a novel equation to compute the time for skin to burn is thereby introduced. The second component is an automated image analysis including image acquisition, hair detection and exclusion, lesion segmentation, feature extraction, and classification. The framework has been developed in a smart-phone application. The experimental results show that the proposed system is efficient, achieving high classification accuracies.

**Keywords:** Image Segmentation, Skin Cancer, Melanoma.

### I. INTRODUCTION

Melanoma is the most frequent type of skin cancer and its incidence has been rapidly increasing over the last few decades. Nevertheless, it is also the most treatable kind of skin cancer, if diagnosed at an early stage. The clinical diagnosis of melanoma is commonly based on the ABCD rule, an analysis of four parameters (asymmetry, border irregularity, color, and dimension), or the 7-points checklist which is a scoring method for a set of different characteristics depending on color, shape, and texture. Melanoma, a type of skin cancer must be diagnosed at an early stage. Early diagnosis makes treatment effective and life of patient can be saved. Dermoscopy has become important technique in early diagnosis of melanoma. In this technique, oil is applied on skin surface where lesion is present and polarized light is made incident on skin. Then image is acquired with digital camera attached to dermatoscope. This process reveals the morphological structures which are present in deeper layer of skin. When image acquisition is done using dermatoscope, some artefacts are introduced in image. The hair which is present on skin can be segmented as lesion because of dark pixels being classified as lesion against lighter pixels which will be categorized as skin. So it is necessary to remove these hair pixels from acquired image. In some of the cases, dermatoscope is provided with ruler markings for measurement of diameter of lesion. So these markings will be there in acquired image. The air bubbles and black frame in image can affect the accuracy of segmentation process and further diagnosis of skin cancer. So these artefacts must be removed from dermoscopic image.

In some of the cases, contrast between skin and lesion can be very poor. It is needed to increase the contrast between skin and lesion. Histogram equalization based technique can be used for contrast enhancement. Histogram equalization gives good results for dermoscopic images. This involves remapping in gray levels to produce uniform distribution in input image. Improved contrast between the lesion and skin improves the accuracy of further diagnosis steps. Dermoscopy is a non-invasive diagnosis technique for the *in vivo* observation of pigmented skin lesions used in dermatology. Dermoscopic images have great potential in the early diagnosis of malignant melanoma, but their interpretation is time consuming and subjective, even for trained dermatologists. Therefore, there is currently a great interest in the development of computer-aided diagnosis systems that can assist the clinical evaluation of dermatologists. The standard approach in automatic dermoscopic image analysis has usually three stages:

- Image segmentation;
- Feature extraction and feature selection
- Lesion classification.

The segmentation stage is one of the most important since it affects the accuracy of the subsequent steps. However, segmentation is difficult because of the great variety of lesion shapes, sizes, and colors along with different skin types and textures. In addition, some lesions have irregular boundaries and in some cases there is a smooth transition between the lesion and the skin. Other difficulties are related to the presence of dark hair covering the lesions and the existence

# Location-Aware and Safer Cards

<sup>1</sup>N.Krishna Chaitanya, <sup>2</sup>K.Kavitha

<sup>1,2</sup>Dept of ECE, PBR Visvadaya Institute of Technology & Science, Kavali, AP, India

## **Abstract**

In this paper, we report on a new approach for improving security and privacy in certain RFID applications whereby location or location-related information (such as speed) can serve as a legitimate access context. Examples of these applications include access cards, toll cards, credit cards, and other payment tokens. We show that location awareness can be used by both tags and back-end servers for defending against unauthorized reading and relay attacks on RFID systems. On the tag side, we design a location-aware selective unlocking mechanism using which tags can selectively respond to reader interrogations rather than doing so promiscuously. On the server side, we design a location-aware secure transaction verification scheme that allows a bank server to decide whether to approve or deny a payment transaction and detect a specific type of relay attack involving malicious readers. The premise of our work is a current technological advancement that can enable RFID tags with low-cost location (GPS) sensing capabilities. Unlike prior research on this subject, our defenses do not rely on auxiliary devices or require any explicit user involvement.

## **Keywords**

Context Recognition, RFID, Mobile Payment System, Relay Attacks, Location Sensing

## **I. Introduction**

Low cost, small size, and the ability of allowing computerized identification of objects make Radio Frequency IDentification (RFID) systems increasingly ubiquitous in both public and private domains. Prominent RFID applications supply chain management (inventory control), e-passports, credit cards, driver's licenses, vehicle systems (toll collection or car key), access cards (building, parking or public transport), and medical implants. NFC, or Near Field Communication, is yet another upcoming RFID technology that allows devices, such as smart phones, to have both RFID tag and reader functionality. In particular, the use of NFC-equipped mobile devices as payment tokens (such as Google Wallet) is considered to be the next generation payment system and the latest buzz in the financial industry.

A typical RFID system consists of tags, readers, and/or back-end servers. Tags are miniaturized wireless radio devices that store information about their corresponding subject. Such information is usually sensitive and personally identifiable. For example, a US e-passport stores the name, nationality, date of birth, digital photograph, and (optionally) fingerprint of its owner. Readers broadcast queries to tags in their radio transmission ranges for information contained in tags and tags reply with such information. The queried information is then sent to the server (which may coexist with the reader) for further processing and the processing result is used to perform proper actions (such as updating inventory, opening gate, charging toll or approving payment).

Due to the inherent weaknesses of underlying wireless radio communication, RFID systems are plagued with a wide variety of security and privacy threats. A large number of these threats are due to the tag's promiscuous response to any reader requests. This renders sensitive tag information easily subject to unauthorized

reading. Information (might simply be a plain identifier) gleaned from a RFID tag can be used to track the owner of the tag, or be utilized to clone the tag so that an adversary can impersonate the tag's owner.

Promiscuous responses also incite different types of relay attacks. One class of these attacks is referred to as "ghost-and-leech". In this attack, an adversary, called a "leech," relays the information surreptitiously read from a legitimate RFID tag to a colluding entity known as a "ghost." The ghost can then relay the received information to a corresponding legitimate reader and vice versa in the other direction. This way a ghost and leech pair can succeed in impersonating a legitimate RFID tag without actually possessing the device.

A more severe form of relay attacks, usually against payment cards, is called "reader-and-ghost"; it involves a malicious reader and an unsuspecting owner intending to make a transaction in this attack, the malicious reader, serving the role of a leech and colluding with the ghost, can fool the owner of the card into approving a transaction which she did not intend to make (e.g., paying for a diamond purchase made by the adversary while the owner only intending to pay for food). We note that addressing this problem requires secure transaction verification, i.e., validation that the tag is indeed authorizing the intended payment amount.

The feasibility of executing relay attacks has been demonstrated on many RFID (or related) deployments, including the Chip-and-PIN credit card system, RFID assisted voting system, and keyless entry and start car key system. With the increasingly ubiquitous deployment of RFID applications, there is a pressing need for the development of security primitives and protocols to defeat unauthorized reading and relay attacks. However, providing security and privacy services for RFID systems presents a unique and formidable set of challenges. The inherent difficulty stems partially from the constraints of RFID tags in terms of computation, memory and power, and partially from the unusual usability requirements imposed by RFID applications (originally geared for automation). Consequently, solutions designed for RFID systems need to satisfy the requirements of the underlying RFID applications in terms of not only efficiency and security, but also usability.

In this paper, we report on our work on utilizing location information to defend against unauthorized reading and relay attacks in certain applications. We notice that in quite some applications, under normal circumstances, tags only need to communicate with readers at some specific locations or while undergoing a certain speed. For example, an access card to an office building needs to only respond to reader queries when it is near the entrance of the building; a credit card should only work in authorized retail stores; toll cards usually only communicate with toll readers in certain fixed locations (toll booths) or when the car travels at a certain speed. Hence, location or location-specific information can serve as a good means to establish a legitimate usage context.

# An Implementation of Adaptive Multipath Routing Algorithm for congestion control

N.Krishna Chaitanya, Research Scholar, ECE Department, JNTUCE, KAKINADA

S.Varadarajan, Professor, ECE Department, S V University College of Engineering, TIRUPATI

**Abstract:-** This paper proposes a better adaptive multi path routing technique for routing the data packets effectively from source to destination under congestion at a router. In traditional adaptive multi path routing techniques, if congestion occurred at a router then the route is changed from source to destination. In a single path routing algorithm, all the data packets transmitted through a single path, where the time taken to transmit the packets is more. This drawback is eliminated by using multi path routing technique, where the packets are transmitted through different paths. The proposed method provides a better solution for minimizing the congestion by rerouting the data packets over other paths, which are not utilized by the same in multi-path routing. This method avoids the unnecessary dropping of packets at a congested router and improves the network performance.

**Keywords:** Congestion, multi-path routing, Packets, router

## I. INTRODUCTION

Most of the routing techniques in a network are based on a single path. As the number of data packets transferring increases, the data traffic increases in the network, as a result congestion will occur. To avoid this, multi-path routing [5] is preferred. In multi-path routing, the total available data is split and transferred among several paths.

Many multi-path routing protocol techniques have been proposed in networks. Some of the multi path routing techniques are Simultaneous Multi Path Communication (SMPC) [1], and Distribution and Congestion Minimized Multipath (DCMM) routing [2]. The existing methods are used to reduce the congestion in multipath routing.

In multi-path routing, still there is every possibility of occurrence of congestion. This paper proposes a method to avoid the congestion occurring in multipath routing. It reduces the unnecessary retransmissions and delay for data

packets, which will effect on the performance of the network. In order to avoid congestion, multi path routing along with load balancing is used [3, 4].

The rest of the paper organized as follows. Section 2 provides the overview on the existing multipath routing techniques. In Section 3, we introduce the proposed Adaptive Multipath Routing for Congestion Control (AMR-CC). The Section 4 discusses the flow chart used in this method. Section 5 presents the simulation results, and section 6 concludes the paper.

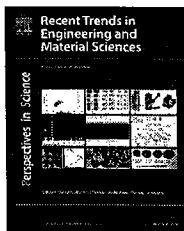
## II. EXISTING METHODS

One of the multipath routing techniques is Simultaneous Multi-Path Communication [3]. There are two types of SMPC's available; they are (i) SMPC-I & (ii) SMPC-P. Here both the techniques are based on bandwidth control.

In SPMC-I [1], all paths for communication are treated equally. The bandwidths of each path are controlled independently. In this technique, it is possible to control the bandwidth for each path with no information of any other path.

In SMPC-P [1], the priority will be given to the paths that are used for data transfer. If the total communication bandwidth used for data transfer is greater than the available bandwidth, it uses priority control scheme. In this, the communication bandwidth is controlled by decreasing the bandwidth of one of the paths in ascending order of priority level among the paths having a lower priority.

In these methods, still there exists a problem because of reducing the transmission bandwidth in the network, which will increase the data transmission delay and reduces the network performance.



# Load distribution using multipath-routing in wired packet networks: A comparative study<sup>☆</sup>



N. Krishna Chaitanya<sup>a,\*</sup>, S. Varadarajan<sup>b</sup>

<sup>a</sup> Research Scholar, ECE Department, JNTUCE, Kakinada, India

<sup>b</sup> Professor, ECE Department, S V University College of Engineering, Tirupati, India

Received 2 February 2016; accepted 11 April 2016

Available online 26 April 2016

## KEYWORDS

Multipath-routing;  
Load balancing;  
Congestion

**Summary** This paper aimed towards the analysis of various multipath routing techniques with and without load balancing as a comparative study. Most of the routing techniques targeted to find best path from source to destination. The basic routing techniques are based on single path; there is only one path from sending end to receiving end. There after multipath routing techniques has been proposed to send the data in multiple paths and eliminates the drawbacks in single path routing. This study gives better idea about multipath routing techniques along with load balance for avoiding congestion in wired packet networks.

© 2016 Published by Elsevier GmbH. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

## Introduction

Routing is the process of sending data from source to destination by making use of the best path through the network. Data packet can be routed either by using single and multipath routing techniques. In a single path routing, data is sent over a single path and in multipath routing, the data is sent over a number of multiple potential paths available at that instant (Domżał et al., 2015; Xin et al., 2009). As

the traffic on internet increases, congestion will occur in the network and its performance decreases (Tanaka, 2011). Most widely used routing to avoid congestion is multi path routing technique (Xin et al., 2009). Major advantage of multi-path routing: any failure in any path, data will be routed in alternate paths and hence throughput will increase dramatically (Domżał et al., 2015). A network is more efficient when a router is capable of dividing the traffic over multiple paths. Packet distribution and delivery is ensured by using multipath-routing technique (Li et al., 2011).

Load balancing is another technique used to eliminate congestion by distributing the data packets through the network based on available network resources. In load balance, it decides how much load should be sent over each path (Key et al., 2007). In which, number of paths is decided by multipath routing algorithm.

<sup>☆</sup> This article belongs to the special issue on Engineering and Material Sciences.

\* Corresponding author. Tel.: +91 8019255212.

E-mail address: nosinakc@gmail.com (N.K. Chaitanya).

# A Speed and Accurate binary multiplier for floating point values

Mudireddy Bala Subba Reddy<sup>1</sup>

T.Suneel Kumar<sup>2</sup>

## **Abstract:**

This paper exhibits a speed and accurate binary multiplier for floating point values in view of Dadda Algorithm. Multiplication of mantissa is carried out utilizing Dadda multiplier supplanting Carry Save Multiplier to enhance the speed of operation. The configuration attains to high speed with maximum recurrence of 526 MHz contrasted with existing floating point multipliers. The floating point multiplier is developed to handle the underflow and overflow occurrences. Adjusting is not brought to give more accuracy for mantissa multiplication. The multiplier is implemented utilizing Verilog HDL furthermore it is focused for Xilinx Virtex-5 FPGA. The multiplier is contrasted and Xilinx floating point multiplier core.

conceivable approaches to stand for real numbers as binary arrangement floating point numbers are; Binary interchange and Decimal interchange format according to the IEEE 754 standard [1]. Single precision normalized binary interchange arrangement is actualized in this outline. Such arrangement is indicated in Figure 1; beginning from MSB it has an one bit sign (S), an eight bit exponent (E), and a twenty three bit fraction called Mantissa (M). Including an additional bit to the fraction to structure and is characterized as significand. If exponent is more noteworthy than 0 and littler than 255, and there is 1 in the MSB of the significand then the number is said to be a normalized number; for this present case the real number is represented by equation (1).

$$Z = (-1)^S \times 2^{(E-\text{Bias})} \times (1.M) \quad (1)$$

## I. Introduction:

The vast majority of the DSP applications need multiplication of numbers of floating point type. The

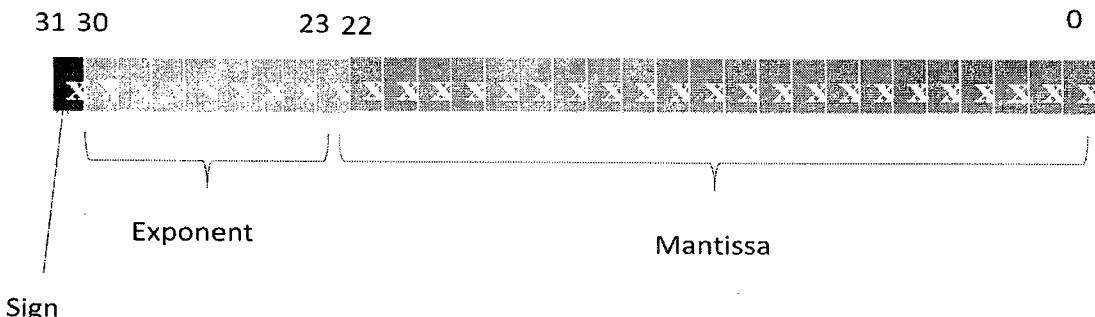


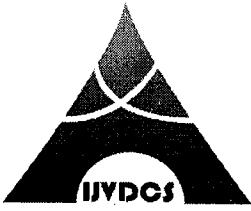
Fig 1: Representation of IEEE single precision floating point format

## II. Floating Point Multiplier Algorithm

Generally there are four stages to carry out the floating point multiplication of two numbers:

Step 1: Addition of two number's exponents and from this result subtracting the extra bias.

Step 2: Multiplication of the significands of the two numbers by the Dadda algorithm.

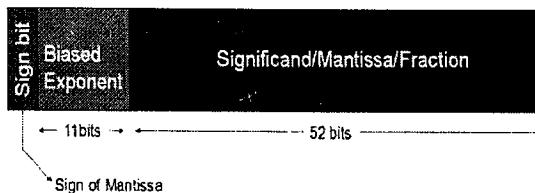
**Implementation of Double Precision Floating Point Multiplier****C. V. KAVYA SUVARCHALA<sup>1</sup>, B. SUKHADEV<sup>2</sup>**<sup>1</sup>Assistant Professor, Dept of ECE, PBR Visvadaya Institute of Technology & Science, Kavali, A.P, India.<sup>2</sup>PG Scholar, Dept of ECE, PBR Visvadaya Institute of Technology & Science, Kavali, AP, India.

**Abstract:** Floating Point (FP) multiplication is broadly utilized in large set of scientific and signal processing calculation. Multiplication is one of the common arithmetic operations in these computations. A high speed floating point double precision multiplier is implemented on a Virtex-6 FPGA. Besides, the proposed design is compliant with IEEE-754 format and handles over flow, under flow, rounding and various exception conditions. The design achieved the better operating frequency and area when compared to single precision.

**Keywords:** Double Precision, Floating Point, Multiplier, FPGA, IEEE-754.

**I. INTRODUCTION**

The real numbers represented in binary format are known as floating point numbers. Based on TEEE-754 standard, floating point formats are classified into binary and decimal interchange formats. Floating point multipliers are very important in DSP applications. This paper focuses on double precision normalized binary interchange format. Figure 1 shows the IEEE- 754 double precision binary format representation. Sign (S) is represented with one bit, exponent (E) and fraction (M or Mantissa) are represented with eleven and fifty two bits respectively. For a number is said to be a normalized number, it must consist of 'one' in the MSB of the significand and exponent is greater than zero and smaller than 1023. The real number is represented by equations (1) & (2).



**Fig1. IEEE-754 double precision floating point format.**

$$Z = (-1^S) * 2^{(E-Bias)} * (1.M)$$
$$Value = (-1^{Sign\ bit}) * 2^{(Exponent-1023)} * (1.Mantissa)$$

Floating point implementation on FPGAs has been the interest of many researchers. In [1], an IEEE-754 single precision pipelined floating point multiplier is implemented on multiple FPGAs (4 Actel A1280). Nabeel Shirazi, Walters, and Peter Athanas implemented custom 16/18 bit three stage pipelined floating point multiplier, that doesn't support rounding modes [2]. L.Louca, T.A.Cook, W.H. Johnson [3] implemented a single precision floating point

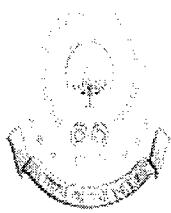
multiplier by using a digit-serial multiplier and Altera FLEX 8000. The design achieved 2.3 MFlops and doesn't support rounding modes. In [4], a parameterizable floating point multiplier is implemented using five stages pipeline, Handel-C software and Xilinx XC1000 FPGA. The design achieved the operating frequency of 28MFlops. The floating point unit [5] is implemented using the primitives of Xilinx Virtex II FPGA. The design achieved the operating frequency of 100 MHz with a latency of 4 clock cycles. Mohamed Al-Ashrafy, Ashraf Salem, and Wagdy Anis [6] implemented an efficient IEEE-754 single precision floating point multiplier and targeted for Xilinx Yirtex-5 FPGA. The multiplier handles the overflow and underflow cases but rounding is not implemented. The design achieves 301 MFLOPs with latency of three clock cycles. The multiplier was verified against Xilinx floating point multiplier core. The double precision floating point multiplier presented here is based on IEEE-754 binary floating standard. We have designed a high speed double precision floating point multiplier using Verilog language and ported on Xilinx Vertex-6 FPGA. It operates at a very high frequency of 414.714 MFlops and occupies 648 slices. It handles the overflow, underflow cases and rounding mode.

**II. FLOATING POINT MULTIPLICATION ALGORITHM**

Multiplying two numbers in floating point format is done by

1. Adding the exponent of the two numbers then
1. subtracting the bias from their result.
2. Multiplying the significand of the two numbers
3. Calculating the sign by XORing the sign of the two numbers.

In order to represent the multiplication result as a normalized number there should be 1 in the MSB of the result (leading one).



PARVATHAREDDY BABUL REDDY

VISVODAYA INSTITUTE OF TECHNOLOGY & SCIENCE

(Affiliated to J.N.T.U.A, Approved by AICTE and Accredited by NAAC with 'A' Grade)

KAVALI - 524201, S.P.S.R Nellore Dist., A.P. India. Ph: 08626-243930



DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

**INTERNATIONAL JOURNAL - SUMMARY**

SCHEMES	NO.OF INTERNATIONAL JOURNELS				
	2019-2020	2018-2019	2017-2018	2016-2017	2015-2016
INTERNATIONAL JOURNAL	7	16	21	17	16

Head of the Department  
Head of the Department  
B.E Visvodaya Institute of  
Technology & Science  
KAVALI - 524 201



**PARVATHAREDDY BABU REDDY**  
**VISWODA INSTITUTE OF TECHNOLOGY & SCIENCE**  
(Affiliated to J.N.T.U.A, Approved by AICTE and Accredited by NAAC with 'A' Grade)  
**KAVALLI – 524201, S.P.S.R Nellore Dist., A.P. India. Ph: 08626-243930**

## **DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING**

### **List of Publications**

**Academic Year: 2015-16**

S.No	Title of paper	Name of the author/s	Department of the teacher	Name of journal	Year of publication	ISSN number	Link to the recognition in UGC enlistment of the paper
1	Implementation of digital clock frequency multiplication & division using floating point multiplier	M. Pavitra	ECE	International Journal of Advanced Technology and Innovative Research	Dec, 2015	ISSN: 2348-2370	<a href="http://www.ijatir.org/uploads/153246IJATIR7904-589.pdf">http://www.ijatir.org/uploads/153246IJATIR7904-589.pdf</a>
2	Design of a high speed single precision floating point unit using Verilog	M. Pavitra	ECE	International Journal of Scientific Engineering & Technology Research	Dec, 2015	ISSN: 2319-8885	<a href="http://ijestr.com/uploads/531642IJESTR8017-1879.pdf">http://ijestr.com/uploads/531642IJESTR8017-1879.pdf</a>
3	Reduction Of Switching Activity In Noc By Using Data Encoding Schemes	R.S.Pratap Singh	ECE	International Journal Of Engineering And Computer Science	Aug, 2015	ISSN: 2319-7242	<a href="http://www.ijecs.in/index.php/ijecs/article/view/3226/3035">http://www.ijecs.in/index.php/ijecs/article/view/3226/3035</a>
4	Recognition of License Plate for Straight and Inclined - Number Plates	V.Phani Bhushan	ECE	International journal of Scientific Engineering and Technology Research	May, 2016	ISSN 2319-8885	<a href="http://www.ijestr.com">www.ijestr.com</a>
5	Robust document image binarization for degraded document images	A.Suman Kumar Reddy	ECE	International journal of innovative research in electronics and communications	July, 2015	ISSN: 2349-4042	<a href="http://www.arcjournals.org">www.arcjournals.org</a>
6	Automatic number plate recognition system using an improved segmentation	N.Krishna Chaitanya	ECE	International Journal of Innovative Technologies (IJTECH)	July, 2015	ISSN: 2321-8665,	
7	Implementation of asymptotic capacity of large relay networks for cooperative communication	N.Krishna Chaitanya	ECE	International Journal of Scientific Engineering and Technology Research (IJSETR)	July, 2015	ISSN : 2319-8885	

## Implementation of Digital Clock Frequency Multiplication and Division Using Floating Point Multiplier

K. PRAVEEN KUMAR<sup>1</sup>, M. PAVITRA<sup>2</sup>

<sup>1</sup>PG Scholar, Dept of ECE, PBR Visvadaya Institute of Technology & Science, Kavali, AP, India.

<sup>2</sup>Associate Professor, Dept of ECE, PBR Visvadaya Institute of Technology & Science, Kavali, AP, India.

**Abstract:** A digital clock frequency multiplier, divider using floating point multiplier which generates the output clock with almost zero frequency error has been presented. The circuit has a wide range of multiplication factors and less delay time, with an internal reference clock period of 2ps has been verified with random multiplication factor values. The design is implemented in Verilog HDL, simulated with Modelsim tool.

**Keywords:** Clock, Clock Multiplication, Clock Division, Floating Point Multiplier.

### I. INTRODUCTION

In synchronous digital circuits, we need a signal that oscillates between a high and a low state and is used to coordinate actions of circuits which is known as clock signal. A clock signal is generated by a clock generator using a crystal. In general the clock signal is a square wave with a 50% duty cycle, usually with a fixed, constant frequency. Many modern microcomputers use a "clock multiplier" which multiplies a lower frequency external clock to the appropriate clock rate of the microprocessor. This allows the CPU to operate at a much higher frequency than the rest of the computer, which affords performance gains in situations where the CPU does not need to wait on an external factor (like memory or input/output). Clock frequency multipliers and dividers are widely used in Integrated Circuits. Conventionally, phase locked loops (PLLs) are used as clock frequency multipliers and dividers to increase or decrease the frequency of an input clock signal. However, PLLs require much time and design efforts to ensure stability. And also PLLs consume large silicon area and often require different external components for usage, resulting in high cost. Because of high lock time of PLL, the input clock signal frequency cannot be changed quickly. PLLs are only suited for handling input clock signals of limited frequency and duty cycle ranges, and individual PLLs have limited multiplication ranges.

The other method of multiplying the frequency is to convert the input frequency to an analog voltage, process the voltage using op-amp, and then convert the processed voltage to a frequency using a V/F converter. At low frequencies, the Frequency to Voltage converter cannot produce a steady voltage output. A large amount of ripple is produced which

may be easily eliminated using DC filters, but the response time of the system becomes very high which is unacceptable. Extensive work has been done on building clock multipliers and dividers, different circuits have been proposed. Still, the major consideration while implementing clock multipliers and dividers will be, to improve the accuracy of the output clock frequency value as much as possible. This issue is being addressed in this paper. The proposed architecture attempts to address the above mentioned issues associated with PLLs, F/V and V/F converters. It has a wide multiplication and division factor range and can generate an output clock with an accurate frequency. The proposed architecture can be used with an input signal of any duty cycle varying from 10-90% and with any multiplication factor.

### II. DESIGN ALGORITHM

The existing algorithm for clock frequency multiplication is based on determining the time period of input clock signal with a high frequency. In order to determine an accurate value of the input clock signal time period, a very high frequency clock should be used, which in turn requires a high frequency clock generation circuit. If the input clock signal and high frequency signal are from different sources, then a synchronizing circuit is required to reduce the phase difference between the clock and high frequency signal. In the proposed digital clock frequency multiplier, instead of a high frequency signal, an internal reference clock is generated to determine time periods. The algorithm of the proposed frequency multiplier is as follows:

**Step 1:** Receive an Input clock signal which has to be multiplied, the multiplication factor (MF).

**Step 2:** With the help of reference internal clock, determine Total time period, ON time and OFF time of an input clock signal.

**Step 3:** Convert the obtained time periods (from step 2) and Multiplication factor (MF) to the IEEE 754 standard format.

**Step 4:** By using floating point multiplication algorithm, multiply the time periods (from step 3) with the multiplication factor (MF) in order to determine the required Total time period, ON time period and OFF time period of output clock signal.

## Design of a High Speed Single Precision Floating Point Unit using Verilog

R. VAMSI KRISHNA<sup>1</sup>, M. PAVITRA<sup>2</sup>

<sup>1</sup>PG Scholar, Dept Of ECE, PBR Visvodaya Institute of Technology & Science, Kavali, AP, India.

<sup>2</sup>Associate Professor, Dept Of ECE, PBR Visvodaya Institute of Technology & Science, Kavali, India.

**Abstract:** The integer representation is no longer appropriate to represent the larger values. These larger values can be represented using the IEEE-754 standard based floating point representation. This paper presents high speed floating point arithmetic unit which can perform addition, subtraction, multiplication, functions on 32-bit operands that use the IEEE 754-2008 standard. Pre-normalization unit and post-normalization units are also discussed along with exceptional handling. All the functions are built by feasible efficient algorithms with several changes introduced that can improve overall latency. The algorithms are modeled in Verilog HDL and have been implemented in modelsim.

**Keywords:** Floating Point Number, Normalization, Latency, Overflow, Exceptions, Underflow, Etc.

### I. INTRODUCTION

An arithmetic circuit which performs digital arithmetic operations has many applications in digital coprocessors, application specific circuits, etc. Because of the advancements in the VLSI technology, many complex algorithms that appeared impractical to put into practice, have become easily realizable today with desired performance parameters so that new designs can be incorporated. The standardized methods to represent floating point numbers have been instituted by the IEEE 754 standard through which the floating point operations can be carried out efficiently with modest storage requirements. IEEE 754 standard floating point numbers have three parts, they are the sign, the exponent, and the mantissa. The sign bit is of 1 bit where 0 refers to positive number and 1 refers to negative number. The mantissa, also called significand which is of 23bits composes of the fraction and a leading digit which represents the precision bits of the number. The exponent with 8 bits represents both positive and negative exponents. A bias is added to the exponent, when it is stored as floating point number. A bias of 127 is added to the exponent to get the stored exponent. Table 1 show the bit ranges for single (32-bit) and double (64-bit) precision floating-point values. A floating point number representation is shown in table 2 The value of binary floating point representation is as follows where S is sign bit, F is fraction bit and E is exponent field. Value of a floating point number=  $(-1)^S \times \text{val}(F) \times 2^{\text{val}(E)}$ .

**TABLE I: Bit Range for Single (32-Bit) and Double (64-Bit) Precision Floating-Point Values**

	Sign	Exponent	Fraction	Bias
Single precision	1[31]	8[30-23]	23[22-0]	127
Double precision	1[63]	11[62-52]	52[51-0]	1023

There are four types of exceptions that occur during floating point operations. The Overflow exception is occur whenever the result cannot be represented as a finite value in the precision format of the destination. The Underflow exception occurs when an intermediate result is too small to be calculated accurately, or if the operation's result rounded to the destination precision is too small to be normalized. The Division by zero exception arises when a finite nonzero number is divided by zero. The Invalid operation exception is raised if the given operands are invalid for the operation to be performed.

**TABLE II: Floating Point Number Representation**

32 bits		
Sign	Exponent	Mantissa
1 bit	8 bits	23 bits

### II. ARCHITECTURE AND METHODOLOGY

The single precision floating point unit performs add, subtract, multiply functions is shown in fig.1. Two pre-normalization units for addition, subtraction and multiplication, division operations has been given. Post normalization unit also has been given that normalizes the mantissa part. The final result can be obtained after post-normalization. To do the arithmetic operations, two IEEE-754 format single precision operands are considered. Pre-normalization of the operands is done for easy recognition of the operands. After completion of the selected operation post-normalization is preformed on the output obtained. At last the exceptions occurred are detected and handled using exceptional handling. The executed operation depends on a three bit control signal (z) which will determine the arithmetic operation is shown in table 3.

## Reduction Of Switching Activity In Noc By Using Data Encoding Schemes

Y.Supraba, R.S.Pratap Singh

P.b.r visvodaya institute of technology and science  
Kavali, s.p.sr.nellore, india

[ysupraba4@gmail.com](mailto:ysupraba4@gmail.com)

P.b.r visvodaya institute of technology and science  
Kavali, s.p.sr.nellore, india  
[rpsvits@rediffmail.com](mailto:rpsvits@rediffmail.com)

**Abstract:** As technology shrinks, the power dissipated by the links of a network-on-chip (NOC) starts to compete with the power dissipated by the other elements of the communication subsystem, namely, the routers and the network interfaces (NIs). In this paper we present a reduction of switching activity in network on chip (NOC) by using data encoding schemes. In proposed schemes there is no need to change link architecture and it will reduce transitions (i.e. nothing but switching activity contains both switching transitions and coupling transitions). due to these transitions lot of power consumption is presented at the network on chip and routers so that by using data encoding schemes we can save consumption of energy and dissipation of power without any degradation of performance.

**Keywords:** Coupling switching activity, data encoding, low power, network-on-chip (NoC), power analysis.

### 1. INTRODUCTION:

Global interconnect length does not scale with smaller transistors and local wires. Chip size remains relatively constant because the chip function continues to increase and RC delay increases exponentially. At 32/28 nm, for instance, the RC delay in a 1-mm global wire at the minimum pitch is 25× higher than the intrinsic delay of a two-input NAND fan out of 5 [1]. If the raw computation horsepower seems to be unlimited, thanks to the ability of instancing more and more cores in a single silicon die, scalability issues, due to the need of making efficient and reliable communication between the increasing number of cores, become the real problem [3]. The network on- chip (NOC) design paradigm [4] is recognized as the most viable way to tackle with scalability and variability issues that characterize the ultra deep sub micron meter era. Nowadays, the on-chip communication issues are as relevant as, and in some cases more relevant than, the computation related issues [4]. In fact, the communication subsystem increasingly impacts the traditional design objectives, including cost (i.e., silicon area), performance, power dissipation, energy consumption, reliability, etc. As technology shrinks, an ever more significant fraction of the total power budget of a complex many-core system-on-chip (SOC) is due to the communication subsystem.

In this paper, we focus on techniques aimed at reducing the power dissipated by the network links. In fact, the power dissipated by the network links is as relevant as that dissipated by routers and network interfaces (NIs) and their contribution is expected to increase as technology scales [5]. In particular, we present a set of data encoding schemes operating at flit level and on an end-to-end basis, which allows us to minimize both the switching activity and

the coupling switching activity on links of the routing paths traversed by the packets.

The proposed encoding schemes, which are transparent with respect to the router implementation, are presented and discussed at both the algorithmic level and the architectural level, and assessed by means of simulation on synthetic and real traffic scenarios. The analysis takes into account several aspects and metrics of the design, including silicon area, power dissipation, and energy consumption. The results show that by using the proposed encoding schemes power and energy can be saved without any significant degradation in performance and with area overhead in the NI.

### II. OVERVIEW OF THE PROPOSAL

The basic idea of the proposed approach is encoding the flits before they are injected into the network with the goal of minimizing the self-switching activity and the coupling switching activity in the links traversed by the flits. In fact self-switching activity and coupling switching activity are responsible for link power dissipation. In this paper, we refer to the end-to-end scheme. This end-to-end encoding technique takes advantage of the pipeline nature of the wormhole switching technique [4]. Note that since the same sequence of flits passes through all the links of the routing path, the encoding decision taken at the NI may provide the same power saving for all the links. For the proposed scheme, an encoder and a decoder block are added to the NI. Except for the header flit, the encoder encodes the outgoing flits of the packet such that the power dissipated by the inter-router point-to-point link is minimized.

### III. PROPOSED ENCODING SCHEMES

## Recognition of License Plate for Straight and Inclined -Number Plates

J. SANKEERTHA<sup>1</sup>, V. PHANIBHUSHAN<sup>2</sup>

<sup>1</sup>PG Scholar, Dept of ECE, PBRVITS, JNTUA, Kavali, AP, India, E-mail: sankeerta.j@gmail.com.

<sup>2</sup>Associate Professor, Dept of ECE, PBRVITS, JNTUA, Kavali, AP, India.

**Abstract:** In this project, for detection of the inclined number plates Hough transform is used .The tilted number plate is converted into straight one which is analyzed by threshold methods to convert image into binary. Connected component analysis method (CCAT) is used to detect candidate objects inside the unknown image. Genetic algorithm (GA) plays a significant role here. Crossover operator which sorts the genes according to X and Y coordinates one at a time is used. The analysis is carried out using basic Image processing formulae and matlab.

**Keywords:** Image processing, Genetic Algorithms.

### I. INTRODUCTION

Analyzing the number plate is the most critical step in vehicle identification systems. There were many previously developed techniques like color based techniques, external shape based, edge based techniques. Out of which none proved to be efficiently working for detection .The main drawback of these techniques was their intensive computational demand and deviation in output characteristics when bumper stickers and model identification symbols are present.

### II. SYSTEM OVERVIEW

The proposed system has two sections of analysis. One section analyses the process of differentiating straight and angular images. The conversion of angular image into straight one is done .Straight ones are analyzed by GA(Genetic Algorithm) phase. The optimum LP system locations depending on GRM(Geometric Relationship Matrix) is obtained. The proposed Flowchart is as shown in Fig.1.

### III. CHECKING IMAGE ANGLE

Image angle is checked if it is in inclined mode modification is done and made into position for easy detection of LP. This uses Hough transform technique. The implementation part deals with short line coding and quick computation.

#### A. Color to Gray Image

RGB to gray is performed by standard NTSC method by eliminating hue and saturation information while retaining the luminance as follows:

$$G_s = 0.299 * R + 0.587 * G + 0.114 * B. \quad (1)$$

#### B. Gray to Binary using Dynamic Threshold Method

Sensitive stage of analysis of LP detection is this one. The global threshold method is not suitable .Simple process of differentiating foreground and background is done. If pixel

intensity is higher than 90% of local mean, it is background and otherwise it is foreground. The 10% offset below the mean is chosen.

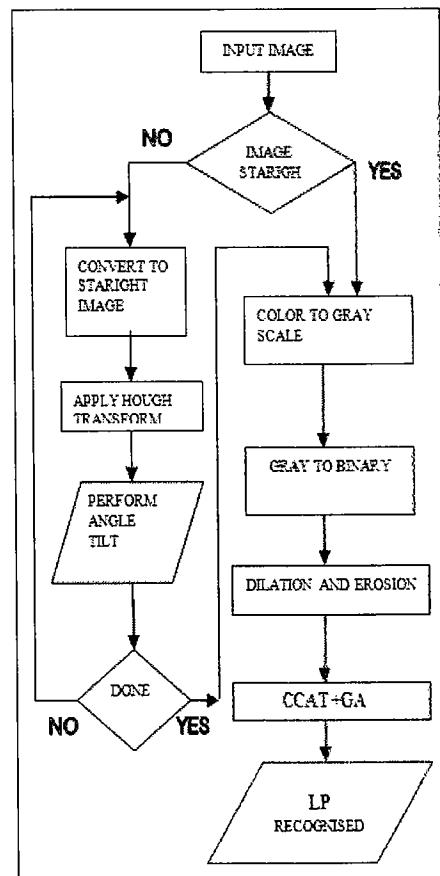


Fig.1. Flowchart.

## **Robust Document Image Binarization Technique for Degraded Document Images**

**Subba Rao Nasina**

M.tech Student,  
PBR VITS,  
Kavali, Nellore(D.t), A.P

**A Suman Kumar Reddy**

Associate Professor,  
PBR VITS,  
Kavali, Nellore(D.t), A.P

---

**Abstract:** Libraries and archives around the world store an abundance of old and historically important documents and manuscripts. These documents accumulate a significant amount of human heritage over time. Segmentation of text from badly degraded document images is a very challenging task due to the high inters/intravariation between the document background and the foreground text of different document images. In this paper, we propose a novel document image binarization technique that addresses these issues by using adaptive image contrast. The adaptive image contrast is a combination of the local image contrast and the local image gradient that is tolerant to text and background variation caused by different types of document degradations. In the proposed technique, an adaptive contrast map is first constructed for an input degraded document image. The contrast map is then binarized and combined with Canny's edge map to identify the text stroke edge pixels. The document text is further segmented by a local threshold that is estimated based on the intensities of detected text stroke edge pixels within a local window. The proposed method is simple, robust, and involves minimum parameter tuning. It has been tested on three public datasets that are used in the recent document image binarization contest (DIBCO) 2009 & 2011 and handwritten-DIBCO 2010 and achieves accuracies of 93.5%, 87.8%, and 92.03%, respectively that are significantly higher than or close to that of the best performing methods reported in the three contests. Experiments on the Bickley diary dataset that consists of several challenging bad quality document images also show the superior performance of our proposed method, compared with other techniques.

**Keywords:** optical character recognition (OCR), document analysis, document image processing, post processing, degraded document image binarization and pixel classification.

---

### **1. INTRODUCTION**

Documents image binarization is performed in the preprocessing stage for document analysis and it aims to segment the foreground text from the document background. A fast and accurate document image binarization technique is important for the ensuing document image processing tasks such as optical character recognition (OCR). Though document image binarization has been studied for many years, the thresholding of degraded document images is still an unsolved problem due to the high inter/intra variation between the text stroke and document background across different document images. Many environmental factors, improper handling, and the poor quality of the materials used in their creation cause them to suffer a high degree of degradation of various types. Today, there is a strong move toward digitization of these manuscripts to preserve their content for future generations. The huge amount of digital data produced requires automatic processing, enhancement, and recognition. A key step in all document image processing workflows is binarization, but this is not a very sophisticated process, which is unfortunate, as its performance has a significant influence on the quality of OCR results. Many research studies have been carried out to solve the problems that arise in the binarization of old document images characterized by many types of degradation including faded ink, bleed-through, show-through, uneven illumination, variations in image contrast, and deterioration of the cellulose structure. There are also differences in patterns of hand-written and machine-printed documents, which add to the difficulties associated with the binarization of old document images.

As illustrated, the handwritten text within the degraded documents often shows a certain amount of variation in terms of the stroke width, stroke brightness, stroke connection, and document background. In addition, historical documents are often degraded by the bleedthrough where the ink

**Automatic Number Plate Recognition System using an Improved Segmentation****P. SOWMYA<sup>1</sup>, N.KRISHNA CHAITANYA<sup>2</sup>**<sup>1</sup>PG Scholar, Dept of ECE, PBR Visvodaya Institute of Technology & Science, Kavali, A.P, India.<sup>2</sup>Associate Professor, Dept of ECE, PBR Visvodaya Institute of Technology & Science, Kavali, A.P, India.

**Abstract:** Automatic Number Plate Recognition (ANPR) is an active area of research. It is a real time embedded system which identifies the characters directly from the image of the license plate. ANPR system eliminates the use of radio frequency identification are very useful to the law enforcement agencies and similar equipments are minimized. Since number plate guidelines are not strictly practiced everywhere, it often becomes difficult to correctly identify the non-standard number plate characters. In this paper we try to address this problem of ANPR by using a pixel based segmentation algorithm of the alphanumeric characters in the license plate. The non-adherence of the system to any particular country-specific standard & fonts effectively means that this system can be used in many different countries a feature which can be especially useful for trans-border traffic e.g. use in country borders etc. Additionally, there is an option available to the end-user for retraining the Artificial Neural Network (ANN) by building a new sample font database. This can improve the system performance and make the system more efficient by taking relevant samples.

**Keywords:** ANPR, Artificial Neural Network, license plate, region growing, Component tag.

**I. INTRODUCTION**

The automatic number plate recognition systems(ANPR) exist for a long time, but only in the late 90s it became an important application because of the large increase in the number of vehicles. The information extracted from the license plates is mainly used for traffic monitoring, access control, parking, motorway road tolling, and border control, making car logs for parking systems, journey time measurement etc. by the law enforcement agencies. The recognition problem is generally sub-divided into 5 parts: (1) image acquisition i.e. capturing the image of the license plate (2) pre-processing the image i.e. normalization, adjusting the brightness, skewness and contrast of the image (3) localizing the license plate (4) character segmentation i.e. locating and identifying the individual symbol images on the plate, (5) optical character recognition. There may be further refinements over these (like matching the vehicle license number with a particular database to track suspected vehicles etc.) but the basic structure remains the same. A guiding parameter in this regard is country-specific traffic norms and standards. This helps to fine tune the system i.e. number of

characters in the license plate, text luminance level (relative index i.e. dark text on light background or light text on dark background) etc. So the problem can then be narrowed down for application in a particular country. For example, in India the norm is printing the license plate numbers in black colour on a white background for private vehicles and on a yellow background for commercial vehicles. The general format for the license plate is two letters (for state code) followed by district code, then a four digit code specific to a particular vehicle. In U.S.A no strict guidelines have been set regarding the fonts that can be used for this purpose.

**A. Related Works**

Such has been the impact of the ANPR systems that the scientific community started to take immense interest in this field since its introduction and today many commercial systems. They used a black pixel projection based image segmentation scheme to recognize Turkish number plates in the binary domain. They tried to localize the number plate in the image by using a smearing technique. Vertical and horizontal runs of the binarized image were taken. This was followed by segmentation of the plate from the rest of the image based on a particular threshold number of pixels. A similar algorithm was used to segment the component characters from the plate after the image was filtered and dilated. Cross correlation coefficient technique have been used to classify the text.



Fig1. Singapore number plate

Hough transform is another approach by which the boundary lines and eventually shapes are detected. The lines are first changed into parameter space of slope and intersect. Two parallel lines are then searched and the region in between the lines is passed as a potential plate region. Tran Duc Duan, Tran Le Hong Du, Tran Vinh Phuoc, and Nguyen Viet Hoang tried to use a contour based algorithm in association with the Hough transform to bring down the computational overhead. This contour algorithm narrows down the sample points on which the Hough transformation is to be applied. This is followed by a projection based

## **Implementation of Asymptotic Capacity of Large Relay Networks for Cooperative Communication**

**GORIPATHI SEENAIH<sup>1</sup>, N.KRISHNA CHAITANYA<sup>2</sup>**

<sup>1</sup>PG Scholar, PBR Visvodaya Institute of Technology & Science, Kavali, Andhra Pradesh, India.

<sup>2</sup>Assistant Professor, PBR Visvodaya Institute of Technology & Science, Kavali, Andhra Pradesh, India.

**Abstract:** This paper analyzes the capacity of a wireless relay network composed of a large number of nodes that operate in an amplify-and-forward mode and that divide into a fixed number of levels. The capacity computation relies on the study of products of large random matrices, whose limiting Eigen value distribution is computed via a set of recursive equations. Using free probability theory and assuming that the noise power at relays but not at destination is negligible, the closed-form expression of the asymptotic instantaneous end-to-end mutual information is derived as the number of antennas at all levels grows large. The so-obtained deterministic expression is independent from the channel realizations while depending only on channel statistics. This expression is also shown to be equal to the asymptotic average end-to-end mutual information. The singular vectors of the optimal pre-coding matrices, maximizing the average mutual information with finite number of antennas at all levels, are also obtained. It turns out that these vectors are aligned to the eigenvectors of the channel correlation matrices. Thus they can be determined using only the channel statistics. As the structure of the singular vectors of the optimal pre-coders is independent from the system size, it is also optimal in the asymptotic regime.

**Keywords:** Large Relay Networks, Conferencing, Asymptotic, Decode-and-Forward, Amplify-and-Forward.

### **I. INTRODUCTION**

Many cooperation strategies have been proposed in the literature based on different relaying techniques, such as amplify and forward (AF), decode and forward (DF) and coded cooperation, compress and forward (CF) etc. when these schemes are employed in a pair-wise cooperating system as shown in the below figure. We can assume that, at each instant in time, only one user acts as the source while the other user serves as the relay that forwards the source's message to the destination. The role between the source and the relay can be interchanged at any instant in time. If the DF scheme is employed the relay will decode and regenerate a new message to the destination in the subsequent time slot. At provide better detection performance. As an extension to the DF scheme, the message generated by the relay can be re-encoded to provide addition error protection, and such a scheme can also be referred to as coded cooperation. If the AF scheme is employed, the relay simply amplifies the received signal and forwards it directly to the destination without explicitly decoding the message. The SR scheme, on the other hand, is a dynamic scheme where relays are selected to retransmit the source message only if the relay path is sufficiently reliable.

This scheme can be applied on the top of both AF and DF schemes to improve cooperation efficiency. Among the many cooperation schemes proposed in the literature, DF, AF, and SR schemes are the most basic and widely adopted. More

sophisticated schemes, such as the CF scheme can also be devised by exploiting the statistical dependencies between the messages received at the relay and destination but require higher implementation complexity. Most cooperation strategies involve two phases of transmission: the coordination phase and the cooperative transmission phase. Coordination is especially required in cooperative transmission phase. Coordination is especially required in cooperative systems since the antennas are distributed among different terminals, as opposed to that in centralized MIMO systems. Although extra coordination may reduce bandwidth inefficiency, the cost is often compensated for by the large diversity gains experienced at high SNR. Specifically coordination can be achieved either by direct inter-user communication or by the use of feedback from the destination. Based on the information obtained through coordination, cooperating partners will compute and transmit messages so as to reduce the transmission cost or enhance the detection performance at the receiver. The rest of the paper is organized as follows. In Section II, we introduce the Methodology. In Section III, we discuss the Cooperation in relay channels. In Section IV, we present some simulation and numerical results. Finally, the paper is concluded in Section V.

### **II. METHODOLOGY**

In this literature we introduce a conferencing link technique to increase the achievable rate of the system that is used for long transmission. For simplicity, the  $p$ -portion deterministic

## **Wireless Communication and GPRS Based Irrigation System**

**N. KRISHNA CHAITANYA<sup>1</sup>, D. SHILPA<sup>2</sup>**

<sup>1</sup>Assoc Prof, Dept of ECE, PBR Visvodaya Institute of Technology & Science, Kavali, Andhra Pradesh, India.

<sup>2</sup>PG Scholar, Dept of ECE, PBR Visvodaya Institute of Technology & Science, Kavali, Andhra Pradesh, India.

**Abstract:** To optimize water use for agricultural crops an automated irrigation system was developed. The system has a distributed wireless network of soil-moisture and temperature sensors placed in the root zone of the plants. Besides, a Gate way unit handles sensor information, triggers actuators, and transmits data to a web application. An algorithm was developed with threshold values of temperature and soil moisture that was programmed into a microcontroller-based gateway to control water quantity. The system was powered by photovoltaic panels and had a duplex communication link based on a cellular-Internet interface that allowed for data inspection and irrigation scheduling to be programmed through a web page. The automated system was tested in a sage crop field for 136 days and water savings of up to 90% compared with traditional irrigation practices of the agricultural zone were achieved. Three replicas of the automated system have been used successfully in other places for 18 months. Because of its energy autonomy and low cost, the system has the potential to be useful in water limited geographically isolated areas.

**Keywords:** Cellular Networks, Measurement, Automation, Internet, Wireless Sensor Networks (WSNs), Irrigation, Water Resources.

### **I. INTRODUCTION**

Agriculture utilizes 85% of available freshwater resources worldwide, and this percentage will continue to be dominant in water consumption because of population growth and increased food demand. There is an urgent need to create strategies based on science and technology for sustainable use of water, including technical, agronomic, managerial, and institutional improvements. There are different systems to achieve water savings in various crops, from basic ones to more technologically advanced ones. For instance, in one system plant water status was monitored and irrigation scheduled based on canopy temperature distribution of the plant, which was acquired with thermal imaging. Besides, other systems have been developed to schedule irrigation of crops and optimize water use by means of a crop water stress index (CWSI). The empirical CWSI was first defined over 30 years ago. This index was later calculated using measurements of infrared canopy temperatures, ambient air temperatures, and atmospheric vapor pressure deficit values to determine when to irrigate broccoli using drip irrigation. Irrigation systems can also be automated through information on volumetric water content of soil, using dielectric moisture sensors to control actuators and save water, instead of a predetermined irrigation schedule at a particular time of the day and with a specific duration.

An irrigation controller is used to open a solenoid valve and apply watering to bedding plants (impatiens, petunia, salvia, and vinca) when the volumetric water content of the substrate drops below a set point. An alternative parameter to

determine crop irrigation needs is estimating plant evapotranspiration (ET). ET is affected by weather parameters, including solar radiation, temperature, relative humidity, wind speed, and crop factors, such as stage of growth, variety and plant density, management elements, soil properties, pest, and disease control. Systems based on ET have been developed that allow water savings of up to 42% on time-based irrigation schedule. In Florida, automated switching tensiometers have been used in combination with ET calculated from historic weather data to control automatic irrigation schemes for papaya plants instead of using fixed scheduled ones. Soil water status and ET-based irrigation methods resulted in more sustainable practices compared with set schedule irrigation because of the lower water volumes applied. A system developed for malting barley cultivations in large areas of land allowed for the optimizing of irrigation through decision support software and its integration with an infiel wireless sensor network (WSNs) driving an irrigation machine converted to make sprinkler nozzles controllable.

The network consisted of five sensing stations and a weather station. Each of the sensing stations contained a data logger with two soil water reflectometers, a soil temperature sensor, and Bluetooth communication. Using the network information and the irrigation machine positions through differential GPS, the software controlled the sprinkler with application of the appropriate amount of water. Software dedicated to sprinkler control has been variously discussed. A data acquisition system was deployed for monitoring crop

# An Implementation of Adaptive Multipath Routing Algorithm for congestion control

**N.Krishna Chaitanya**

Research Scholar, ECE Department, JNTUCE,  
KAKINADA

**S.Varadarajan**

Professor, ECE Department, S V University College of  
Engineering TIRUPATI

## Abstract

This paper proposes a better adaptive multi path routing technique for routing the data packets effectively from source to destination under congestion at a router. In traditional adaptive multi path routing techniques, if congestion occurred at a router then the route is changed from source to destination. In a single path routing algorithm, all the data packets transmitted through a single path, where the time taken to transmit the packets is more. This drawback is eliminated by using multi path routing technique, where the packets are transmitted through different paths. The proposed method provides a better solution for minimizing the congestion by rerouting the data packets over other paths, which are not utilized by the same in multi-path routing. This method avoids the unnecessary dropping of packets at a congested router and improves the network performance.

## Keywords

Congestion, multi-path routing, Packets, router

## 1. Introduction

Most of the routing techniques in a network are based on a single path. As the number of data packets transferring increases, the data traffic increases in the network, as a result congestion will occur. To avoid this, multi-path routing [5] is preferred. In multi-path routing, the total available data is split and transferred among several paths. Many multi-path routing protocol techniques have been proposed in networks. Some of the multi path routing techniques are Simultaneous Multi Path Communication (SMPC) [1], and Distribution and Congestion Minimized Multipath (DCMM) routing [2]. The existing methods are used to reduce the congestion in multipath routing. In multi-path routing, still there is possibility of occurrence of congestion. This paper proposes a method to avoid the congestion occurring in multipath routing. It reduces the unnecessary retransmissions and delay for data packets, which will affect the performance of the network. In order to avoid congestion, multi path routing along with load balancing is used [3, 4].

The rest of the paper organized as follows. Section 2 provides the overview on the existing multipath routing techniques. In Section 3, we introduce the proposed Adaptive Multipath Routing for Congestion Control (AMR-CC). The Section 4 discusses the flow chart used in

this method. Section 5 presents the simulation results, and section 6 concludes the paper.

## 2. Existing Methods

One of the multipath routing techniques is Simultaneous Multi-Path Communication [3]. There are two types of SMPC's available; they are (i) SMPC-I & (ii) SMPC-P. Here both the techniques are based on bandwidth control. In SPMC-I [1], all paths for communication are treated equally. The bandwidths of each path are controlled independently. In this technique, it is possible to control the bandwidth for each path with no information of any other path.

In SMPC-P [1], the priority will be given to the paths that are used for data transfer. If the total communication bandwidth used for data transfer is greater than the available bandwidth, it uses priority control scheme. In this, the communication bandwidth is controlled by decreasing the bandwidth of one of the paths in ascending order of priority level among the paths having a lower priority.

In these methods, still there exists a problem because of reducing the transmission bandwidth in the network, which will increase the data transmission delay and reduces the network performance.

Another existing method is Distribution and Congestion Minimized Multipath (DCMM) routing. Here, in this method, the routing decisions minimize network congestion, routing decisions address link congestion avoidance topology and maximum flow optimization. Here, number of paths in multi path routing is reduced, and as a result, it is unable to minimize the congestion [5]. Because of the limitations in the available techniques, a new technique has been proposed to minimize the network congestion and to improve network performance.

## 3. Proposed Method

A method was proposed with an algorithm, flow chart and presented by Chaitanya, N. Krishna, S. Varadarajan, and P.

## **Melanoma Early Detection using Dual Classifier**

**N. KRISHNA CHAITANYA<sup>1</sup>, I. PAVANI<sup>2</sup>**

<sup>1</sup>Associate Professor, Dept of ECE, PBR VITS, Kavali, AP, India.

<sup>2</sup>PG Scholar, Dept of ECE- VLSI, PBR VITS, Kavali, AP, India.

**Abstract:** Melanoma spreads through metastasis, and therefore it has been proved to be very fatal. A system to prevent this type of skin cancer is being awaited and is highly in-demand. It is important to highlight that excess exposure to radiations from the sun gradually erode melanin in the skin. Moreover, such radiations penetrate into the skin thereby destroying the melanocyte cells. Melanomas are asymmetrical and have irregular borders, notched edges, and color variations, so analyzing the shape, color, and texture of the skin lesion is important for melanoma early detection and prevention. In this work, the components of a portable real-time noninvasive skin lesion analysis system to assist in the melanoma prevention and early detection are proposed. The first component is a real-time alert to help users to prevent skin burn caused by sunlight; a novel equation to compute the time for skin to burn is thereby introduced. The second component is an automated image analysis including image acquisition, hair detection and exclusion, lesion segmentation, feature extraction, and classification. The framework has been developed in a smart-phone application. The experimental results show that the proposed system is efficient, achieving high classification accuracies.

**Keywords:** Image Segmentation, Skin Cancer, Melanoma.

### **I. INTRODUCTION**

Melanoma is the most frequent type of skin cancer and its incidence has been rapidly increasing over the last few decades. Nevertheless, it is also the most treatable kind of skin cancer, if diagnosed at an early stage. The clinical diagnosis of melanoma is commonly based on the ABCD rule, an analysis of four parameters (asymmetry, border irregularity, color, and dimension), or the 7-points checklist which is a scoring method for a set of different characteristics depending on color, shape, and texture. Melanoma, a type of skin cancer must be diagnosed at an early stage. Early diagnosis makes treatment effective and life of patient can be saved. Dermoscopy has become important technique in early diagnosis of melanoma. In this technique, oil is applied on skin surface where lesion is present and polarized light is made incident on skin. Then image is acquired with digital camera attached to dermatoscope. This process reveals the morphological structures which are present in deeper layer of skin. When image acquisition is done using dermatoscope, some artefacts are introduced in image. The hair which is present on skin can be segmented as lesion because of dark pixels being classified as lesion against lighter pixels which will be categorized as skin. So it is necessary to remove these hair pixels from acquired image. In some of the cases, dermatoscope is provided with ruler markings for measurement of diameter of lesion. So these markings will be there in acquired image. The air bubbles and black frame in image can affect the accuracy of segmentation process and further diagnosis of skin cancer. So these artefacts must be removed from dermoscopic image.

In some of the cases, contrast between skin and lesion can be very poor. It is needed to increase the contrast between skin and lesion. Histogram equalization based technique can be used for contrast enhancement. Histogram equalization gives good results for dermoscopic images. This involves remapping in gray levels to produce uniform distribution in input image. Improved contrast between the lesion and skin improves the accuracy of further diagnosis steps. Dermoscopy is a non-invasive diagnosis technique for the *in vivo* observation of pigmented skin lesions used in dermatology. Dermoscopic images have great potential in the early diagnosis of malignant melanoma, but their interpretation is time consuming and subjective, even for trained dermatologists. Therefore, there is currently a great interest in the development of computer-aided diagnosis systems that can assist the clinical evaluation of dermatologists. The standard approach in automatic dermoscopic image analysis has usually three stages:

- Image segmentation;
- Feature extraction and feature selection
- Lesion classification.

The segmentation stage is one of the most important since it affects the accuracy of the subsequent steps. However, segmentation is difficult because of the great variety of lesion shapes, sizes, and colors along with different skin types and textures. In addition, some lesions have irregular boundaries and in some cases there is a smooth transition between the lesion and the skin. Other difficulties are related to the presence of dark hair covering the lesions and the existence

1/9/2021

CHANNEL SENSING IN COGNITIVE RADIO BY USING MATLAB | Request PDF

Request now · 1 citation · 8 reads · 1 page

Article

CHANNEL SENSING IN COGNITIVE RADIO BY USING MATLAB

July 2018

Authors:



**Bimal Bhattacharai**  
Universitetet i Agder



**Ashok Subedi**  
Jawaharlal Nehru Technological University, Anantapur



**Nosina Krishna Chaitanya**  
PBR Visvodaya Institute of Technology and Science College

[Request full-text](#)

[Download citation](#)

[Copy link](#)



To read the full-text of this research, you can request a copy directly from the authors.

References (8)

Discover the world's research

- 19+ million members
- 135+ million publications
- 700k+ research projects

[Join for free](#)

No full-text available

To read the full-text of this research,  
you can request a copy directly from the authors.

[Request full-text PDF](#)

Citations (0)

References (8)

Ten Years of Research in Spectrum Sensing and Sharing in Cognitive Radio

Article [Full-text available](#)

Dec 2012 · EURASIP J WIREL COMM

Ji Lu · Xiangwei Zhou · Uzoma Onunkwo · Geoffrey Li

[View](#) [Show abstract](#)

# Location-Aware and Safer Cards

<sup>1</sup>N.Krishna Chaitanya, <sup>2</sup>K.Kavitha

<sup>1,2</sup>Dept of ECE, PBR Visvodaya Institute of Technology & Science, Kavali, AP, India

## **Abstract**

In this paper, we report on a new approach for improving security and privacy in certain RFID applications whereby location or location-related information (such as speed) can serve as a legitimate access context. Examples of these applications include access cards, toll cards, credit cards, and other payment tokens. We show that location awareness can be used by both tags and back-end servers for defending against unauthorized reading and relay attacks on RFID systems. On the tag side, we design a location-aware selective unlocking mechanism using which tags can selectively respond to reader interrogations rather than doing so promiscuously. On the server side, we design a location-aware secure transaction verification scheme that allows a bank server to decide whether to approve or deny a payment transaction and detect a specific type of relay attack involving malicious readers. The premise of our work is a current technological advancement that can enable RFID tags with low-cost location (GPS) sensing capabilities. Unlike prior research on this subject, our defenses do not rely on auxiliary devices or require any explicit user involvement.

## **Keywords**

Context Recognition, RFID, Mobile Payment System, Relay Attacks, Location Sensing

## **I. Introduction**

Low cost, small size, and the ability of allowing computerized identification of objects make Radio Frequency IDentification (RFID) systems increasingly ubiquitous in both public and private domains. Prominent RFID applications supply chain management (inventory control), e-passports, credit cards, driver's licenses, vehicle systems (toll collection or car key), access cards (building, parking or public transport), and medical implants. NFC, or Near Field Communication, is yet another upcoming RFID technology that allows devices, such as smart phones, to have both RFID tag and reader functionality. In particular, the use of NFC-equipped mobile devices as payment tokens (such as Google Wallet) is considered to be the next generation payment system and the latest buzz in the financial industry.

A typical RFID system consists of tags, readers, and/or back-end servers. Tags are miniaturized wireless radio devices that store information about their corresponding subject. Such information is usually sensitive and personally identifiable. For example, a US e-passport stores the name, nationality, date of birth, digital photograph, and (optionally) fingerprint of its owner. Readers broadcast queries to tags in their radio transmission ranges for information contained in tags and tags reply with such information. The queried information is then sent to the server (which may coexist with the reader) for further processing and the processing result is used to perform proper actions (such as updating inventory, opening gate, charging toll or approving payment).

Due to the inherent weaknesses of underlying wireless radio communication, RFID systems are plagued with a wide variety of security and privacy threats. A large number of these threats are due to the tag's promiscuous response to any reader requests. This renders sensitive tag information easily subject to unauthorized

reading. Information (might simply be a plain identifier) gleaned from a RFID tag can be used to track the owner of the tag, or be utilized to clone the tag so that an adversary can impersonate the tag's owner.

Promiscuous responses also incite different types of relay attacks. One class of these attacks is referred to as "ghost-and-leech". In this attack, an adversary, called a "leech," relays the information surreptitiously read from a legitimate RFID tag to a colluding entity known as a "ghost." The ghost can then relay the received information to a corresponding legitimate reader and vice versa in the other direction. This way a ghost and leech pair can succeed in impersonating a legitimate RFID tag without actually possessing the device.

A more severe form of relay attacks, usually against payment cards, is called "reader-and-ghost"; it involves a malicious reader and an unsuspecting owner intending to make a transaction. In this attack, the malicious reader, serving the role of a leech and colluding with the ghost, can fool the owner of the card into approving a transaction which she did not intend to make (e.g., paying for a diamond purchase made by the adversary while the owner only intending to pay for food). We note that addressing this problem requires secure transaction verification, i.e., validation that the tag is indeed authorizing the intended payment amount.

The feasibility of executing relay attacks has been demonstrated on many RFID (or related) deployments, including the Chip-and-PIN credit card system, RFID assisted voting system, and keyless entry and start car key system. With the increasingly ubiquitous deployment of RFID applications, there is a pressing need for the development of security primitives and protocols to defeat unauthorized reading and relay attacks. However, providing security and privacy services for RFID systems presents a unique and formidable set of challenges. The inherent difficulty stems partially from the constraints of RFID tags in terms of computation, memory and power, and partially from the unusual usability requirements imposed by RFID applications (originally geared for automation). Consequently, solutions designed for RFID systems need to satisfy the requirements of the underlying RFID applications in terms of not only efficiency and security, but also usability.

In this paper, we report on our work on utilizing location information to defend against unauthorized reading and relay attacks in certain applications. We notice that in quite some applications, under normal circumstances, tags only need to communicate with readers at some specific locations or while undergoing a certain speed. For example, an access card to an office building needs to only respond to reader queries when it is near the entrance of the building; a credit card should only work in authorized retail stores; toll cards usually only communicate with toll readers in certain fixed locations (toll booths) or when the car travels at a certain speed. Hence, location or location-specific information can serve as a good means to establish a legitimate usage context.

# An Implementation of Adaptive Multipath Routing Algorithm for congestion control

N.Krishna Chaitanya, Research Scholar, ECE Department, JNTUCE, KAKINADA

S.Varadarajan, Professor, ECE Department, S V University College of Engineering, TIRUPATI

**Abstract:-** This paper proposes a better adaptive multi path routing technique for routing the data packets effectively from source to destination under congestion at a router. In traditional adaptive multi path routing techniques, if congestion occurred at a router then the route is changed from source to destination. In a single path routing algorithm, all the data packets transmitted through a single path, where the time taken to transmit the packets is more. This drawback is eliminated by using multi path routing technique, where the packets are transmitted through different paths. The proposed method provides a better solution for minimizing the congestion by rerouting the data packets over other paths, which are not utilized by the same in multi-path routing. This method avoids the unnecessary dropping of packets at a congested router and improves the network performance.

**Keywords:** Congestion, multi-path routing, Packets, router

## I. INTRODUCTION

Most of the routing techniques in a network are based on a single path. As the number of data packets transferring increases, the data traffic increases in the network, as a result congestion will occur. To avoid this, multi-path routing [5] is preferred. In multi-path routing, the total available data is split and transferred among several paths.

Many multi-path routing protocol techniques have been proposed in networks. Some of the multi path routing techniques are Simultaneous Multi Path Communication (SMPC) [1], and Distribution and Congestion Minimized Multipath (DCMM) routing [2]. The existing methods are used to reduce the congestion in multipath routing.

In multi-path routing, still there is every possibility of occurrence of congestion. This paper proposes a method to avoid the congestion occurring in multipath routing. It reduces the unnecessary retransmissions and delay for data

packets, which will effect on the performance of the network. In order to avoid congestion, multi path routing along with load balancing is used [3, 4].

The rest of the paper organized as follows. Section 2 provides the overview on the existing multipath routing techniques. In Section 3; we introduce the proposed Adaptive Multipath Routing for Congestion Control (AMR-CC). The Section 4 discusses the flow chart used in this method. Section 5 presents the simulation results, and section 6 concludes the paper.

## II. EXISTING METHODS

One of the multipath routing techniques is Simultaneous Multi-Path Communication [3]. There are two types of SMPC's available; they are (i) SMPC-I & (ii) SMPC-P. Here both the techniques are based on bandwidth control.

In SPMC-I [1], all paths for communication are treated equally. The bandwidths of each path are controlled independently. In this technique, it is possible to control the bandwidth for each path with no information of any other path.

In SMPC-P [1], the priority will be given to the paths that are used for data transfer. If the total communication bandwidth used for data transfer is greater than the available bandwidth, it uses priority control scheme. In this, the communication bandwidth is controlled by decreasing the bandwidth of one of the paths in ascending order of priority level among the paths having a lower priority.

In these methods, still there exists a problem because of reducing the transmission bandwidth in the network, which will increase the data transmission delay and reduces the network performance.



**PARVATHAREDDY BABUL REDDY**

**VISVODAYA INSTITUTE OF TECHNOLOGY & SCIENCE**

(Affiliated to J.N.T.U.A, Approved by AICTE and Accredited by NAAC with 'A' Grade)

KAVALI – 524201, S.P.S.R Nellore Dist., A.P. India. Ph: 08626-243930



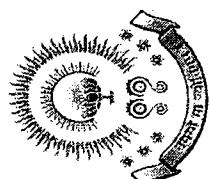
**DEPARTMENT OF MECHANICAL ENGINEERING**

**INTERNATIONAL JOURNAL – SUMMARY**

SCHEMES	NO. OF INTERNATIONAL JOURNALS				
	2019-2020	2018-2019	2017-2018	2016-2017	2015-2016
INTERNATIONAL JOURNAL	1	16	5	15	21

  
**HEAD OF THE DEPARTMENT**

Head of Department  
MECHANICAL ENGINEERING  
PBR Visvodaya Institute of Technology & Science  
KAVALI - 524 201, Nellore District. A.P



## PARVATHAREDDY BABUL REDDY

## VISVODAYA INSTITUTE OF TECHNOLOGY & SCIENCE

(Affiliated to J.N.T.U.A, Approved by AICTE and Accredited by NAAC with 'A' Grade)

KAVALI - 524201, S.P.S.R Nellore Dist., A.P. India. Ph: 08626-243930



### DEPARTMENT OF MECHANICAL ENGINEERING

ACADEMIC YEAR : 2019-20

SL.NO	TITLE OF PAPER	NAME OF FACULTY	JOURNAL	YEAR	ISSN NO	LINK
1	Design And Coupled Field Analysis Of Exhaust Manifold By Using Different Materials	A.Madhava Rao	International Journal of Research	2019-20	p-ISSN: 2348-6848e-ISSN: 2348-795X	<a href="https://journals.pen2print.org/index.php/ijr/article/download/19712/19350">https://journals.pen2print.org/index.php/ijr/article/download/19712/19350</a>

  
Head of Department  
MECHANICAL ENGINEERING  
PBR Visvodaya Institute of Technology & Science  
KAVALI - 524 201, Nellore District, A.P.

# Design And Coupled Field Analysis Of Exhaust Manifold By Using Different Materials

B.V. Harish Kumar<sup>1</sup>, A.Madhava Rao<sup>2</sup>

<sup>1</sup>P.G. Scholar, <sup>2</sup>Guide, Asst. Professor

<sup>1,2</sup> Branch: M.TECH, Machine Design (MD)

<sup>1,2</sup> PBR Visvodaya institute of technology & science, Kavali

Mail Id : <sup>1</sup>[bvharishkumar@yahoo.com](mailto:bvharishkumar@yahoo.com), <sup>2</sup>[maddy.2009avula@gmail.com](mailto:maddy.2009avula@gmail.com)

## ABSTRACT:

Exhaust manifold receives the exhaust gases comes out from chamber and passes to environment. They usually assembled with cylinder. The exhaust manifold is mounted on the cylinder head of the engine.

Back pressure can be produced at two places, i.e., when the exhaust valve opens and cam overlap taking place. Pressure measurements at the exhaust valve during the start of the exhaust stroke at bottom dead centre (BDC) to cam overlap at the end of the exhaust stroke/beginning of the intake stroke at top dead centre (TDC). The exhaust gases emitted from the cylinder come out at temperatures of nearly  $800^{\circ}\text{C}$  and with pressures ranging from 100 to 500 kPa. The exhaust manifold is subjected to high temperatures and pressures which will lead to thermo mechanical failure.

This project aims in redesigning an exhaust manifold by determining Thermal stresses and deflections exhibited under various operating conditions with different materials and temperatures. The objective is to ensure the suitability of the design for a particular material from the view point of reliability and serviceability. High end cad cam software such as Unigraphics and Ansys is used for modeling and analysis. The 3d Model of exhaust manifold is subjected to thermal and structural loads and results are tabulated according to the procedure for the Exhaust manifold.

CAD TOOL: UNIGRAPHICS

CAE TOOL: ANSYS

**Keywords:-** Exhaust manifold, Cast iron, Metal matrix, Turbulence effect, Thermal stress

## INTRODUCTION

### 1.1 EXHAUST MANIFOLD

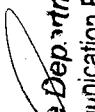
Exhaust manifold receives the exhaust gases comes out from chamber and passes to environment. The usually assembled with cylinder. Cast iron is material used for exhaust manifolds. Factors to be considered during the design and development of exhaust manifold

**A. Runner length** This is arguably one of the most important factors. First would be to make sure that the runners are as equal length as possible. The idea being that the exhaust pulses will be spaced out evenly and arriving at the turbine wheel on the turbo at their own time in the firing order.

**B. Runner volume** Runner volume needs to be considered when building a turbo manifold. While a larger runner diameter does facilitate lower exhaust backpressure for better flow on the top-end, it does cause a lower exhaust velocity. A lower exhaust velocity will cause longer spool times, and less transient response out of the turbo.

**C. Collectors** A collector's job is to tie all of the cylinder's pipes together in one common place and send them into a single exit pipe. A collector is generally a conglomeration of pipes all merged together, allowing for a smooth transition from the primaries or secondaries into the rest of the exhaust.

S. No	Title of paper	Name of the author/s	Department of the teacher	Name of journal	Year of publication	ISSN number	Link to the recognition in UGC enlistment of the
8	An implementation of Adaptive Multipath Routing Algorithm for Congestion Control	N.Krishna Chaitanya	ECE	19th International Conference on Circuits, Systems, Communications and Computers (CSSCC 2015), Zakynthos island, Greece	July, 2015	ISBN: 978-1-61804-318-4	<a href="http://ijsetr.com/uploads/164235IJSETR6806-1305.pdf">http://ijsetr.com/uploads/164235IJSETR6806-1305.pdf</a>
9	Wireless communication and gprs based irrigation system	N.Krishna Chaitanya	ECE	International Journal of Scientific Engineering and Technology Research (IJSETR).	Sept, 2015	ISSN: 2319-8885	
10	Melanoma early detection using dual classifier	N.Krishna Chaitanya	ECE	International Journal of Scientific Engineering and Technology Research (IJSETR)	Sept, 2015	ISSN :2319-8885	<a href="https://www.researchgate.net/publication/326316599_CHANNEL_SENSING_IN_COGL">https://www.researchgate.net/publication/326316599_CHANNEL_SENSING_IN_COGL</a>
11	Channel sensing in cognitive radio by using matlab	N.Krishna Chaitanya	ECE	The IUP Journal of Telecommunication	Nov, 2015	ISSN: 0975-5551	<a href="https://www.inapse.org/library/2015/zakynthos/bypaper/COMMUN/COMMUN-48.pdf">http://www.inapse.org/library/2015/zakynthos/bypaper/COMMUN/COMMUN-48.pdf</a>
12	Location-aware and safer cards	N.Krishna Chaitanya	ECE	International Journal of Electronics & Communication Technology (IJECT)	Dec, 2015	ISSN: 2230-9543	
13	An implementation of Adaptive Multipath Routing Algorithm for Congestion Control	N.Krishna Chaitanya	ECE	International Journal of Computer Science and Network Security (IJCSNS)	Feb,2016	ISSN 1738-7906	<a href="https://reader.elsevier.com/reader/sd/pii/S2213020916300581?token=7F5AF76E299839DFC9BA644296563E7B26624C1AEFFC5D51028B8E">https://reader.elsevier.com/reader/sd/pii/S2213020916300581?token=7F5AF76E299839DFC9BA644296563E7B26624C1AEFFC5D51028B8E</a>
14	Load Distribution using Multipath-Routing In Data Networks: A Comparative Study	N.Krishna Chaitanya	ECE	International Conference on recent trends in Engineering and Material Sciences (ICEMS-2016), Jaipur National University, Jaipur, India.	Mar,2016	ISSN : 2213-0209	<a href="http://ijaree.org/wp-content/uploads/2015/09/IJAREE-VOL-4-ISSUE-8-2315-2321.pdf">http://ijaree.org/wp-content/uploads/2015/09/IJAREE-VOL-4-ISSUE-8-2315-2321.pdf</a>
15	A Speed and Accurate Binary Multiplier for Floating Point values	T. Suneel Kumar	ECE	International Journal of Advance research in Electrical, Electronics and Communication Engineering	Sept, 2015	ISSN:2278 – 909X	
16	Implementation of Double Precision Floating Point Multiplier	C.V.Kavya Suvarchala	ECE	International Journal Of VLSI Design and Communication Systems	Dec, 2015	ISSN 2322-0929	<a href="http://www.ijvdcn.org/uploads/236514IJVDCS8259-268.pdf">http://www.ijvdcn.org/uploads/236514IJVDCS8259-268.pdf</a>

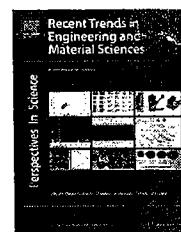
  
**Head of the Department**  
 Electronics & Communication Engineering  
**Dr. B. Venkateswara Rao**  
 Head of the Department of  
 Electronics & Communication Engineering  
 KAVALI - 524 201



Available online at [www.sciencedirect.com](http://www.sciencedirect.com)

ScienceDirect

journal homepage: [www.elsevier.com/pisc](http://www.elsevier.com/pisc)



# Load distribution using multipath-routing in wired packet networks: A comparative study<sup>☆</sup>



N. Krishna Chaitanya<sup>a,\*</sup>, S. Varadarajan<sup>b</sup>

<sup>a</sup> Research Scholar, ECE Department, JNTUCE, Kakinada, India

<sup>b</sup> Professor, ECE Department, S V University College of Engineering, Tirupati, India

Received 2 February 2016; accepted 11 April 2016

Available online 26 April 2016

## KEYWORDS

Multipath-routing;  
Load balancing;  
Congestion

**Summary** This paper aimed towards the analysis of various multipath routing techniques with and without load balancing as a comparative study. Most of the routing techniques targeted to find best path from source to destination. The basic routing techniques are based on single path; there is only one path from sending end to receiving end. There after multipath routing techniques has been proposed to send the data in multiple paths and eliminates the drawbacks in single path routing. This study gives better idea about multipath routing techniques along with load balance for avoiding congestion in wired packet networks.

© 2016 Published by Elsevier GmbH. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

## Introduction

Routing is the process of sending data from source to destination by making use of the best path through the network. Data packet can be routed either by using single and multipath routing techniques. In a single path routing, data is sent over a single path and in multipath routing, the data is sent over a number of multiple potential paths available at that instant (Domzal et al., 2015; Xin et al., 2009). As

the traffic on internet increases, congestion will occur in the network and its performance decreases (Tanaka, 2011). Most widely used routing to avoid congestion is multi path routing technique (Xin et al., 2009). Major advantage of multi-path routing: any failure in any path, data will be routed in alternate paths and hence throughput will increase dramatically (Domzal et al., 2015). A network is more efficient when a router is capable of dividing the traffic over multiple paths. Packet distribution and delivery is ensured by using multipath-routing technique (Li et al., 2011).

Load balancing is another technique used to eliminate congestion by distributing the data packets through the network based on available network resources. In load balance, it decides how much load should be sent over each path (Key et al., 2007). In which, number of paths is decided by multipath routing algorithm.

<sup>☆</sup> This article belongs to the special issue on Engineering and Material Sciences.

\* Corresponding author. Tel.: +91 8019255212.

E-mail address: nosinakc@gmail.com (N.K. Chaitanya).

# A Speed and Accurate binary multiplier for floating point values

Medireddy Bala Subba Reddy<sup>1</sup>

T.Suneel Kumar<sup>2</sup>

## Abstract:

This paper exhibits a speed and accurate binary multiplier for floating point values in view of Dadda Algorithm. Multiplication of mantissa is carried out utilizing Dadda multiplier supplanting Carry Save Multiplier to enhance the speed of operation. The configuration attains to high speed with maximum recurrence of 526 MHz contrasted with existing floating point multipliers. The floating point multiplier is developed to handle the underflow and overflow occurrences. Adjusting is not brought to give more accuracy for mantissa multiplication. The multiplier is implemented utilizing Verilog HDL furthermore it is focused for Xilinx Virtex-5 FPGA. The multiplier is contrasted and Xilinx floating point multiplier core.

## I. Introduction:

The vast majority of the DSP applications need multiplication of numbers of floating point type. The

conceivable approaches to stand for real numbers as binary arrangement floating point numbers are; Binary interchange and Decimal interchange format according to the IEEE 754 standard [1]. Single precision normalized binary interchange arrangement is actualized in this outline. Such arrangement is indicated in Figure 1; beginning from MSB it has an one bit sign (S), an eight bit exponent (E), and a twenty three bit fraction called Mantissa (M). Including an additional bit to the fraction to structure and is characterized as significand. If exponent is more noteworthy than 0 and littler than 255, and there is 1 in the MSB of the significand then the number is said to be a normalized number; for this present case the real number is represented by equation (1).

$$Z = (-1)^S \times 2^{(E-\text{Bias})} \times (1.M) \quad (1)$$

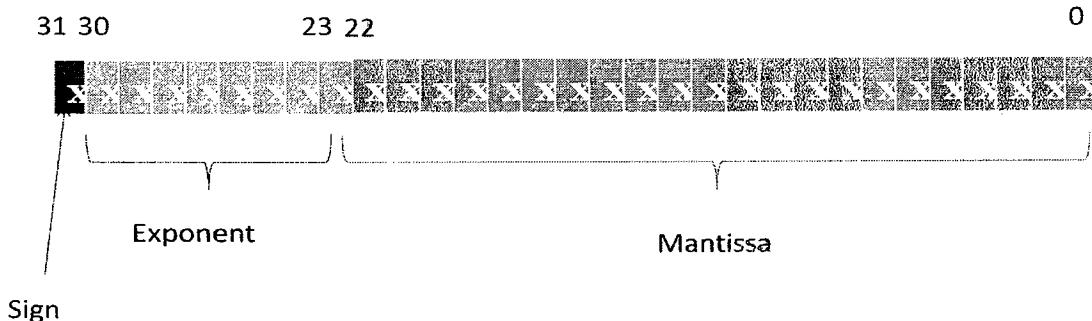


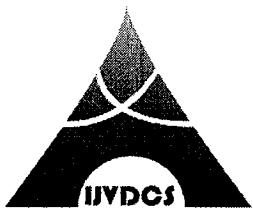
Fig 1: Representation of IEEE single precision floating point format

Step 1: Addition of two number's exponents and from this result subtracting the extra bias.

## II. Floating Point Multiplier Algorithm

Generally there are four stages to carry out the floating point multiplication of two numbers:

Step 2: Multiplication of the significands of the two numbers by the Dadds algorithm.



## Implementation of Double Precision Floating Point Multiplier

C. V. KAVYA SUVARCHALA<sup>1</sup>, B. SUKHADEV<sup>2</sup>

<sup>1</sup>Assistant Professor, Dept of ECE, PBR Visvadaya Institute of Technology & Science, Kavali, A.P, India.

<sup>2</sup>PG Scholar, Dept of ECE, PBR Visvadaya Institute of Technology & Science, Kavali, AP, India.

**Abstract:** Floating Point (FP) multiplication is broadly utilized in large set of scientific and signal processing calculation. Multiplication is one of the common arithmetic operations in these computations. A high speed floating point double precision multiplier is implemented on a Virtex-6 FPGA. Besides, the proposed design is compliant with IEEE-754 format and handles over flow, under flow, rounding and various exception conditions. The design achieved the better operating frequency and area when compared to single precision.

**Keywords:** Double Precision, Floating Point, Multiplier, FPGA, IEEE-754.

### I. INTRODUCTION

The real numbers represented in binary format are known as floating point numbers. Based on TEEE-754 standard, floating point formats are classified into binary and decimal interchange formats. Floating point multipliers are very important in DSP applications. This paper focuses on double precision normalized binary interchange format. Figure 1 shows the IEEE- 754 double precision binary format representation. Sign (S) is represented with one bit, exponent (E) and fraction (M or Mantissa) are represented with eleven and fifty two bits respectively. For a number is said to be a normalized number, it must consist of 'one' in the MSB of the significand and exponent is greater than zero and smaller than 1023. The real number is represented by equations (1) & (2).

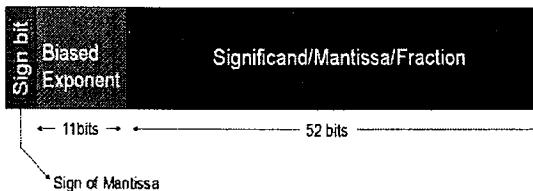


Fig1. IEEE-754 double precision floating point format.

$$Z = (-1^S) * 2^{(E-Bias)} * (1.M)$$

$$\text{Value} = (-1^{\text{Sign bit}}) * 2^{(\text{Exponent}-1023)} * (1.\text{Mantissa})$$

Floating point implementation on FPGAs has been the interest of many researchers. In [1], an IEEE-754 single precision pipelined floating point multiplier is implemented on multiple FPGAs (4 Actel A1280). Nabeel Shirazi, Walters, and Peter Athanas implemented custom 16/18 bit three stage pipelined floating point multiplier, that doesn't support rounding modes [2]. L.Louca, T.A.Cook, W.H. Johnson [3] implemented a single precision floating point

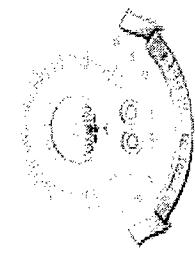
multiplier by using a digit-serial multiplier and Altera FLEX 8000. The design achieved 2.3 MFlops and doesn't support rounding modes. In [4], a parameterizable floating point multiplier is implemented using five stages pipeline, Handel-C software and Xilinx XCV1000 FPGA. The design achieved the operating frequency of 28MFlops. The floating point unit [5] is implemented using the primitives of Xilinx Virtex II FPGA. The design achieved the operating frequency of 100 MHz with a latency of 4 clock cycles. Mohamed Al-Ashrafy, Ashraf Salem, and Wagdy Anis [6] implemented an efficient IEEE-754 single precision floating point multiplier and targeted for Xilinx Yirtex-5 FPGA. The multiplier handles the overflow and underflow cases but rounding is not implemented. The design achieves 301 MFLOPs with latency of three clock cycles. The multiplier was verified against Xilinx floating point multiplier core. The double precision floating point multiplier presented here is based on IEEE-754 binary floating standard. We have designed a high speed double precision floating point multiplier using Verilog language and ported on Xilinx Vertex-6 FPGA. It operates at a very high frequency of 414.714 MFlops and occupies 648 slices. It handles the overflow, underflow cases and rounding mode.

### II. FLOATING POINT MULTIPLICATION ALGORITHM

Multiplying two numbers in floating point format is done by

1. Adding the exponent of the two numbers then
1. subtracting the bias from their result.
2. Multiplying the significand of the two numbers
3. Calculating the sign by XORing the sign of the two numbers.

In order to represent the multiplication result as a normalized number there should be 1 in the MSB of the result (leading one).



**PARVATHAREDDY BABUL REDDY**  
**VISVODAYA INSTITUTE OF TECHNOLOGY & SCIENCE**  
(Affiliated to J.N.T.U.A. Approved by AICTE and Accredited by NAAC with 'A' Grade)  
KAVALLI – 524201, S.P.S.R Nellore Dist., A.P. India. Ph: 08626-243930

### DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

*Academic Year: 2016-17*

List of Publications					Link to the recognition in UGC enlistment of the journal	
S.No	Title of paper	Name of the author/s	Department of the teacher	Name of journal	Year of publication	ISSN number
1	Texture Image Segmentation Based on threshold hold Techniques	Dr. D Prathyusha Reddi	ECE	International Journal of Computer Engineering In Research Trends	March-2017	ISSN (O): 2349-7084
2	A New Approach For The Design Of Low Power Dynamic Differential Logic For Secure Integrated Circuits	M.Pavitra	ECE	International Journal of Innovative Research and Advanced Studies (IJIRAS)	Dec., 2016	ISSN: 2394-4404 <a href="https://pdfs.semanticscholar.org/bae6/558fb3f4f9e393c254b3fe758cb6edbfcc29f.pdf?ga=2.17474466.158756099.1592841538-1665813400.1587522006">https://pdfs.semanticscholar.org/bae6/558fb3f4f9e393c254b3fe758cb6edbfcc29f.pdf?ga=2.17474466.158756099.1592841538-1665813400.1587522006</a>
3	Personal Health Monitoring Using Andriod Based Mobile Device	R.Prathp singh	ECE	International Journal Of Professional Engineering Studies	Sept., 2016	
4	Reduction of switching Activity in NOC By using Data Encoding Schemes	R.Prathp singh	ECE	International Journal Of Engineering and computer Sciences Volume	Sept., 2016	ISSN : 2319-7242 <a href="http://www.ijecs.in/index.php/ijecs/article/view/3276/3035">http://www.ijecs.in/index.php/ijecs/article/view/3276/3035</a>
5	Objective quality assessment and optimization for high Dynamic range image tone mapping	V.Phani Bhushan	ECE	Anveshana's International Journal Of Research In Engineering And Applied Sciences	Dec., 2016	ISSN-2455-6300

# Texture Image Segmentation Based on threshold Techniques

<sup>1</sup>Dodla. Likhith Reddy, <sup>2</sup>Dr. D Prathyusha Reddi

<sup>2</sup>Professor, Dept.of ECE, PBR VITS, KAVALI.

Email: [likhithdodla@gmail.com](mailto:likhithdodla@gmail.com) , [prathyu65@yahoo.co.in](mailto:prathyu65@yahoo.co.in)

---

**Abstract:** Image segmentation is the process of partitioning a digital image into multiple segments. The goal of segmentation is to simplify change the representation of an image into something that is more meaningful and easier to analyze. Image segmentation is used to give the values of objects and boundaries of a selected image like lines, curves. The image segmentation plays a critical role in a variety of pattern recognition applications such as robot vision, cartography, criminal investigation, remote sensing, object identification and recognition, military surveillance, quality assurance in industries, facial recognition and medical imaging, etc. The main aim of this paper is to propose methods are improving image segmentation and give the clear object about the image by using different techniques. This article presents a brief outline of some of the most commonly used segmentation techniques like Thresholding, Region based and Edge detection methods. The proposed methods implemented in MATLAB.

**Index Terms---** Segmentation, Edge Detection, Region Based, threshold-based segmentation techniques.

---

## 1. Introduction

Image segmentation divides an image in the form of groups of different regions depending on various attributes, such that every region is uniformly based on specific properties. Segmentation results can be used for further image analysis and processing like object classification and identification. Segmentation methods can classify into supervised or unsupervised. Unsupervised segmentation is one of the critical and demanding issues of the segmentation because no prior information about the image textures is available. That is why it has only limited success so far. Early methods of unsupervised segmentation are developed based on various methods like pyramid node linking [26], split-and-merge methods [40], a quadtree method [28] and particular feature smoothing with clustering [43]. Later the segmentation methods based on feature smoothing [32], local linear transforms, Markov random field models [4, 11], autoregressive models [38], fractal dimension [10], multichannel filtering

[30], hidden Markov models [42], Markov random fields for color textures [22] are proposed. These methods achieved good results for a minute set of fine-grained texture like mosaics; however, they need to have prior knowledge of the image contents like some textures and regions. Moreover, some segmentation methods typically performed poor results for natural images containing non-uniform textures. The segmentation methodologies, including Edge based segmentation, threshold based image segmentation, and Region-based image segmentation [3]. To test the derived methods the present paper plans to work on four large databases, namely Indian facial expressions, WANG [32], official images from Google [33] and natural textures of Brodtaz album [34].

## 2. Image Segmentation Techniques

The segmentation methods are broadly divided into three categories:

# A New Approach For The Design Of Low Power Dynamic Differential Logic For Secure Integrated Circuits

M. Pavitra

Associate Professor, ECE Dept., PBR VITS,  
Kavali, Nellore (Dt.), AP, India

SK.Afrin

PG Scholar, DSCE, ECE Dept., PBR VITS,  
Kavali, Nellore (Dt.), AP, India

**Abstract:** Production of cost effective secure integrated chips, such as smart cards, requires hardware designers to consider tradeoffs in size, security, and power consumption. To design successful security-centric designs, the low-level hardware must contain built-in protection mechanisms to supplement cryptographic algorithms, such as advanced encryption standard and triple data encryption standard by preventing side-channel attacks, such as differential power analysis (DPA). Dynamic logic obfuscates the output waveforms and the circuit operation, reducing the effectiveness of the DPA attack. For stronger mitigation of DPA attacks, we propose the implementation of adiabatic dynamic differential logic (ADDL) for applications in secure integrated circuit (IC) design. Such an approach is effective in reducing power consumption, demonstrated using HSPICE simulations with 22-nm predictive technology. Then, a high-performance ADDL is presented for an implementation in high-frequency secure ICs. This method improves the differential power over previous dynamic and differential logic methods by up to 76.41%.

**Index Terms:** Adiabatic logic, Differential Power Analysis (DPA) attacks, Forward body biasing, Reversible logic.

## I. INTRODUCTION

SMART cards are small integrated circuits (ICs) embedded onto plastic or tokens, and are used for authentication, identification, and personal data storage. They are used by the military, in automatic teller machines, mobile phone subscriber identity module cards, by schools for tracking class attendance, and storing certificates for use in secure web browsing. They are also used internationally as alternatives to credit and debits cards by Euro pay, MasterCard, and Visa. They are application specific, so their size and software overhead may be minimized. In addition, smart cards use tamper-resistant secure file cryptosystems. They are more difficult to forge than Tokens, Money, and Government issued identification cards [1].

They can be programmed to deter theft by preventing immediate reuse, making them more effective than cards with magnetic strips. Due to their emphasis on security at both the software and hardware levels, smart-card technology is emerging as the platform of choice in key vertical markets [10]. Smart-card technology is moving toward multiple

applications, higher interoperability, and multiple interfaces, such as TCP/IP, near-field communicators, and contact less chips.

Due to their recent proliferation, smart cards are targets of attacks motivated by identity theft, fraud, and fare evasion. Despite their secure software design, smart cards may still be susceptible to side-channel attacks, which are based on correlations of leaked secondary information and the IC output signals. In smart cards, these include electromagnetic emanations (EM leakage) [2], measuring the amount of time required to perform private-key operations [3], and analysis of noisy power consumption.

One of the most effective attacks is a differential power analysis (DPA) attack [5], where the attacker analyzes the power consumption in the IC and compares it to the ICs output signals. The leaked side-channel information is due to the presence of entropy gain in the system. These attacks are effective, since most modern computing technology is CMOS based, and the power consumption tendencies of these devices are well studied. Reducing the power consumption of the circuit makes a DPA attack more difficult.



## PERSONAL HEALTH MONITORING USING ANDROID BASED MOBILE DEVICES

M VENKATA NAGA NITHESH<sup>1</sup> R. PRATHAP SINGH<sup>2</sup>

<sup>1</sup> M Venkata Naga Nithesh, Dept of ECE, PBR Visvodaya Institute Of Technology & Science,Kavali,KavaliMandal,SPSR Nellore Dist, A.P., India

<sup>2</sup> Guide Details,R. Prathap Singh,M.Tech, Associate professor,PBR Visvodaya Institute Of Technology & Science,Kavali,KavaliMandal,SPSR Nellore Dist, A.P., India

**Abstract:** We have developed an Android based mobile data acquisition (DAQ) solution, which collects personalized health information of the end-user, store analyze and visualize it on the smart device and optionally sends it towards to the datacenter for further processing. The smart mobile device is capable to collect information from a large set of various wireless (Bluetooth, and WiFi, cloud, gprs) and wired (USB) sensors. Embedded sensors of the mobile device provide additional useful status information (such as: user location, magnetic or noise level, acceleration, temperature, etc.). The user interface of our software solution is suitable for different skilled users, highly configurable and provides diary functionality to store information (about sleep problems, can act as a diet log, or even can be used as a pain diary). The software enables correlation analysis between the various sensor data sets. The developed system is tested successfully within our Living Lab facility. Sensor data acquisition on the personal mobile device enables both endusers and care givers to provide better and more effective health monitoring and facilitate prevention. The paper describes the internal architecture of the software solution and its main functionalities.

**Keywords:** Microcontroller, ECG sensor, cloud, PC, B.P., sensor.

### I. Introduction

The aging population of industrialized countries grows and this increases also among other things the health care costs. Transparently embedded remote health care can become a new cost effective paradigm, which can solve most of the problems primarily centralized Health Care system's have. Currently, there is a large number of enabling technologies to measure the patient's physiological signals remotely. With handheld and PC devices used as data acquisition (DAQ) systems we are able to collect vital information about the (elderly and demented) patients remotely. Due to the different - in most cases proprietary and incompatible- sensor technologies and solutions, it is a hard task to create generic, user friendly DAQ systems.

There are already remote patient monitoring solutions available such as the Android based MyFitnessCompanion, which is able to support the following therapy fields: Fitness, Diabetes, Asthma, Obesity, Hypertension, CHD, or the iCare[which provides medical guidance, emergency alarm functionality and collects personal health information. Other example is the Microsoft HealthVault which supports care of elderly persons (e.g.: neurodegenerative diseases, stroke etc.), additionally it provides online web interface to manage (process and share) health information.

# Reduction Of Switching Activity In Noc By Using Data Encoding Schemes

**Y.Supraba, R.S.Pratap Singh**

P .b .r visvodaya institute of technology and science

Kavali, s.p.sr.nellore, india

[Ysupraba4@gmail.com](mailto:Ysupraba4@gmail.com)

P .b .r visvodaya institute of technology and science

Kavali, s.p.sr.nellore, india

[rpsvits@rediffmail.com](mailto:rpsvits@rediffmail.com)

**Abstract:** As technology shrinks, the power dissipated by the links of a network-on-chip (NOC) starts to compete with the power dissipated by the other elements of the communication subsystem, namely, the routers and the network interfaces (NIs). In this paper we present a reduction of switching activity in network on chip (NOC) by using data encoding schemes. In proposed schemes there is no need to change link architecture and it will reduce transitions (i.e. nothing but switching activity contains both switching transitions and coupling transitions).due to these transitions lot of power consumption is presented at the network on chip and routers so that by using data encoding schemes we can save consumption of energy and dissipation of power without any degradation of performance .

**Keywords:** Coupling switching activity, data encoding, low power, network-on-chip (NoC), power analysis.

## 1. INTRODUCTION:

Global interconnect length does not scale with smaller transistors and local wires. Chip size remains relatively constant because the chip function continues to increase and RC delay increases exponentially. At 32/28 nm, for instance, the RC delay in a 1-mm global wire at the minimum pitch is 25× higher than the intrinsic delay of a two-input NAND fan out of 5 [1]. If the raw computation horsepower seems to be unlimited, thanks to the ability of instancing more and more cores in a single silicon die, scalability issues, due to the need of making efficient and reliable communication between the increasing number of cores, become the real problem [3]. The network on- chip (NOC) design paradigm [4] is recognized as the most viable way to tackle with scalability and variability issues that characterize the ultra deep sub micron meter era. Nowadays, the on-chip communication issues are as relevant as, and in some cases more relevant than, the computation related issues [4]. In fact, the communication subsystem increasingly impacts the traditional design objectives, including cost (i.e., silicon area), performance, power dissipation, energy consumption, reliability, etc. As technology shrinks, an ever more significant fraction of the total power budget of a complex many-core system-on-chip (SOC) is due to the communication subsystem.

In this paper, we focus on techniques aimed at reducing the power dissipated by the network links. In fact, the power dissipated by the network links is as relevant as that dissipated by routers and network interfaces (NIs) and their contribution is expected to increase as technology scales [5]. In particular, we present a set of data encoding schemes operating at flit level and on an end-to-end basis, which allows us to minimize both the switching activity and

the coupling switching activity on links of the routing paths traversed by the packets.

The proposed encoding schemes, which are transparent with respect to the router implementation, are presented and discussed at both the algorithmic level and the architectural level, and assessed by means of simulation on synthetic and real traffic scenarios. The analysis takes into account several aspects and metrics of the design, including silicon area, power dissipation, and energy consumption. The results show that by using the proposed encoding schemes power and energy can be saved without any significant degradation in performance and with area overhead in the NI.

## II. OVERVIEW OF THE PROPOSAL

The basic idea of the proposed approach is encoding the flits before they are injected into the network with the goal of minimizing the self-switching activity and the coupling switching activity in the links traversed by the flits. In fact self-switching activity and coupling switching activity are responsible for link power dissipation. In this paper, we refer to the end-to-end scheme. This end-to-end encoding technique takes advantage of the pipeline nature of the wormhole switching technique [4].Note that since the same sequence of flits passes through all the links of the routing path, the encoding decision taken at the NI may provide the same power saving for all the links. For the proposed scheme, an encoder and a decoder block are added to the NI. Except for the header flit, the encoder encodes the outgoing flits of the packet such that the power dissipated by the inter-router point-to-point link is minimized.

## III. PROPOSED ENCODING SCHEMES



## OBJECTIVE QUALITY ASSESSMENT AND OPTIMIZATION FOR HIGH DYNAMIC RANGE IMAGE TONE MAPPING

V.PHANI BHUSHAN,

Associate Professor, ECE Dept., PBR  
VITS, Kavali, Nellore (Dt.), AP, INDIA

B.SRAVANI,

PG Scholar, DSCE, ECE Dept., PBR VITS,  
Kavali, Nellore (Dt.), AP, INDIA

### ABSTRACT

Tone mapping operators aim to compress high dynamic range (HDR) images to low dynamic range ones so as to visualize HDR images on standard displays. Most existing works were demonstrated on specific examples without being thoroughly tested on well-established and subject-validated image quality assessment models. A recent tone mapped image quality index (TMQI) made the first attempt on objective quality assessment of tone mapped images. TMQI consists of two fundamental building blocks: structural fidelity and statistical naturalness. In this thesis, we propose an enhanced tone mapped image quality index (eTMQI) by 1) constructing an improved nonlinear mapping function to better account for the local contrast visibility of HDR images and 2) developing an image dependent statistical naturalness model to quantify the unnaturalness of tone mapped images based on a subjective study. The advantages of this algorithm are twofold: 1) eTMQI and TMQI can be compared in a more straightforward way; 2) better quality tone mapped images can be automatically generated by using eTMQI as the optimization goal. Numerical and subjective experiments demonstrate that eTMQI is a superior objective quality assessment metric for tone mapped images and consistently outperforms.

**Index Terms—** High dynamic range image, image quality assessment, tone mapping operator, perceptual image processing, structural similarity, statistical naturalness.

### I.INTRODUCTION

The luminance of a natural scene often has a high dynamic range(HDR),varying

between  $10^{-3}$  to  $10^5 \text{cd/m}^2$ . However, a normal digital display only has a low dynamic range (LDR)

about  $10^2 \text{cd/m}^2$ . Tone mapping operators fill in the gap between HDR imaging and visualizing HDR images on standard displays by compressing the dynamic range of HDR images. TMOs provide a useful surrogate for HDR display technology, which is currently still expensive. Regardless of how fast HDR display technology penetrates the market, there will be a strong need to prepare HDR imagery for display on LDR devices. In addition, compressing the dynamic range of an HDR image while preserving its structural detail and natural appearance is by itself an interesting and challenging problem for human and computer vision study.

Most of them were demonstrated on specific examples without being thoroughly evaluated using well-designed and subject-validated image quality assessment (IQA) models. With multiple TMOs at hand, a natural question is: which TMO produces the best quality tone mapped LDR image? This question could possibly be answered by subjective evaluation which is expensive, time consuming, and

# Smart Traffic Control System for Prevention and Control of Blockade, Emergency Vehicle Clearance and Stolen Vehicle Identification

**YASWANTH SAI JALADANKI**

M.Tech Student, Dept of ECE

PBR Visvodaya Institute of Technology & Science  
Kavali, Nellore(Dist.), A.P, India

**A SUMAN KUMAR REDDY**

Associate Professor, Dept of ECE

PBR Visvodaya Institute of Technology & Science  
Kavali, Nellore(Dist.), A.P, India

**Abstract:** This paper presents a smart traffic control system to avoid traffic congestion and to allow the emergency vehicles to pass with high priority. The main aim of this project is to implement the smart traffic control system to prevent and control of blockade, emergency vehicle detection and identification of stolen vehicle. An RFID tag is implanted on every vehicle such that it is impossible to remove or destroy the tag. These RFID tags are scanned by using the RFID scanner, NSK EDK-125-TTL and ARM7 LPC2148 microcontroller. The number of vehicles that cross the particular predefined path in certain duration will be specified and hence congestion is prevented or controlled by determining the necessary green light duration. If the RFID tag (Identification number) belonging to any stolen vehicle is identified by the RFID scanner at traffic signal junction, then the respective way will be blocked and also a SMS will be sent to the owner as well as the police control room by using the GSM SIM900 regarding the location of identified stolen vehicle. The emergency vehicle approaching the signal will be identified using RF modules on ARM7 LPC248 microcontroller which establish the wireless communication between the emergency vehicle and the controller unit at the traffic signal junction. The model is developed in such a way that if two emergency vehicles are approaching the junction from two different directions, then the emergency vehicle which is at shortest distance and first established the communication with master kit at the signal is allowed to cross the junction first by giving the green signal where the second one is given with green signal immediately after the first vehicles crosses the junction.

**Keywords:** GSM, RFID, RF, Traffic, Congestion, Emergency Vehicle, Stolen

## I. INTRODUCTION

India is the second highest populated country in the world with a fast growing economy. The blockade of traffic has become one of the biggest problems of transport in India which is faced by millions of commuters each day. [1] The number of vehicles in India is quickly increasing as a growing middle class can now afford to buy cars. Indian roads are mostly non-lane based and messy in most of the major metro cities across the country. Traffic control systems which are currently being used are not able to meet the desired requirements in reducing the congestion of traffic. The recent trends of road transport include the usage of various wireless technologies to reduce the congestion and to provide the cost effective solutions for smooth transition of traffic. Wireless technologies like RFID,GSM,RF modules, Zigbee can be used in providing the cost effective solutions for congestion control of traffic to achieve the smooth transition of traffic. RFID uses the radio frequency electromagnetic energy to transfer the information between RFID reader and RFID tag. Some general RFID readers will work only for shorter distance of few inches, while some work for a distance of 100 meters or more. A GSM modem contains a slot for SIM card where we can insert a SIM card and operates on a subscription to a mobile operator similar to a mobile phone. These GSM modems are

operated and controlled using AT commands. The RF modules use radio waves for transmission and the frequency of radio waves varies from 3Hz to 300GHz. Frequency refers to the rate of oscillation of the radio waves. Radio Frequency propagation occurs at the speed of light. RF waves are naturally produced from sun flares, lightning and from stars in space that radiate RF waves in the process of aging.

## II. LITERATURE SURVEY

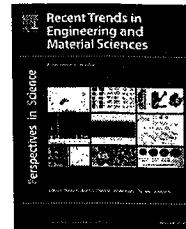
Congestion of traffic has become a major problem in almost all the cities of developing countries like India. Congestion of traffic is leading to the slow movement of vehicles and blockade of emergency vehicles like ambulance and fire trucks. A simple and traditional system of green and red lights which is operated by giving green and red signals to traffic at a multi road junctions are not able to provide the solution for today's traffic problems.[2] Green wave system which was used for emergency vehicle clearance is not able to meet the current requirements because it fails when there is any disturbance of green wave and causes the remaining vehicles to have more delay before they reach green signal. The current road transport system is using RFID systems. [3] The advantage of RFID system is a multilane, multi road junction and multi vehicle based system. This system can



Available online at [www.sciencedirect.com](http://www.sciencedirect.com)

**ScienceDirect**

journal homepage: [www.elsevier.com/pisc](http://www.elsevier.com/pisc)



# Load distribution using multipath-routing in wired packet networks: A comparative study<sup>☆</sup>

N. Krishna Chaitanya<sup>a,\*</sup>, S. Varadarajan<sup>b</sup>

<sup>a</sup> Research Scholar, ECE Department, JNTUCE, Kakinada, India

<sup>b</sup> Professor, ECE Department, S V University College of Engineering, Tirupati, India

Received 2 February 2016; accepted 11 April 2016

Available online 26 April 2016

## KEYWORDS

Multipath-routing;  
Load balancing;  
Congestion

**Summary** This paper aimed towards the analysis of various multipath routing techniques with and without load balancing as a comparative study. Most of the routing techniques targeted to find best path from source to destination. The basic routing techniques are based on single path; there is only one path from sending end to receiving end. There after multipath routing techniques has been proposed to send the data in multiple paths and eliminates the drawbacks in single path routing. This study gives better idea about multipath routing techniques along with load balance for avoiding congestion in wired packet networks.

© 2016 Published by Elsevier GmbH. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

## Introduction

Routing is the process of sending data from source to destination by making use of the best path through the network. Data packet can be routed either by using single and multi-path routing techniques. In a single path routing, data is sent over a single path and in multipath routing, the data is sent over a number of multiple potential paths available at that instant (Domzal et al., 2015; Xin et al., 2009). As

the traffic on internet increases, congestion will occur in the network and its performance decreases (Tanaka, 2011). Most widely used routing to avoid congestion is multi path routing technique (Xin et al., 2009). Major advantage of multi-path routing: any failure in any path, data will be routed in alternate paths and hence throughput will increase dramatically (Domzal et al., 2015). A network is more efficient when a router is capable of dividing the traffic over multiple paths. Packet distribution and delivery is ensured by using multipath-routing technique (Li et al., 2011).

Load balancing is another technique used to eliminate congestion by distributing the data packets through the network based on available network resources. In load balance, it decides how much load should be sent over each path (Key et al., 2007). In which, number of paths is decided by multipath routing algorithm.

<sup>☆</sup> This article belongs to the special issue on Engineering and Material Sciences.

\* Corresponding author. Tel.: +91 8019255212.

E-mail address: nosinakc@gmail.com (N.K. Chaitanya).



## A Novel Method for Segmentation of Tissues in MR Images Based on C-Means Algorithm

S. DIVYA<sup>1</sup>, N. KRISHNA CHAITANYA<sup>2</sup>

<sup>1</sup>PG Scholar, Dept of ECE, PBR Visvadaya Institute of Technology and Science, Kavali, JNTUA, AP, India.

<sup>2</sup>Associate Professor, Dept of ECE, PBR Visvadaya Institute of Technology and Science, Kavali, JNTUA, AP, India.

**Abstract:** This paper presented a new approach for robust segmentation of Magnetic Resonance images that have been corrupted by intensity in homogeneities and noise. The algorithm is formulated by modifying the objective function of the standard fuzzy C-means (FCM) method to compensate for intensity in homogeneities. A additional term is injected into the objective function to constrain the behavior of membership functions with the neighborhood effect. And an adaptive K-means clustering algorithm that initializes the centroids is described. The efficacy of the algorithm is demonstrated on both simulated and real Magnetic Resonance images.

**Keywords:** Wrapping Based Curvelet, Spatial Fuzzy C Means, Segmentation and Magnetic Resonance Imaging.

### I. INTRODUCTION

In Many clinical and research applications using Magnetic Resonance images require a segmentation into different intensity classes which are regarded as the best available representations for biological tissues. Unfortunately, segmentation methods for performing tissue classification are hindered by multiple imaging artifacts such as noise, intensity in homogeneities, and partial volume effects. The majority of intensity in homogeneities are caused by the irregularities of the scanner magnetic fields—static ( $B_0$ ), radio-frequency ( $B_1$ ) and gradient fields, which produce spatial changes in tissue statics. Partial volume effects occur where multiple tissues contribute to a single voxel, making the distinction between tissues along boundaries more difficult. Noise in MR images can induce segmentation regions to become disconnection. Therefore, it is important to take advantage of useful date while at the same time overcoming potential difficulties. Segmentation can be a fully automatic process, but it achieves its best results with semi-automatic algorithms, i.e. algorithms that are guided by a human operator. This concept of semi-automatic process naturally involves an environment in which the human operator will interact with the algorithms and the data in order to produce optimal segmentations. The simplest example of the need of a human intervention during the task of segmentation results from the specificity of the existing algorithms: depending on the type of input data, the operator will have to carefully pick the best adapted algorithm, which most of the time cannot be done in an automatic way.

The subjective point of view of the human is required. Image segmentation has become an essential tool in the medical field with the generalization of diagnosis using Magnetic Resonance Imaging (referred to as MRI), image segmentation is often required to allow doctors and surgeons to analyze the patients data, e.g. prior to surgery to determine the exact location of an organ or a tumor. MRI, also known as Nuclear Magnetic Resonance, is a method used mainly (but not only) in medical applications to visualize the insides of a patient in a harmless fashion. It relies on the relaxation properties of excited hydrogen nuclei in water after the body or part of the body to image has been placed in a powerful and uniform magnetic field. The obvious benefit of this technique is its harmless character, compared to other techniques such as CT scans and X-rays in which the patient is exposed to ionizing radiations. 3D and 4D (3D + time) MRI is increasingly used in diagnosis and therapy.

The data acquired from MRI is generally presented as a volumetric image that can be viewed as a series of slices following one of the 3 axes: sagittal (following the X axis), coronal (following the Y axis) or axial (following the Z axis). The aim of the segmentation process is to locate with the highest accuracy possible the boundaries of a special part of the image (an organ, a tumor...), thus allowing the use of 3D information for planning of treatment, navigation or visualization. Once this task is achieved, simulation, pre-computations or training can be performed to prepare the real operation. In this project we try to develop a segmentation algorithm for abnormal MRI images using Fuzzy C-means clustering technique and also to compare the results with the earlier techniques like Region growing method, K-means clustering algorithms. Abnormal brain images from four classes metastases, meningioma, glioma and astrocytoma are being used in this work.

### II. BACKGROUND

#### A. A mathematical definition of segmentation

The following is a very general definition of image segmentation. It uses a homogeneity predicate  $P()$  that helps formalizing the notion of homogeneity in an image: a region  $R$  is homogeneous if and only if  $P(R) = \text{True}$ . Therefore, the homogeneity can be defined in infinity of

# Removal Of Salt And Pepper Noise Using Advanced Modified Decision Based Unsymmetric Trimmed Median Filter In Colour And Gray Scale Images

N.KRISHNA CHAITANYA

Associate Professor, ECE Dept.,

PBR VITS, Kavali, Nellore (Dt.), AP, INDIA

SK.MAHENDRA BABU

PG Scholar, DSCE, ECE Dept.,

PBR VITS, Kavali, Nellore (Dt.), AP, INDIA

**Abstract:-** An improved decision-based algorithm for the restoration of gray-scale and colour images that are highly corrupted by Salt-and-Pepper noise, is proposed in this paper which efficiently removes the salt and pepper noise while preserving the details in colour images using Iterative Modified Decision based Unsymmetric Trimmed Median Filter. The performance of the proposed method is analyzed by using various qualities of metrics, such as Mean Square Error (MSE) and Peak Signal to Noise ratio (PSNR). Simulation results clearly show that the proposed method is out performs both in qualitative as well quantitative fidelity criteria, when it is compared with MDBUTMF.

**Index Terms-** Image; Impulse Noise; Median Filter; Noise Density;

## I. INTRODUCTION

Image noise is random (not present in the object imaged) variation of brightness or colour information in images, and is usually an aspect of electronic noise. It can be produced by the sensor and circuitry of a scanner or digital camera. Image noise can also originate in film grain and in the unavoidable shot noise of an ideal photon detector. Image noise is an undesirable by-product of image capture that adds spurious and extraneous information.

The original meaning of "noise" was and remains "unwanted signal"; unwanted electrical fluctuations in signals received by AM radios caused audible acoustic noise ("static"). By analogy unwanted electrical fluctuations themselves came to be known as "noise".[1] Image noise is, of course, inaudible.[2]

The magnitude of image noise can range from almost imperceptible specks on a digital photograph taken in good light, to optical and radio astronomical images that are almost entirely noise, from which a small amount of information can be derived by sophisticated processing (a noise level that would be totally unacceptable in a photograph since it would be impossible to determine even what the subject was).

Fat-tail distributed or "impulsive" noise is sometimes called salt-and-pepper noise or spike noise.[7] An image containing salt-and-pepper noise will have dark pixels in bright regions and bright pixels in dark regions.[8] This type of noise can be caused by analog-to-digital converter errors, bit errors in transmission, etc.[9][10] It can be mostly eliminated by using dark frame subtraction,

median filtering and interpolating around dark/bright pixels.

An image is a picture, photograph or any other form of 2D representation of any scene.[21] Most algorithms for converting image sensor data to an image, whether in-camera or on a computer, involve some form of noise reduction. There are many procedures for this, but all attempt to determine whether the actual differences in pixel values constitute noise or real photographic detail, and average out the former while attempting to preserve the latter. However, no algorithm can make this judgment perfectly, so there is often a tradeoff made between noise removal and preservation of fine, low-contrast detail that may have characteristics similar to noise. Many cameras have settings to control the aggressiveness of the in-camera noise reduction.

A simplified example of the impossibility of unambiguous noise reduction: an area of uniform red in an image might have a very small black part. If this is a single pixel, it is likely (but not certain) to be spurious and noise; if it covers a few pixels in an absolutely regular shape, it may be a defect in a group of pixels in the image-taking sensor (spurious and unwanted, but not strictly noise); if it is irregular, it may be more likely to be a true feature of the image. But a definitive answer is not available.

This decision can be assisted by knowing the characteristics of the source image and of human vision. Most noise reduction algorithms perform much more aggressive chroma noise reduction, since there is little important fine chroma detail that one risks losing. Furthermore, many people find luminance noise less objectionable to the eye, since



## A Novel Method for Image Denoising using Non local Means Filter Based On Similarity Validation

K. HIMA BINDU<sup>1</sup>, N. KRISHNA CHAITANYA<sup>2</sup>

<sup>1</sup>PG Scholar, Dept of ECE, PBR Visvodaya Institute of Technology and Science, Kavali, JNTUA AP, India.

<sup>2</sup>Associate Professor, Dept of ECE, PBR Visvodaya Institute of Technology and Science, Kavali, JNTUA, AP, India.

**Abstract:** Nonlocal means is one of the well known and mostly used image denoising methods. The conventional nonlocal means approach uses weighted version of all patches in a search neighbourhood to denoise the center patch. However, this search neighbourhood can include some dissimilar patches. In this paper, we propose a pre-processing hard thresholding algorithm that eliminates those dissimilar patches. Consequently, the method improves the performance of nonlocal means. The threshold is calculated based on the distribution of distances of noisy similar patches. The method denoted by Similarity Validation Based Nonlocal Means (NLM-SVB) shows improvement in terms of PSNR and SSIM of the retrieved image in comparison with nonlocal means and some recent variations of nonlocal means.

**Keywords:** NLM-SVB, PSNR and SSIM.

### I. INTRODUCTION

As digital imaging technologies become more advanced, the issue of image denoising still remains as a challenging stage. Removing additive noise is an essential pre-processing step in the majority of image processing techniques such as classification and object recognition, or it can be used for the purpose of improving image visual quality. Some of the earliest methods of denoising are simple averaging filters such as mean, median, Gaussian smoothing filters, and bilateral filters [1]. There are methods that transform data to other bases for the purpose of denoising such as wavelet or curvelet based methods [2]. The concentration of this paper is on nonlocal means methods (NLM) that are preferred when algorithm complexity is an issue. Most local methods only consider a local patch around the target pixel, assuming adjacent pixels tend to have similar patches. On the other hand, nonlocal means takes advantage of existence of a pattern or similar features in including the non-adjacent pixels [3]. NLM exploits self-similarities in the search neighbourhood to estimate the true value of the noisy pixel. Since the introduction of NLM, many other variations have been proposed to further improve the method from various perspectives. For example, NLM with shape adaptive patches (NLM-SAP) is examined in [4].

The work in [5], improves NLM by a post processing denoising step based on method noise smoothing. Another recent improvement, probabilistic nonlocal means (PNLM) [6], implements a new weight function based on the distribution of the distances of similar patches. This weighting scheme outperforms the Gaussian kernel weights in traditional NLM. Regardless of the choice of the weights, many dissimilar patches in the search neighbourhood are processed through NLM. Methods such as probabilistic early termination (NLM-PET) [7] attempt to reduce this number by a pre-processing hard-thresholding. However, the overall performance of this method is worse than that of the traditional NLM. A pre-filtering process is suggested in [8] to eliminate unnecessary patches by comparing gradient and average gray value of candidate similar patches. Motivated by the issue of unnecessary processing of dissimilar patches, we propose a new hard thresholding pre-processing algorithm to eliminate dissimilar patches before the weighting process. Our proposed method is faithful to the probabilistic distribution of the distance of similar patches. Our simulation results confirm superiority of this approach compared to the traditional NLM and the above variations of this method.

### II. PROBLEM FORMULATION

We consider an image corrupted with an additive white Gaussian noise (AWGN) with zero mean and variance  $\sigma^2$ , where  $y_i$  is the  $i$ th noisy pixel value and  $x_i$  is the  $i$ th true pixel value:

$$y_i = x_i + n_i; \quad \forall i: n_i \sim \mathcal{N}(0, \sigma^2) \quad (1)$$

The goal is to recover the noise free image from the observed noisy image. In the conventional NLM methods, each estimated pixel,  $\hat{x}_i$ , is a weighted average of other pixels in a search neighbourhood  $S_i$ :

$$\hat{x}_i = \frac{\sum_{j \in S_i} w_{i,j} y_j}{\sum_{j \in S_i} w_{i,j}} \quad (2)$$

Where  $w_{i,j}$  is the weight between square patches centered at pixels  $i$  and  $j$ . The weight is a function of squared value of  $l_2$ -norm distance between two local patches  $P_i$  and  $P_j$  with centers at pixels  $i$  and  $j$ :

## A NEW QUEUING TECHNIQUE IN ADAPTIVE MULTIPATH ROUTING FOR CONGESTION CONTROL WITH PACKET PRIORITY IN WIRED DATA NETWORKS

N.Krishna Chaitanya<sup>1</sup>, S.Varadarajan<sup>2</sup>

<sup>1</sup>Research Scholar, ECE Department, JNT University College of Engineering, Kakinada, INDIA;

<sup>2</sup>Professor, ECE Department, S V University College of Engineering, Tirupati, INDIA

Corresponding Author, Received: 15 June 2016, Revised: 08 August 2016, Accepted: 29 Nov 2016

**ABSTRACT:** This paper proposes a new queuing technique in Adaptive Multi-Path routing based on packet priority. Simultaneous Multi-Path routing is used to improve the data performance over a congested network. The traditional method of transmitting the data is done by using Simultaneous Multi Path Communication (SMPC). Two types of SMPCs are proposed, in which SMPC-I, which uses multiple paths independently and SMPC-P, which uses path priority control algorithm in conjunction with SMPC. SMPC-I and SMPC-P maintains throughput regardless of path length and priority control. In addition to available SMPC methods, proposed method provides better solution to improve the performance of communication network. A theoretical approach of AMPC-PP proposed here based on packet priority for important data over normal data on a congestion network with route adaptability.

**Keywords:** *Multi-path communication, Path priority, Independent paths, Packet priority.*

### 1. INTRODUCTION

A Network comprises a number of nodes and links for processing of data from source to destination. The process of transmitting the data from source to destination is called routing and it is done by making use of the best path through the network. Data packet can be routed either by using single or multipath routing techniques [1]. Single path routing is the traditional method of transmitting the data through the network. But, the major problems here with this scenario are: less network bandwidth utilization, more delay; if any node or link fails entire data will be lost, less throughput and leads to scope for congestion. These problems can be minimized by using multipath routing. Here in this method, a number of hosts are connected by using a number of nodes and links. All node and link capacities differ in the network. Data packets are transmitted from source to destination through a number of paths. Best paths are selected based on shortest path and it is computed in the network based on traffic. Paths are selected by the type of service requested by the user in the network. For different applications, multiple paths may be used to meet their requirements [2].

Multipath transmission is realized in source and hop-by-hop routing, multi-topology routing, Software-Defined Networks, Multi-Protocol Label Switching, Flow-Aware Multi-Topology Adaptive Routing that interconnects a number of links in network virtualization, and Multipath TCP [2]. The major advantage of choosing multi-path routing is reduced delay.

### 2. LITERATURE REVIEW

Although, multi-path routing is used to reduce congestion by splitting the data over several potential paths without knowing the path capacity. This problem can be minimized by using load balancing technique. In load balancing, load over a path is decided by available resources and traffic in that particular path [1]. A number of multipath routing techniques have been proposed. The basic technique is Simultaneous Multi-Path Communication (SMPC) [3]. First method in SMPC is SMPC-I based on independent paths. This method is based on bandwidth control. Second method is SMPC-P, which is based on path priority. These techniques does not support for packet priority. The major drawbacks in these methods are greater delay and reduced network performance [4].

A method proposed by Peter Key et al. [5] for avoiding congestion in multi path routing using load balancing, but this method is unable to route the data packets if there are more link failures.

There after a number of multi path routing techniques proposed with load balancing [1], [6-9], but these methods requires more control messages, does not support for route recovery, as well as supports only for single link failures.

Paganini proposed Multi Protocol Label Switching (MPLS). This method provides better routing and capable of interfacing to existing routing protocols, but it requires additional layer between data link and network layer and also router requires knowledge about MPLS [10].

**BLOCK BASED SVD APPROACH FOR ADDITIVE WHITE GAUSSIAN NOISE LEVEL ESTIMATION IN SATELLITE IMAGES****M.Srinivas<sup>1</sup> and K. Ravi Babu<sup>2</sup>**<sup>1</sup>Asst. Professor, Dept. of EIE, VR Siddhartha Engineering College, Vijayawada<sup>2</sup>Assoc. Professor, Dept. of ECE, PBRVITS, Kavali, ravibab

**Abstract-** In this digital era, estimation of noise and de-noise of digital image is one of the chart-topping fields. In real time, noise may happen at any stage starts from capturing to reception. Noise estimation is ever challenging field even till now. Additive White Gaussian Noise is the basic type when dealing with images on statically way of studying. So, In this paper, as a first step we proposed an effective technique for the estimation of noise in a satellite image by using Block based SVD approach. This paper addresses the following steps 1)Noise estimation by trail method of singular values 2) Corrupting the image by known noise and study the change 3) Divide the whole image into blocks and add the known noise to the image and finally retrieve the effect on original image. It is one of best techniques for estimating AWGN in a real-time.

**Keywords-** Additive White Gaussian Noise, Estimation of noise, Singular Values, Singular Value Decomposition

**I. INTRODUCTION**

One of the inevitable things in image processing is the. It can severely disturb the original image. It corrupts the image visually or in any manner. As a basic step for my paper focused on SVD Domain noise estimation[1],[6].There are so many sources of the noise [7]-[8] for a digital image. As a start for this paper is to study the noise in an image, estimate the noise by following the specific method. Final step is De-noising the image to enhance the visual interpretation (Enhancement).Image segmentation [9]-[10] is also one of the best areas of research fields for studying Radar, Remote sensing data, Medical Images etc. There is a lot of research is going on image de- noising methods and restoration fields. A Plenty of beautiful algorithms are have been discussed in [11] but in this paper we have simply focused on the estimation of AWGN noise rather than how to remove it. In fact a thorough investigation is deeply needed in this digital domain to present best over the better version. As a step going further Segmentation, Feature Extraction, Motion Detection, Compression are one of the most research fields in Digital Image Processing.

For simplicity (Zero mean Additive Noise) started with AWGN noise estimation A can be expressed as

$$A(x, y) = Ao(x, y) + N(x, y) \dots\dots\dots(1)$$

Where  $A(x, y)$  represents original image and  $N(x,y)$  is the noise present at that location.

$x, y$  are the spatial coordinates of an image. The representation of Gaussian Image is

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \dots\dots\dots(2)$$

Where  $\sigma$  is the noise standard deviation and  $\mu$  represents the average of the noise .Generally consider the zero AWGN noise whose  $\mu$  value is zero ( $\mu=0$ ).Now the distribution of noise is purely depends on standard deviation  $\sigma$ , which places the main role in our paper.

Let us going into the concept in depth, there mainly two problems are coming into picture to proceed further. 1. Preparation of the noise database having the minimum impact on original image. 2. How blocking pattern is implemented on a whole image. Basically three methods are have been implemented so far. They are 1. Filtering 2. Block based 3. Transform based. Adaptability of noise



## Fault Tolerant of FIFO Buffers of NoC Router

G.PRASANTHI<sup>1</sup>, T.SUNEEL KUMAR<sup>2</sup>

<sup>1</sup>PG Scholar, Dept of ECE, PBR Visvodaya Institute of Technology and Science, Kavali, Affiliated to JNTUA, AP, India.  
<sup>2</sup>Assistant Professor, Dept of ECE, PBR Visvodaya Institute of Technology and Science, Kavali, Affiliated to JNTUA, AP, India.

**Abstract:** This brief proposes an on-line straightforward test system for discovery of inert hard blames which create in first info first yield supports of switches amid field operation of NoC. The method includes rehashing tests intermittently to forestall collection of deficiencies. A model usage of the proposed test calculation has been incorporated into the switch channel interface and on-line test has been performed with manufactured self-comparable information activity. The execution of the NoC after expansion of the test circuit has been explored as far as throughput while the region overhead has been considered by integrating the test equipment. Likewise, an on-line test strategy for the directing rationale has been proposed which considers using the header bounces of the information activity development in transporting the test designs.

**Keywords:** FIFO Cushions, In-Field Test, NoC, Changeless Blame, Straightforward Test.

### I. INTRODUCTION

Throughout the most recent decade, organize on-chip (NoC) has risen as a superior correspondence foundation contrasted and transport based correspondence arrange for complex chip outlines conquering the troubles identified with data transfer capacity, flag respectability, and power dispersal [1]. Be that as it may, similar to every single other framework on-a-chip (SoCs), NoC-based SoCs should likewise be tried for deformities. Testing the components of the NoC framework includes testing switches and interrouter joins. Significant measure of zone of the NoC information transport medium is possessed by switches, which is overwhelmingly involved by FIFO supports and directing rationale. In like manner, the probabilities of run-time blames or deformities happening in supports and rationale are altogether higher contrasted and alternate segments of the NoC. In this way, test prepare for the NoC framework must start with trial of cradles and routing rationale of the switches. Also, the test must be performed occasionally to guarantee that no blame gets collected. The incidental run-time practical issues have been one of the significant worries amid testing of profoundly scaled CMOS-based recollections. These shortcomings are an aftereffect of physical impacts, for example, environmental susceptibility, maturing, and low supply voltage and subsequently are irregular (nonpermanent showing gadget harm or glitch) in nature [2]. Be that as it may, these discontinuous blames for the most part display a generally high event rate and in the long run tend to wind up distinctly changeless [2]. In addition, destroy of recollections likewise cause irregular flaws to end up distinctly visit enough to be delegated changeless. In this way, there is a requirement for online test procedure that can distinguish the run-time shortcomings, which are irregular in nature yet bit by bit get to be distinctly changeless after some time.

### A. Contribution

In this brief, we have proposed an onlineransparent test method for first-input first-yield (FIFO) supports and directing rationale presentwithin the switches of the NoC framework. Our commitments are as per the following. A straightforward SOA-MATS++ test era calculation has proposed focusing in-field perpetual shortcomings created in SRAMbased FIFO recollections and it has been used to perform on the web and intermittent trial of FIFO memory exhibit inside the switches of the NoC. Likewise, we have additionally proposed an online test method for the directing rationale that is performed all the while with the trial of cushions. The proposition includes two methods for using the unused segment of the header bounces of the approaching information parcels in transporting the test designs. In the first place, deterministic test designs for the directing rationale produced by Tetramax are set in the unused fields of the header flutter and are transported amid the ordinary cycle. Second, the pseudorandom designs in the engineered information activity utilized amid ordinary operation and touching base at the steering rationale are considered as test examples. Blame scope is evaluated for both of the two recommendations.

### B. Fault Models Considered for the Work

The run-time lasting shortcomings considered in this brief are thought to be discontinuous deficiencies, which have turned out to be changeless after some time. Thusly, the blame models considered in this brief are that of discontinuous flaws. The essential variables that prompt to irregular issues are maturing impacts, for example, time-subordinate dielectric breakdown (TDDB), electromigration, negative inclination temperature flimsiness (NBTI), and hot bearer infusion (HCl), as said in [3]. TDDB is a marvels where the oxide underneath the door material of a MOSFET

## Effective Implementation of AES Algorithm using Reversible Logic

C. V. KAVYA SUVARCHALA

Assistant Professor, Dept of ECE, PBR Visvadaya Institute of Technology and Science, Kavali, Nellore, AP, India.

**Abstract:** With the fast progression of data exchange in electronic way information security is becoming more important in data storage & transmission. There are so many implementations for providing security. This effective implementation of aes algorithm using reversible logic is one of the method for providing security. In this field we are providing security to the network through cryptographic algorithms. The present project presents an effective implementation of aes algorithm using reversible logic and it presents the design of a 128 bit encoder for data encryption. Optimized & synthesized VHDL code is developed for the implementation of 128 bit encryption process. XILINX ISE 13.2I software is used for synthesis.

**Keywords:** Advanced Encryption Standard (AES), Add Round Key (ARK), Byte Substitution (BS), Shift Row (SR) and Mix Columns (MC).

### I. INTRODUCTION

Reversible logic circuits have attracted the attention of researchers in recent years for mainly two reasons. Firstly, Landauer showed that during logic computation, every bit of information loss generates  $KT\ln 2$  joules of heat energy, where  $K$  is the Boltzmann's constant and  $T$  is the absolute temperature of environment. And, according to Bennet[1] , for theoretically zero energy dissipation, computations have to be reversible in nature. Secondly, quantum computations which are the basis of quantum computers are reversible in nature. In the field of cryptography, there has been many works that propose hardware implementations of cryptographic primitives[5]. Some of these implementations use optimized architectures for high-speed operations, some for area-efficiency targeted to low-cost implementations where speed is not the major concern, some more general-purpose with limited capabilities of reconfigurability, while some optimized for low-power applications. By their very design, some of the cryptographic primitives like encryption and decryption are reversible in nature. However, to the best of the knowledge of the authors, no complete reversible logic implementations of such algorithms have been reported. However, some works on the reversible implementations of specific subsystems of a cryptographic processor, namely the Montgomery multiplier, have been published [3] [4].

Another motivation for studying reversible logic implementation of cryptographic algorithms results from the fact that side-channels in hardware implementations of such

algorithms have been widely studied in recent times [2]. Side-channel attack is considered to be a very cost-effective alternative to attacking traditional cryptographic algorithms, and designers use various countermeasures in this regard. Power analysis attack is one of the easiest attack to mount, and is based on the variations in power dissipation during a computation. Since reversible logic circuits are expected to consume much less energy as compared to traditional CMOS logic, variations in power consumptions will be less and hence side-channel attacks will be more difficult to mount. With this motivation, this paper reportsthe results of reversible logic implementation of a state-of-the-art block cipher, the 128-bit Advanced Encryption Standard (AES). The rest of the paper is organized as follows. Section 2 introduces some basic concepts in reversible logic synthesis. Section 3 serves dual purpose; it gives brief introductions to the various steps in AES encryption process, and also discusses the reversible logic implementations of the same. Section 4 discusses the synthesis framework, and presents the experimental results. Section 5 summarizes the paper and identifies a few areas for future work.

### II. REVERSIBLE LOGIC & REVERSIBLE GATES

A Boolean function  $f : B^n \rightarrow B^n$  is said to be reversible if it is bijective. In other words every input vector is uniquely mapped to an output vector. The problem of synthesis is to determine a reversible circuit that realizes a given function  $f$ . In this paper, for the purpose of synthesis we consider the gate library consisting of multiple-control Toffoli (MCT) gates. An  $n$ -input MCT gate with inputs  $(x_1, x_2, \dots, x_n)$  pass the first  $(n-1)$  inputs unchanged, and complements the last input if all the remaining  $(n-1)$  inputs are at 1. Fig.1 shows an  $n$ -input MCT gate. A simple NOT ( $n = 1$ ) and controlled-NOT ( $n = 2$ ) are special cases of the MCT gate.

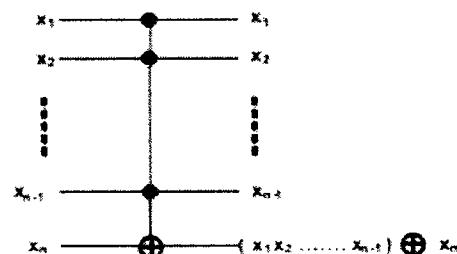
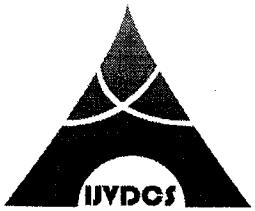


Fig.1. n-input MCT gate.

**Effective Implementation of AES Algorithm using Reversible Logic****C.V. KAVYA SUVARCHALA**

Assistant Professor, Dept of ECE, PBR Visvodaya Institute of Technology and Science, Kavali, Nellore, AP, India.

**Abstract:** With the fast progression of data exchange in electronic way information security is becoming more important in data storage & transmission. There are so many implementations for providing security. This Effective Implementation of AES Algorithm using Reversible Logic is one of the method for providing security. In this field we are providing security to the network through cryptographic algorithms. The present project presents An Effective Implementation of AES Algorithm Using Reversible Logic and it presents the design of a 128 bit encoder for data encryption. Optimized & synthesized VHDL code is developed for the implementation of 128 bit encryption process. XILINX ISE 13.2I software is used for synthesis.

**Keywords:** AES, Effective Implementation, Algorithm, Reversible, Logic, Xilinx, ISE.

**I. INTRODUCTION**

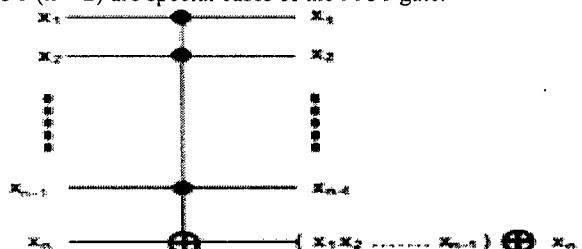
Reversible logic circuits have attracted the attention of researchers in recent years for mainly two reasons. Firstly, Landauer showed that during logic computation, every bit of information loss generates  $KT\ln 2$  joules of heat energy, where  $K$  is the Boltzmann's constant and  $T$  is the absolute temperature of environment. And, according to Bennet[1], for theoretically zero energy dissipation, computations have to be reversible in nature. Secondly, quantum computations which are the basis of quantum computers are reversible in nature. In the field of cryptography, there has been many works that propose hardware implementations of cryptographic primitives[5]. Some of these implementations use optimized architectures for high-speed operations, some for area-efficiency targeted to low-cost implementations where speed is not the major concern, some more general-purpose with limited capabilities of reconfigurability, while some optimized for low-power applications. By their very design, some of the cryptographic primitives like encryption and decryption are reversible in nature. However, to the best of the knowledge of the authors, no complete reversible logic implementations of such algorithms have been reported. However, some works on the reversible implementations of specific subsystems of a cryptographic processor, namely the Montgomery multiplier, have been published [3] [4].

Another motivation for studying reversible logic implementation of cryptographic algorithms results from the fact that side-channels in hardware implementations of such algorithms have been widely studied in recent times [2]. Side-channel attack is considered to be a very cost-effective alternative to attacking traditional cryptographic algorithms, and designers use various countermeasures in this regard. Power analysis attack is one of the easiest attack to mount, and is based on the variations in power dissipation during a computation. Since reversible logic circuits are expected to consume much

less energy as compared to traditional CMOS logic, variations in power consumptions will be less and hence side-channel attacks will be more difficult to mount. With this motivation, this paper reports the results of reversible logic implementation of a state-of-the-art block cipher, the 128-bit Advanced Encryption Standard (AES). The rest of the paper is organized as follows. Section 2 introduces some basic concepts in reversible logic synthesis. Section 3 serves dual purpose; it gives brief introductions to the various steps in AES encryption process, and also discusses the reversible logic implementations of the same. Section 4 discusses the synthesis framework, and presents the experimental results. Section 5 summarizes the paper and identifies a few areas for future work.

**II. REVERSIBLE LOGIC & REVERSIBLE GATES**

A Boolean function  $f : B^n \rightarrow B^n$  is said to be reversible if it is bijective. In other words every input vector is uniquely mapped to an output vector. The problem of synthesis is to determine a reversible circuit that realizes a given function  $f$ . In this paper, for the purpose of synthesis we consider the gate library consisting of multiple-control Toffoli (MCT) gates. An  $n$ -input MCT gate with inputs  $(x_1, x_2, \dots, x_n)$  pass the first  $(n-1)$  inputs unchanged, and complements the last input if all the remaining  $(n-1)$  inputs are at 1. Figure 1 shows an  $n$ -input MCT gate. A simple NOT ( $n = 1$ ) and controlled-NOT or CNOT ( $n = 2$ ) are special cases of the MCT gate.

**Fig.1. n-Input MCT Gate**



## High Throughput Architecture for the Advanced Encryption Standard Algorithm

C. V. KAVYA SUVARCHALA<sup>1</sup>, V. SWAPNA<sup>2</sup>

<sup>1</sup>Assistant Professor, Dept of ECE, PBR Visvodaya Institute of Technology and Science, Kavali, Affiliated to JNTUA, AP, India.

<sup>2</sup>PG Scholar, Dept of ECE, PBR Visvodaya Institute of Technology and Science, Kavali, Affiliated to JNTUA, AP, India.

**Abstract:** A high throughput architecture is proposed for an efficient implementation of the Advanced Encryption Standard (AES) Algorithm. The presented architecture is adapted for AES encryptor-only as well as integrated AES encryptor/ decryptor designs. The SubBytes/InvSubBytes operations are implemented using composite field arithmetic in order to exploit the sub-pipelining advantage within the loop unrolling methodology. The proposed architecture minimizes the critical path delay through the modification of the SubBytes/InvSubBytes as well as the KeyExpansion modules. Compared to previously reported AES encryptors and integrated AES encryptors/decryptors designs, the proposed architecture provides an efficiency improvement of 61% and 29% respectively.

**Keywords:** Advanced Encryption Standard, FPGA, Sub-pipelining, Composite Field Arithmetic, Throughput.

### I. INTRODUCTION

The continuously growing number of internet and wireless communications users has marked security as a crucial designing factor for reliable communications. The Advanced Encryption Standard (AES) algorithm [1] was approved in October 2000 by the National Institute of Standards and Technologies to become the new encryption standard for its high flexibility and strong security. Several hardware implementations for the AES algorithm were previously presented targeting either ASIC as [2-4], or FPGA as [5-11]. The AES algorithm operates on 128-bit data blocks using a cipher key of possible lengths 128/192/256-bits throughout 10/12/14 iterative rounds respectively. Each round consists of a set of transformations namely: SubBytes, ShiftRows, MixColumns, AddRound Key or their corresponding inverses during decryption. All operations are performed on the 128-bits arranged in a  $4 \times 4$  matrix of bytes called State. In a parallel manner, the input cipher key is processed through a KeyExpansion module to produce 10/12/14 round keys used in each respective round [1]. The architecture of the AES round unit is the core which distinguishes each hardware design. The implementation of the SubBytes/ InvSubBytes and KeyExpansion modules is the design key for the AES round. The SubBytes/ InvSubBytes modules are implemented either using storage memory units Key Expansion module follows either the pre-computing and

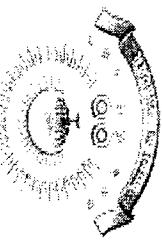
storage method as [12], or the on-the-fly computation as [4-7]. In addition, the AES complete structure may adopt the loop-unrolling approach aiming for high throughput or the iterative looping approach aiming for area minimization.

### II. RELATED WORKS

One of the best symmetric security algorithms is used to provide data security in AES. The pipelined architecture of the AES algorithm increases the throughput of the algorithm. In this Architecture, instead of passing the output of each round to the next round directly, a register is used. It avoids the direct contact between two rounds. The speed of the AES algorithm is increased by inserting compact and flexible architecture for Mix Column transform. The modifications in each round of the AES algorithm was improved for the complexity of the encryption method and making it complicated for the attacker to predict a pattern in the algorithm. In each transformation of the modified architecture, the 8-bit values are separated in to 4-bits and they are grouped and then perform the transformation process. A high data throughput AES hardware architecture is proposed in by partitioning the 10 rounds into sub blocks of repeated AES modules. To provide a complete ten stages of AES, the intermediate buffers are used to separate the blocks. Using this pipelined architecture scheme, time complexity is reduced to greater extension. A simple, linear and cryptanalysis is done on the standard S-Box to take advantage of high probability occurrences of linear expressions involving plain text bits, cipher text bits and sub-key bits. The design can run at 1.2GHz which is sufficient for online data encryption. The optimized architecture of data encryption unit and key schedule unit is applicable to wireless sensor networks. A 128-bit AES encryption and decryption using Rijndael Algorithm is designed and synthesized using verilog code which can be easily implemented with the help of FPGA. The design and performance testing algorithm was implemented with the help of dynamic partially reconfigurable FPGA.

### III. PROPOSED SYSTEM

Using composite fields, we introduce a low cost multiple parity based fault detection scheme for the s-box and inverse s-box. The s-box and inverse s-box are non-linear operations which take 8 bit input and generate 8 bit output. Normally,



## PARVATHAREDDY BABU REDDY

**VISVODAYA INSTITUTE OF TECHNOLOGY & SCIENCE**  
 (Affiliated to J.N.T.U.A, Approved by AICTE and Accredited by NAAC with 'A' Grade)  
**KAVALLI – 524201, S.P.S.R Nellore Dist., A.P. India. Ph: 08626-243930**

## **DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING**

### *List of Publications*

*Academic Year: 2017-18*

S.No	Title of paper	Name of the author/s	Department of the teacher	Name of journal	Year of publication	ISSN number	Link to the recognition in UGC enlistment of the Journal
1	A Novel Method for Transmission of Data using Barcode Modulation For Handheld Electronic Devices	Dr. A.Maheswara Rao	ECE	International Journal of Scientific Engineering and Technology Research	Sep. 2017	ISSN 2319-8885	<a href="http://ijser.com/issue.php?issue=ISSUE%2030&amp;volume=Volume6&amp;page=2">http://ijser.com/issue.php?issue=ISSUE%2030&amp;volume=Volume6&amp;page=2</a>
2	LDPC Decoding for NAND Flash Memory by using Array Dispersion	V.Narayana Reddy	ECE	International Journal of Innovative Technologies	Sep. 2017	ISSN 2321-8665	<a href="http://ijitech.org/uploads/236514ijIT15697-359.pdf">http://ijitech.org/uploads/236514ijIT15697-359.pdf</a>
3	Implementation of Area Efficient Carry-Select Adder	V.Narayana Reddy	ECE	International Journal of VLSI System Design and Communication Systems	Jan., 2018	ISSN 2322-0929	<a href="http://www.ijvdes.org/issue.php?issue=ISSUE%201 &amp; volume=Volume6&amp;page=5">http://www.ijvdes.org/issue.php?issue=ISSUE%201 &amp; volume=Volume6&amp;page=5</a>
4	Fingerprint Compression Based on Sparse Representation using FFT Method	V.Phani Bhushan	ECE	International Journal of Advanced Technology and Innovative Research	Jan., 2018	ISSN 2348-2370	<a href="http://www.ijair.org/issue.php?issue=Volume10">http://www.ijair.org/issue.php?issue=Volume10</a>
5	A Critical Research Analysis of Low-Energy Techniques for Instruction Memory Organisations in Embedded Systems	A.Suman Kumar Reddy	ECE	COMPUSOFT, An international journal of advanced computer technology	Dec. 2017	ISSN:2320-0790	<a href="https://www.ijact.in/index.php/ijact/article/view/693/563">https://www.ijact.in/index.php/ijact/article/view/693/563</a>
6	A Research Study of Power Impact of Loop Buffer Schemes for Biomedical Wireless Sensor Nodes	A.Suman Kumar Reddy	ECE	International Journal of Research	Feb.2018	e-ISSN: 2248-6848 & p-ISSN 2348-795X	<a href="http://www.ijesi.org/papers/Vol(7)/2/Versio n-3/C0702033951.pdf">http://www.ijesi.org/papers/Vol(7)/2/Versio n-3/C0702033951.pdf</a>
7	Exploration Tool for Instruction Memory Organisations Based On Accurate Cycle-Level Energy Modelling	A.Suman Kumar Reddy	ECE	International Journal of Engineering Science Invention (IJESI)	Feb.2018	ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726	<a href="http://www.ijair.org/issue.php?issue=ISSUE%201 &amp; volume=Volume10">http://www.ijair.org/issue.php?issue=ISSUE%201 &amp; volume=Volume10</a>
8	Trace of JPEG Compression and Forgery Detection using Saliency Method(Tentative)	N.Krishna Chaitanya	ECE	International Journal of Advanced Technology and Innovative Research,	Jan.2018	ISSN 2348–2370	<a href="http://www.ijvdes.org/uploads/265134IJVD CS15158-131.pdf">http://www.ijvdes.org/uploads/265134IJVD CS15158-131.pdf</a>
9	Design of High Speed Variable Latency 64-Bit Carry Skip Adder	M.Pavitra	ECE	International Journal of VLSI System Design and Communication Systems,	July.2017	ISSN 2322-0929	<a href="http://www.ijvdes.org/uploads/CS15158-131.pdf">http://www.ijvdes.org/uploads/CS15158-131.pdf</a>

10	Design of Redundant Binary Multipliers using Modified Partial Product Generator	M.Pavitra	ECE	International Journal of Research, e-	Nov,2017	ISSN: 2348-6848 p-ISSN: 2348-795X	<a href="https://journals.pen2print.org/index.php/jjr/article/view/9854">https://journals.pen2print.org/index.php/jjr/article/view/9854</a>
11	A Review on Design and Implementation of Fault Tolerant Parallel FFTs using ECC and Parseval Checks	N.V.Saichand	ECE	International Journal of Innovative Technologies	Sep,2017	ISSN 2321-8665	<a href="http://ijitech.org/uploads/153642IJIT15521-330.pdf">http://ijitech.org/uploads/153642IJIT15521-330.pdf</a>
12	Implementation of Conventional Multiplier in Reversible Logic	K.Rajesh	ECE	International Journal of VLSI System Design and Communication Systems,	Sep, 2017	ISSN 2322-0929	<a href="http://www.ijvdes.org/issue.php?issue= ISSUE%209&amp;volume=Volume5">http://www.ijvdes.org/issue.php?issue= ISSUE%209&amp;volume=Volume5</a>
13	Facial Feature Identification and Matching using Face Sketch Synthesis by Modified Sparse Technique	K.Rajesh	ECE	International Journal of Advanced Technology and Innovative Research	Jan,2018	ISSN 2348-2370	<a href="http://www.ijatir.org/issue.php?issue= ISSUE%201&amp;volume=Volume10">http://www.ijatir.org/issue.php?issue= ISSUE%201&amp;volume=Volume10</a>
14	Non-Uniform Templates for Near Duplicate Image Matching	K.Rajesh	ECE	International Journal of Advanced Technology and Innovative Research,	April,2018	ISSN 2348-2370	<a href="http://www.ijatir.org/uploads/362451IJATIR16825-94.pdf">http://www.ijatir.org/uploads/362451IJATIR16825-94.pdf</a>
15	Efficient Approaches for Designing Quantum Costs of Various Reversible Gates	M.Surekha	ECE	International Journal of Engineering Studies	Nov, 2017	ISSN 0975-6469	<a href="https://pdfs.semanticscholar.org/928e/5871ff652916babfb65062d15cc3eb14492.pdf">https://pdfs.semanticscholar.org/928e/5871ff652916babfb65062d15cc3eb14492.pdf</a>
16	Design of Area Efficient High-Performance 2-4 and 4-16 Mixed-Logic Line Decoders	LML.Narayana reddy	ECE	INTERNATIONAL JOURNAL OF PROFESSIONAL ENGINEERING STUDIES	Dec,2017		<a href="http://www.ipies.com/pdf37/46.pdf">http://www.ipies.com/pdf37/46.pdf</a>
17	Transferring the Health Details of Animal using Zigbee Module	K.Ashok Kumar	ECE	International Journal of Scientific Engineering and Technology Research	Sep,2017	ISSN 2319-8885	<a href="http://ijsetr.com/uploads/461235IJSETR1551-996.pdf">http://ijsetr.com/uploads/461235IJSETR1551-996.pdf</a>
18	An Approach to Control and Monitor Environmental Parameters in Greenhouse using ARM	K.Ashok Kumar	ECE	International Journal of Advanced Technology and Innovative Research,	Oct,2017	ISSN 2348-2370	<a href="http://www.ijatir.org/issue.php?issue= ISSUE%201&amp;volume=Volume1351.pdf">http://www.ijatir.org/issue.php?issue= ISSUE%201&amp;volume=Volume1351.pdf</a>
19	Design And Implementation of FM0/Manchester Encoder Using Sols Technique	K.Ashok Kumar	ECE	International Journal of VLSI Design and Communication Systems	Jan, 2018	ISSN 2322-0929	<a href="http://www.ijvdes.org/issue.php?issue= ISSUE%206&amp;volume=Volume6&amp;page=6">http://www.ijvdes.org/issue.php?issue= ISSUE%206&amp;volume=Volume6&amp;page=6</a>
20	A Novel High Speed Memory Solution using TCAM	K.Ashok Kumar	ECE	International Journal of Innovative Technologies	Jan, 2018	ISSN 2321-8665	<a href="http://www.internationaljournalssg.org/IJECE/2017/Volume4-Issue4/IJECE-V4I7P102.pdf">http://www.internationaljournalssg.org/IJECE/2017/Volume4-Issue4/IJECE-V4I7P102.pdf</a>
21	Construction and Design of Microcontroller Embedded Based Viscometer	D.Uma Maheswara Reddy	ECE	SRRG International Journal of Electronics and Communication Engineering (SRRG-IIECE)	July, 2017	ISSN: 2348 – 8549	<a href="http://www.internationaljournalssg.org/IJECE/2017/VOLUME4-ISSUE4/IJECE-V4I7P102.pdf">http://www.internationaljournalssg.org/IJECE/2017/VOLUME4-ISSUE4/IJECE-V4I7P102.pdf</a>

*V. Brosoth Kumar*  
Faculty Incharge

*Head of the Department*  
Electronics & Co-Head of the Department  
**BVR Visvodaya Institute of**  
**Technology & Science CP**  
VATI

## A Novel Method for Transmission of Data using Barcode Modulation for Handheld Electronic Devices

SK. MUJEEBA<sup>1</sup>, A. MAHESWARA RAO<sup>2</sup>

<sup>1</sup>PG Scholar, Dept of ECE, PBR Visvodaya Institute of Technology and Science, Kavali, JNTUA, AP, India.

<sup>2</sup>Professor, Dept of ECE, PBR Visvodaya Institute of Technology and Science, Kavali, JNTUA, AP, India.

**Abstract:** The concept of 2-D barcodes is of great relevance for use in wireless data transmission between handheld electronic devices. In a typical setup, any file on a cell phone, for example, can be transferred to a second cell phone through a series of images on the LCD which are then captured and decoded through the camera of the second cell phone. In this study, a new approach for data modulation in 2-D barcodes is introduced, and its performance is evaluated in comparison to other standard methods of barcode modulation. In this new approach, orthogonal frequency-division multiplexing (OFDM) modulation is used together with differential phase shift keying (DPSK) over adjacent frequency domain elements. A specific aim of this study is to establish a system that is proven tolerant to camera movements, picture blur, and light leakage within neighboring pixels of an LCD.

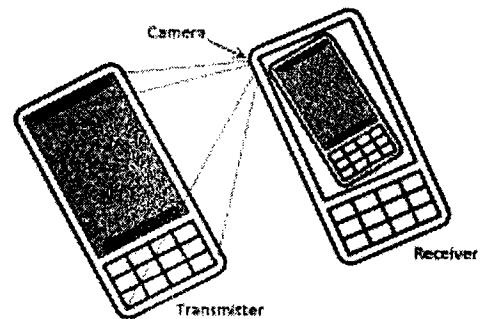
**Keywords:** Barcode, Data Transfer, Differential Phase Shift Keying, Orthogonal Frequency-Division Multiplexing (OFDM) Modulation.

### I. INTRODUCTION

Barcodes have played a great role in facilitating numerous identification processes since their invention in 1952 [1]. In fact barcode is a simple and cost-effective method of storing machine readable digital data on paper or product packages. As pressing needs to transfer even more data faster and with high reliability have emerged, there have been many improvements that were made on the original barcode design. Invention of two dimensional (2D) or matrix barcodes opened a new front for these cost-effective codes and their application in more complex data transfer scenarios like storing contact information, URLs among other things, in which QR codes [2] have become increasingly popular. A comparison of 2D barcode performance in camera phone applications can be found in [3]. Much of the efforts in matrix barcode development have been dedicated to barcodes displayed on a piece of paper as that is the way they are normally used. With the replacement of books with tablets and e-Book readers one could contemplate that replacement of the paper with LCD may open another promising front for broader applications of 2D barcodes as a mean of data transfer. Moreover unlike the static paper, the LCD may display time-varying barcodes for the eventual transfer of streams of data to the receiving electronic device(s) as depicted in Fig1.

This idea has been implemented in [4] where transmission of data between two cell phones through a series of 2D QR codes is studied, achieving bit rates of under 10 kbps for state of the art mobile devices. Later the idea was further

developed in [5] in which a computer monitor and a digital camera are used for transmission and reception with bit rates of more than 14 Mbps achieved in docked transmitter and receiver conditions over distances of up to 4 meters. However, this rate drops to just over 2 Mbps when the distance is increased to 14 meters.



**Fig.1.** An illustration of transmission of data between two handheld cameraphones using a sequence of 2D barcodes.

Furthermore their performance degradation is confined to known portions of the decoded data. This prior knowledge on non-uniform error probability may be used for adaptive error correction coding based on data region as in [5]. There is an increasing interest in design and implementation of LCD-Camera based communication systems as indicated in [6]–[8]. This would require additional investigations in determining optimal modulation and demodulation schemes

## LDPC Decoding for NAND Flash Memory by using Array Dispersion

KARNATI YAMINI<sup>1</sup>, V. NARAYANA REDDY<sup>2</sup>

<sup>1</sup>PG Scholar, Dept of ECE(VLSI Design), PBR Visvadaya Institute of Technology and Science, Kavali, AP, India.

<sup>2</sup>Associate Professor, Dept of ECE, PBR Visvadaya Institute of Technology and Science, Kavali, AP, India.

**Abstract:** The reliability of data stored in an high-density Flash memory devices tends to drop off rapidly because of the reduced cell size and multilevel cell technology. The Soft-decision error correction algorithms make use of multiple-precision sensing for reading memory which can solve this problem. They require a very complex hardware for high-throughput decoding method. In this method, we present a rate-0.97 (68254, 65536) summarized Euclidean geometry low-density parity-check code and its VLSI operation for increased throughput NAND Flash memory system. The aim employ the normalized a posterior probability (APP)-based algorithm, serial schedule, and unrestricted update, which will lead to simple functional unit, halve decoding iterations, and compact power consumption. The pipelined equivalent structural design is adopted for high-throughput decodes, and memory-reduction techniques are employed to minimize the total chip size. The proposed decoder method is implemented in 0.13- $\mu\text{m}$  CMOS tools, and the chip size and power consumption of the decoder are compared with those that of a BCH (Bose-Chaudhuri-Hocquenghem) decoding circuit performance compared with the error-correcting presentation and throughput.

**Keywords:** Channel Coding, Low-Density Parity check (LDPC) Codes, NAND Flash Memory, Sequential Scheduling.

### I. INTRODUCTION

NAND Flash memory is widely used in many mobile devices, such as cellular phones, digital cameras, and smart pads, because of high capacity, fast access speed, and low power consumption. In particular, solid-state drives (SSDs) for notebook computers have become popular as high density NAND Flash memory devices are available. NAND Flash memory stores the information by changing the threshold voltage of floating gate transistors. Most of today's high-density NAND Flash memory devices store multiple (usually two) bits in a cell, and this multilevel cell (MLC) technology significantly increases the bit-error rate (BER). Moreover, the feature size of NAND Flash memory shrinks, the number of electrons in the floating gate of a transistor also decreases, and as a result, the memory is very prone to charge loss caused by long data retention. The cell-to-cell interference (CCI) also increasingly deteriorates the reliability of information stored at the floating gates. It is also well known that SSD applications usually demand high program and-erase cycles, which greatly affects the reliability of NAND Flash memory. NAND Flash memory devices have a spare region at each page, where parity

bits for error correction can be stored. Hard-decision decoding algorithms, such as Hamming and BCH codes, have been widely used for NAND Flash memory error correction. However, as the process technology scales down continuously, more advanced error-correcting codes are needed to keep NAND Flash memory reliable. It is especially important to employ error-correcting algorithms that show good performance with a limited parity data ratio. Soft-decision error correcting methods that sense the threshold voltage of a memory cell in multiple-precision can increase the error-correcting performance because the reliability of stored information can also be utilized.

### II. EXISTING SYSTEM

The parity-check matrix of our proposed LDPC code without masking is shown in Fig. 1. It consists of  $30 \times 300$  submatrices with a submatrix size ( $z$ ) of 63. There are six successive nonzero submatrices in each column block. Due to the second level array dispersion, the locations of nonzero submatrices are downward cyclic shift by one position between each column group. Based on the NMS-VSS decoding algorithm, the parity-check matrix is divided into 300 groups ( $G = 300$ ). In other words, one group is equivalent to one column block. The proposed decoder has one VNU block and six CNU block processing units. At each cycle, the VNU and CNU blocks process the six successive nonzero submatrices in one column block. Let us define  $h_{i,j}$  as the submatrix located at  $i^{\text{th}}$  row block and  $j^{\text{th}}$  column block for  $0 \leq i < 30$  and  $0 \leq j < 300$ .  $B_k$  is denoted as  $k^{\text{th}}$  CNU block processing unit for  $0 \leq k < 6$ , and  $m_i$  is denoted as the messages belong to  $i^{\text{th}}$  row block.

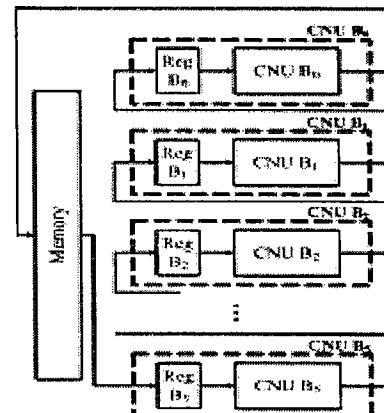


Fig 1. Block diagram of the hybrid storage architecture

**Implementation of Area Efficient Carry-Select Adder****K. RENUKA PRIYADARSHINI<sup>1</sup>, V. NARAYANA REDDY<sup>2</sup>**<sup>1</sup>PG Scholar, Dept of ECE, PBR Visvodaya Institute of Technology And Science, Affiliated to JNTU Anantapur, Kavali, Nellore (Dt), AP, India, E-mail: renukapriyadarshini17@gmail.com.<sup>2</sup>Associate Professor, Dept of ECE, PBR Visvodaya Institute of Technology And Science, Affiliated to JNTU Anantapur, Kavali, Nellore (Dt), AP, India, E-mail: vnr.nlr.kvl@gmail.com.

**Abstract:** In this concise, the reason operations required in standard pass on select snake (CSLA) and twofold to excess 1 converter (BEC)- based CSLA are penniless down to focus the data reliance and to recognize tedious basis operations. We have discarded all the tedious basis operations display in the routine CSLA and proposed another method of reasoning arrangement for CSLA. In the Proposed plot, the pass on select (CS) operation is arranged before the estimation of convincing entire, which is one of a kind in connection to the standard approach. Bit cases of two expecting pass on words (contrasting with  $\text{cin} = 0$  and 1) and settled c in bits are used for basis progression of CS and time units. A viable CSLA setup is gained using enhanced method of reasoning units. The proposed CSLA arrangement incorporates basically less zone and deferment than the starting late proposed BEC-based CSLA. In view of the little pass on yield delay, the proposed CSLA setup is a better than average plausibility for square-root (SQRT) CSLA. A speculative gage exhibits that the proposed SQRT-CSLA incorporates around 35% less area-delay-product (ADP) than the BEC-based SQRT-CSLA, which is best among the current SQRT-CSLA arranges, all things considered, for different piece widths. The application-decided composed circuit (ASIC) union result exhibits that the BEC-based SQRT-CSLA design incorporates 48% more ADP and eats up half more imperativeness than the proposed SQRT-CSLA, all things considered, for different piece widths.

**Keywords:** BEC, CSLA, ASIC, ADP and SQRT.**I. INTRODUCTION**

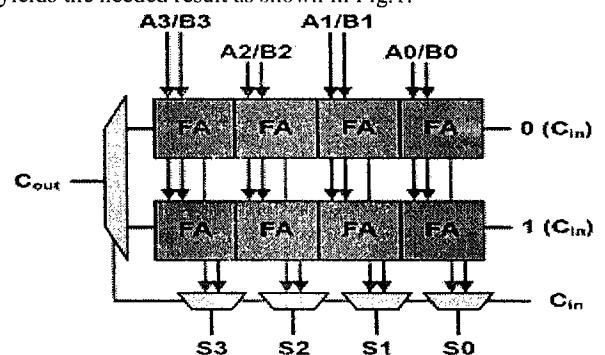
Low-Power, zone capable, and tip top VLSI structures are logically used as a piece of advantageous and PDAs, multi standard remote beneficiaries, and biomedical instrumentation [1], [2]. A snake is the essential part of a calculating unit. A complex propelled hail get ready (DSP) system incorporates a couple of adders. A powerful snake arrangement fundamentally improves the execution of a complex DSP structure. A swell pass on snake (RCA) uses a clear blueprint, however pass on expansion delay (CPD) is the essential stress in this snake. Pass on look-ahead and pass on select (CS) procedures have been proposed to diminish the CPD of adders.

**A. Carry Select Adder (CSA)**

They pass on select snake generally includes two swell pass on adders and a multiplexer. Counting two n-bit numbers with pass on select snake is done with two adders (in this way two swell pass on adders) remembering the ultimate objective to play out the calculation twice, one time with the assumption of they pass on in being zero and the other tolerating it will be one. After the two results are figured, the correct entire, and furthermore the privilege finish, is then picked with the multiplexer once the privilege pass on in is known.

**B. Basic Building Block**

The following is the basic building square of pass on select snake, where the piece size is 4. Two 4-bit swell pass on adders are multiplexed together, where the ensuing pass on and entire bits are picked by pass on in. Since one swell pass on snake acknowledge a pass on in of 0, and interchange expect a pass on in of 1, selecting which wind had the correct supposition by method for the honest to goodness pass on in yields the needed result as shown in Fig.1.

**Fig.1. Building Block.**

A routine pass on select snake (CSLA) is a RCA-RCA outline that delivers two or three total words and yield pass on bits looking at the normal data pass on ( $\text{cin} = 0$  and 1) and

## **Fingerprint Compression Based on Sparse Representation using FFT Method**

**KALLAGUNTA RAJYALAKSHMI<sup>1</sup>, V. PHANI BHUSHAN<sup>2</sup>**

<sup>1</sup>PG Scholar, Dept of ECE, PBR VITS, Kavali, AP, India.

<sup>2</sup>Associate Professor, Dept of ECE, PBR VITS, Kavali, AP, India.

**Abstract:** Recognition of people by means of their biometric features is very popular among the society. There are a variety of biometric techniques including fingerprint recognition, face recognition and eye detection that are used for the privacy and safety purposes in different applications. In current years there has been an increasing interest in the learning of sparse representation of signals. Using an over complete glossary that contains prototype signal-atoms, signals are illustrated by sparse linear combinations of these atoms. Among several biometric recognition technologies, fingerprint compression is very popular for personal identification. One more fingerprint compression algorithm based on sparse representation is introduced. In the algorithm, first we construct a dictionary for predefined fingerprint photocopy patches. For a new given fingerprint images, suggest its patches according to the dictionary by computing 10-minimization by FFT method and then quantize and encode the representation. This paper compares dissimilar Compression standards like JPEG, JPEG-2000, WSQ, K-SVD etc. The experiments demonstrate that this is often cost effective compared with many competitive compression techniques particularly at high compression ratios.

**Keywords:** Discrete Cosine Transform, Peak Signal to Noise Ratio, Fast Fourier Transform.

### **I. INTRODUCTION**

Recognition of persons by means of biometric characteristics is an important technology in the society, because biometric identifiers can't be shared and they intrinsically represent the individual's bodily identity. Among many biometric recognition technologies, fingerprint recognition is very popular for personal identification due to the uniqueness, universality, collectability and invariance [1]. Lossless compression allows the exact original images to be reconstructed from the compressed data. Lossless compression technologies are used in cases where it is important that the original and the decompressed data are identical. Avoiding distortion limits their compression efficiency. When used in image compression where slight distortion is acceptable, lossless compression technologies are often employed in the output coefficients of lossy compression. Lossy compression technologies usually transform an image into another domain, quantize and encode its coefficients. During the last three decades,

transform-based image compression technologies have been extensively researched and some standards have appeared. Two most common options of transformation are the Discrete Cosine Transform (DCT) [2] and the Discrete Wavelet Transform (DWT) [3].

The DCT-based encoder can be thought of as compression of a stream of  $8 \times 8$  small block of images. This transform has been adopted in JPEG [4]. The JPEG compression scheme has many advantages such as simplicity, universality and availability. However, it has a bad performance at low bit-rates mainly because of the underlying block-based DCT scheme. For this reason, as early as 1995, the JPEG-committee began to develop a new wavelet-based compression standard for still images, namely JPEG 2000 [5], [6]. The DWT-based algorithms include three steps: a DWT computation of the normalized image, quantization of the DWT coefficients and lossless coding of the quantized coefficients. The detail can be found in [7] and [8]. Compared with JPEG, JPEG 2000 provides many features that support scalable and interactive access to large-sized image. It also allows extraction of different resolutions, pixel fidelities, regions of interest, components and etc. There are several other DWT-based algorithms, such as Set Partitioning in Hierarchical Trees (SPIHT) Algorithm [9]. These algorithms have a common shortcoming, namely, without the ability of learning. The fingerprint images can't be compressed well now. They will not be compressed well later. In this paper, a novel approach based on sparse representation is given. The proposed method has the ability by updating the dictionary.

The specific process is as follows: construct a base matrix whose columns represent features of the fingerprint images, referring the matrix dictionary whose columns are called atoms; for a given whole fingerprint, divide it into small blocks called patches whose number of pixels are equal to the dimension of the atoms; use the method of sparse representation to obtain the coefficients; then, quantize the coefficients; last, encode the coefficients and other related information using lossless coding methods. In most instances, the evaluation of compression performance of the algorithms is restricted to Peak Signal to Noise Ratio (PSNR) computation. The effects on actual fingerprint matching or recognition are not investigated. In this paper, we will take it into consideration. In most Automatic



ISSN:2320-0790

**COMPUSOFT**

An International Journal of Advanced Computer Technology

## A Critical Research Analysis of Low-Energy Techniques for Instruction Memory Organisations in Embedded Systems

Prof.Dr.G.Manoj Someswar<sup>1</sup>, A.Suman Kumar Reddy<sup>2</sup>

1. Research Supervisor, Dr.APJ Abdul Kalam Technical University, Lucknow, U.P., India
2. Research Scholar, Dr.APJ Abdul Kalam Technical University, Lucknow, U.P., India

**Abstract:** The plan of current implanted frameworks is obliged by the necessities of present day installed applications. A considerable lot of these applications require not just supported operation for drawn out stretches of time, yet additionally to be executed on battery controlled frameworks. Under the imperative of not being mains-associated, the nonappearance of wires to supply a steady wellspring of vitality causes that the utilization of a vitality gathering source or an incorporated vitality provider restrains the operation time of these electronic gadgets. Direction memory associations are called attention to as one of the real wellsprings of vitality utilization in installed frameworks. As these frameworks are portrayed by prohibitive assets and a low-vitality spending plan, any improvement that is presented in the direction memory association permits to diminish the vitality utilization, as well as to have a superior circulation of the vitality spending plan all through the installed framework. This Ph.D. theory concentrates on the examination, investigation, proposition, usage, and assessment of low-vitality streamlining procedures that can be utilized as a part of the guideline memory associations of implanted frameworks. Genuine installed uses of the specific sub-domain of remote sensor hubs are utilized as benchmarks to appear, examine, and authenticate the benefits and disservices of every last one of the ideas in which this Ph.D. proposal depends on. The first key commitment is the efficient investigation of existing low-vitality improvement systems that are utilized as a part of guideline memory associations, delineating their similar points of interest, disadvantages, and exchange o s. Over that, the exploratory assessment that is introduced in this Ph.D. proposition utilizes a precise strategy with a specific end goal to have an exact estimation of parasitic and exchanging movement. Because of this reality, this assessment guides implanted frameworks architects to settle on the right choice in the exchange o s that exist between vitality spending plan, required execution, and region cost of the inserted framework. The second key commitment is the improvement of an abnormal state vitality estimation device that, for a given application and compiler, permits the investigation of building and compiler configurations, as well as of code changes that are identified with the guideline memory association. The third key commitment is the proposition and examination of a few promising usage of vitality efficient direction memory associations for a specific set of utilization codes and installed designs. In view of the past commitments, the work that is exhibited in this Ph.D. proposition demonstrates why additionally upgrading direction memory associations from the vitality utilization perspective will remain a critical pattern later on.

**Keywords:** Energy; Performance; Area; Design Space Exploration; Loop Buffer Architecture; Instruction Memory Organisation; Embedded System

### 1. INTRODUCTION

Never walk on the travelled path because it only leads where others have been. The work that is introduced in this Chapter gives a combination on the low-vitality procedures that are utilized as a part of guideline memory associations, plotting their near preferences, disadvantages, and exchange off. Aside from providing for the peruse a first get a handle on the essential

attributes and outline limitations of different sorts of guideline memory associations, the compositional classification that is introduced in this Chapter has the upside of unmistakably displaying lesser investigated procedures, and subsequently giving clues to future research on the directions memory associations that are utilized as a part of inserted frameworks. Inserted frameworks have different and specific



## A Research Study of Power Impact of Loop Buffer Schemes for Biomedical Wireless Sensor Nodes

Prof.Dr.G.Manoj Someswar<sup>1</sup>, A.Suman Kumar Reddy<sup>2</sup>

1. Research Supervisor, Dr.APJ Abdul Kalam Technical University, Lucknow, U.P., India

2. Research Scholar, Dr.APJ Abdul Kalam Technical University, Lucknow, U.P., India

### Abstract

The plan of current implanted frameworks is obliged by the necessities of present day installed applications. A considerable lot of these applications require not just supported operation for drawn out stretches of time, yet additionally to be executed on battery controlled frameworks. Under the imperative of not being mains-associated, the nonappearance of wires to supply a steady wellspring of vitality causes that the utilization of a vitality gathering source or an incorporated vitality provider restrains the operation time of these electronic gadgets. Direction memory associations are called attention to as one of the real wellsprings of vitality utilization in installed frameworks. As these frameworks are portrayed by prohibitive assets and a low-vitality spending plan, any

improvement that is presented in the direction memory association permits to diminish the vitality utilization, as well as to have a superior circulation of the vitality spending plan all through the installed framework. This Ph.D. theory concentrates on the examination, investigation, proposition, usage, and assessment of low-vitality streamlining procedures that can be utilized as a part of the guideline memory associations of implanted frameworks. Genuine

installed uses of the specific sub-domain of remote sensor hubs are utilized as benchmarks to appear, examine, and authenticate the benefits and disservices of every last one of the ideas in which this Ph.D. proposal depends on.

The first key commitment is the efficient investigation of existing low-vitality improvement systems that are utilized as a part of guideline memory associations, delineating their similar points of interest, disadvantages, and exchange o s. Over that, the exploratory assessment that is introduced in this Ph.D. proposition utilizes a precise strategy with a specific end goal to have an exact estimation of parasitic and exchanging movement. Because of this reality, this assessment guides implanted frameworks architects to settle on the right choice in the exchange o s that exist between vitality spending plan, required execution, and region cost of the inserted framework. The second key commitment is the improvement of an abnormal state vitality estimation device that, for a given application and compiler, permits the investigation of building and compiler configurations, as well as of code changes that are identified with the guideline memory

## Exploration Tool for Instruction Memory Organisations Based On Accurate Cycle-Level Energy Modelling

Prof.Dr.G.Manoj Someswar<sup>1</sup>, A.Suman Kumar Reddy<sup>2</sup>

1. Research Supervisor, Dr.APJ Abdul Kalam Technical University, Lucknow, U.P., India  
2. Research Scholar, Dr.APJ Abdul Kalam Technical University, Lucknow, U.P., India

*Corresponding Author: Prof.Dr.G.Manoj Someswar*

**ABSTRACT:** The plan of current implanted frameworks is obliged by the necessities of present day installed applications. A considerable lot of these applications require not just supported operation for drawn out stretches of time, yet additionally to be executed on battery controlled frameworks. Under the imperative of not being mains-associated, the nonappearance of wires to supply a steady wellspring of vitality causes that the utilization of a vitality gathering source or an incorporated vitality provider restrains the operation time of these electronic gadgets. Direction memory associations are called attention to as one of the real wellsprings of vitality utilization in installed frameworks. As these frameworks are portrayed by prohibitive assets and a low-vitality spending plan, any improvement that is presented in the direction memory association permits to diminish the vitality utilization, as well as to have a superior circulation of the vitality spending plan all through the installed framework. This Ph.D. theory concentrates on the examination, investigation, proposition, usage, and assessment of low-vitality streamlining procedures that can be utilized as a part of the guideline memory associations of implanted frameworks. Genuine installed uses of the specific sub-domain of remote sensor hubs are utilized as benchmarks to appear, examine, and authenticate the benefits and disservices of every last one of the ideas in which this Ph.D. proposal depends on.

**KEYWORDS:** ITRS (International Technology Roadmap for Semiconductors), DMH (Data Memory Hierarchy), IMO (Instruction Memory Organization), LB (Loop Buffer), CELB (Central Loop Buffer Architecture for Single Processor Organization)

Date of Submission: 09-02-2018

Date of acceptance: 24-02-2018

The first key commitment is the efficient investigation of existing low-vitality improvement systems that are utilized as a part of guideline memory associations, delineating their similar points of interest, disadvantages, and exchange o s. Over that, the exploratory assessment that is introduced in this Ph.D. proposition utilizes a precise strategy with a specific end goal to have an exact estimation of parasitic and exchanging movement. Because of this reality, this assessment guides implanted frameworks architects to settle on the right choice in the exchange o s that exist between vitality spending plan, required execution, and region cost of the inserted framework. The second key commitment is the improvement of an abnormal state vitality estimation device that, for a given application and compiler, permits the investigation of building and compiler configurations, as well as of code changes that are identified with the guideline memory association. The third key commitment is the proposition and examination of a few promising usage of vitality efficient direction memory associations for a specific set of utilization codes and installed designs. In view of the past commitments, the work that is exhibited in this Ph.D. proposition demonstrates why additionally upgrading direction memory associations from the vitality utilization perspective will remain a critical pattern later on.  
IMOSIM: Exploration Tool for Instruction Memory Organisations based on Accurate Cycle-Level Energy Modelling

Technology is nothing. What's important is that you have a faith in people, that they're basically good and smart, and if you give them tools, they'll do wonderful things with them. Due to the fact that the design space of the enhancements for reducing the energy consumption of the instruction memory organisation is huge, this Chapter proposes a high-level energy estimation tool that, for a given application and compiler, allows the exploration not only of architectural and compiler configurations, but also of code transformations that are related to the instruction memory organisation. The proposed tool, with a mean error of  $^{3.95}\%$ , achieves reductions in time and effort to explore the design space of the instruction memory organisation.

### Introduction and Related Work

Installed frameworks request different equipment structures to run applications that range from sight and sound shopper gadgets to industry control frameworks. In any case, not at all like broadly useful PC frameworks, implanted frameworks need to give high-computing capacity, unwavering quality, consistency, and meet continuous imperatives with restricted assets, as well as a low-vitality spending plan. The mix of past

## Trace of JPEG Compression and Forgery Detection using Saliency Method(Tentative)

N. KRISHNA CHAITANYA<sup>1</sup>, GOLLAMUDI MEGHANA<sup>2</sup>

<sup>1</sup>Associate Professor, Dept of ECE, PBR Visvadaya Institute of Technology and Science, Kavali, AP, India.

<sup>2</sup>PG Scholar, Dept of ECE, PBR Visvadaya Institute of Technology and Science, Kavali, AP, India.

**Abstract:** To identify whether an image has been JPEG compressed or not is an important issue in forensic practice. The state-of-the-art methods fail to identify high-quality compressed images, which are common on the Internet. In this paper, we provide a novel quantization noise-based solution to reveal the traces of JPEG compression. Based on the analysis of noises in multiple-cycle JPEG compression, we define a quantity called forward quantization noise. We analytically derive that a decompressed JPEG image has a lower variance of forward quantization noise than its uncompressed counterpart. With the conclusion, we develop a simple yet very effective detection algorithm to identify decompressed JPEG images. We show that our method outperforms the state-of-the-art methods by a large margin, especially for high-quality compressed images through extensive experiments on various sources of images. We also demonstrate that the proposed method is robust to small image size and chroma subsampling. The proposed algorithm can be applied in some practical applications, such as Internet image classification and forgery detection.

**Keywords:** JPEG Compression, Discrete Cosine Transform (DCT), Quantization Noise.

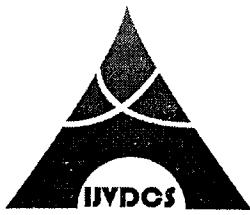
### I. INTRODUCTION

The popularization of imaging components equipped in Personal portable devices, together with the rapid development of the high-speed Internet, makes digital images become an important media for communications. Various types of image compression standards, including lossy and lossless, coexist due to different kinds of requirements on image visual quality, storage, and transmission. Among them, JPEG is a very popular lossy compression format. Knowledge about the JPEG compression history of images from unknown sources is of important interest to image forensics experts, whose aim is to trace the processing history of an image and detect possible forgeries [1], [2]. There are some reported working on identifying whether an image is uncompressed or has been compressed previously [3], [4], whether an image has been compressed once or twice [5], whether an JPEG image has been compressed again with a shifted JPEG grid position [1]–[5], and on estimating the JPEG quantization table [6] or quantization. In this paper, we focus on the problem of identifying whether an image currently in uncompressed form is truly uncompressed or has been previously JPEG

compressed. Being able to identify such a historical record may help to answer some forensics questions related to the originality and the authenticity of an image, such as where is the image coming from, whether it is an original one, or whether any tampering operation has been performed [4]. For example, the solution facilitates the detection of image forgeries created by replacing a part of an image with a fragment from another image with a different compression historical record. The mismatch of historical records reveals the act of image tampering. The JPEG identification problem [3], [4] may also be the starting point for other forensics applications, such as JPEG quantization step estimation [4], for that forensics experts can save time by only performing estimation on the decompressed images after filtering out the uncompressed images. There are also some techniques, called JPEG anti forensics [2], [3], aiming to fool the forensics detectors by concealing the traces of JPEG compression. However, as noted by [4], removing the traces of JPEG compression is not an easy task. Some targeted anti-forensics detectors [5]–[7] are designed to detect the traces left by anti-forensics operations.

### II. EXISTING SYSTEM

Due to the increasing requirements for transmission of images in computer, mobile environments, the research in the field of image compression has increased significantly. Image compression plays a crucial role in digital image processing, it is also very important for efficient transmission and storage of images. When I compute the number of bits per image resulting from typical sampling rates and quantization methods, I find that Image compression is needed. Therefore development of efficient techniques for image compression has become necessary. This project is a survey for lossy image compression using Discrete Cosine Transform, it covers JPEG compression algorithm which is used for full-colour still image applications and describes all the components of it. Fortunately there are several methods available in image compression. They fall into two lossless & lossy compression. The JPEG is widely used for lossy image compression that centres around the discrete cosine transform. The DCT works by separating images into parts of differing frequencies. During a step called quantization where part of compression actually occurs the less important frequencies are discarded, hence the use of lossy. Then only the frequencies that remain are used to retrieve image in the



## **Design of High Speed Variable Latency 64-Bit Carry Skip Adder**

M. PAVITRA<sup>1</sup>, CH. SRAVANI<sup>2</sup>

<sup>1</sup>Associate Professor, Dept of ECE, PBR Visvadaya Institute of Technology & Science, Kavali, AP, India.

<sup>2</sup>PG Scholar, Dept of ECE(VLSI), PBR Visvadaya Institute of Technology & Science, Kavali, AP, India.

**Abstract:** In this paper, we present a carry skip adder (CSKA) structure that has a higher speed yet lower energy consumption compared with the conventional one. The speed enhancement is achieved by applying concatenation and incrimination schemes to improve the efficiency of the conventional CSKA (Conv-CSKA) structure. In addition, instead of utilizing multiplexer logic, the proposed structure makes use of AND-OR-Invert (AOI) and OR-AND-Invert (OAI) compound gates for the skip logic. The structure may be realized with both fixed stage size and variable stage size styles, wherein the latter further improves the speed and energy parameters of the adder. Finally, a hybrid variable latency 64 Bit Carry Skip Adder improves the speed.

**Keywords:** Carry Skip Adder (CSKA), Energy Efficient, High-Performance, Hybrid Variable Latency Adders, Voltage Scaling.

### **I. INTRODUCTION**

Adders are a key building block in arithmetic and logic units (ALUs) [1] and hence increasing their speed and reducing their power/energy consumption strongly affect the speed and power consumption of processors. There are many works on the subject of optimizing the speed and power of these units, which have been reported in [2]–[9]. Obviously, it is highly desirable to achieve higher speeds at low-power/energy consumptions, which is a challenge for the designers of general purpose processors. One of the effective techniques to lower the power consumption of digital circuits is to reduce the supply voltage due to quadratic dependence of the switching energy on the voltage. Moreover, the sub threshold current, which is the main leakage component in OFF devices, has an exponential dependence on the supply voltage level through the drain-induced barrier lowering effect [10]. Depending on the amount of the supply voltage reduction, the operation of ON devices may reside in the super threshold, near-threshold, or sub threshold regions. Working in the super threshold region provides us with lower delay and higher switching and leakage powers compared with the near/sub threshold regions. In the sub threshold region, the logic gate delay and leakage power exhibit exponential dependences on the supply and threshold voltages. Moreover, these voltages are (potentially) subject to process and environmental variations in the nanoscale technologies. The variations increase uncertainties in the aforesaid performance parameters. In addition, the small sub threshold current causes a large delay for the circuits operating in the subthreshold region [10].

Recently, the near-threshold region has been considered as a region that provides a more desirable tradeoff point between delay and power dissipation compared with that of the subthreshold one, because it results in lower delay

compared with the subthreshold region and significantly lowers switching and leakage powers compared with the superthreshold region. In addition, near-threshold operation, which uses supply voltage levels near the threshold voltage of transistors [11], suffers considerably less from the process and environmental variations compared with the subthreshold region. The dependence of the power (and performance) on the supply voltage has been the motivation for design of circuits with the feature of dynamic voltage and frequency scaling. In these circuits, to reduce the energy consumption, the system may change the voltage (and frequency) of the circuit based on the workload requirement [2]. For these systems, the circuit should be able to operate under a wide range of supply voltage levels. Of course, achieving higher speeds at lower supply voltages for the computational blocks, with the adders as one of the main components, could be crucial in the design of high-speed, yet energy efficient, processors. In addition to the knob of the supply voltage, one may choose between different adder structures/families for optimizing power and speed. There are many adder families with different delays, power consumptions, and area usages. Examples include ripple carry adder (RCA), carry increment adder (CIA), carry skip adder (CSKA), carry select adder (CSLA), and parallel prefix adders (PPAs).

The descriptions of each of these adder architectures along with their characteristics may be found in [1] and [3]. The RCA has the simplest structure with the smallest area and power consumption but with the worst critical path delay. In the CSA, the speed, power consumption, and area usages are considerably larger than those of the RCA. The PPAs, which are also called carry look-ahead adders, exploit direct parallel prefix structures to generate the carry as fast as possible [4]. There are different types of the parallel



## Design of Redundant Binary Multipliers using Modified Partial Product Generator

<sup>1</sup>P.Harikrishna.  
M.Tech.

<sup>2</sup>Mrs.M.Pavitra  
Associate Professor.

<sup>1,2</sup> Dept of ECE (VLSID).  
<sup>1,2</sup> PBR VITS College of Engineering, Kavali, Andhra Pradesh

**Abstract:** Multiplication is one of the basic functions used in digital signal processing (DSP). Due to its high modularity and carry-free addition, a redundant binary (RB) representation can be used when designing high performance multipliers. The conventional RB multiplier requires an additional RB partial product (RBPP) row, because an error-correcting word (ECW) is generated by both the radix-4 Modified Booth encoding (MBE) and the RB encoding.

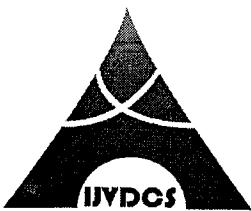
This incurs in an additional RBPP accumulation stage for the MBE multiplier. In this paper, a new RB modified partial product generator (RBMPPG) is proposed; it removes the extra ECW and hence, it saves one RBPP accumulation stage. Therefore, the proposed RBMPPG generates fewer partial product rows than a conventional RB MBE multiplier. Simulation results show that the proposed RBMPPG based designs significantly improve the area and High speed when the word length of each operand in the multiplier is at least 32 bits; these reductions over previous NB multiplier designs incur in

a modest delay increase. The delay can be reduced using the proposed RB multipliers when compared with existing RB multipliers.

**Index Terms-** Redundant binary modified booth encoding, RB partial product generator, RB multiplier.

### 1 INTRODUCTION

Digital multipliers are widely used in arithmetic units of microprocessors, multimedia and digital signal processors. Many algorithms and architectures have been proposed to design high-speed and low-power multipliers. A normal binary (NB) multiplication by digital circuits includes three steps. In the first step, partial products are generated; in the second step, all partial products are added by a partial product reduction tree until two partial product rows remain. In the third step, the two partial product rows are added by a fast carry propagation adder. Two methods have been used to perform the second step for the partial product reduction. A first method uses four-two compressors, while a second method uses redundant binary (RB) numbers. Both methods allow the partial product reduction tree to be reduced at a rate of 2:1.



www.ijvdcs.org

# International Journal of VLSI System Design and Communication Systems

ISSN 2322-0929  
Vol.05, Issue.09,  
September-2017,  
Pages:0920-0923

## Implementation of Conventional Multiplier in Reversible Logic

B. SRILAKSHMI<sup>1</sup>, KASA RAJESH<sup>2</sup>

<sup>1</sup>PG Scholar, Dept of ECE, PBR VITS, Kavali, AP, India.

<sup>2</sup>Assistant Professor, Dept of ECE, PBR VITS, Kavali, AP, India.

**Abstract:** Reversible logic attains the attraction of researchers in the last decade mainly due to low-power dissipation. Designers' endeavours are thus continuing in creating complete reversible circuits consisting of reversible gates. Reversible gates offer a considerable reduction in energy compared to conventional gates. This paper presents a design methodology for the realization of Booth's multiplier in reversible mode. As FPGA is having limited number of multipliers and which consumes large area and time consuming. As number of bits in the multiplicand or multiplier increases, delay increases due to the number of additions. Booth's multiplier is considered as one of the fastest multipliers in literature and we have shown an efficient design methodology in reversible paradigm. The proposed architecture is capable of performing both signed and unsigned multiplication of two operands without having any feedbacks, whereas existing multipliers in reversible mode consider loop which is strictly prohibited in reversible logic design. Theoretical underpinnings, established for the proposed design, show that the proposed circuit is very efficient from reversible circuit design point of view. The design proposed here shows a considerable reduction in delay thereby the frequency of design will be improved.

**Keywords:** Booth's Multiplier, Garbage Output, Low Power Design, Quantum Cost.

### I. INTRODUCTION

The field of reversible logic is achieving a growing interest by its possibility in quantum computing, low-power CMOS, nanotechnology, and optical computing. It is now widely accepted that the CMOS technology implementing irreversible logic will hit a scaling limit beyond 2016, and thus the increased power dissipation is a major limiting factor. Landauer's principle states that, logic computations that are not reversible generate heat  $kT\ln 2$  for every bits of information that is lost. According to Frank , computers based on reversible logic operations can reuse a fraction of signal energy that theoretically can approach arbitrarily near 100%. An n-input n-output function (gate) is called reversible if and only if it maps each input instance to a unique output instance. The only possible structure for a reversible network is the cascade of reversible gates. In practice, not all of the  $n!$  possible reversible functions can be realized as a single reversible gate. Several reversible gates have been proposed in literature so far, where the synthesis of reversible circuits differs significantly from synthesis in traditional irreversible circuits. Two restrictions are added for reversible networks, namely fan-outs and back-feeds. The aim of the paper is to design a Booth's multiplier in reversible mode which is capable of working with both signed and unsigned numbers and to reduce the delay thereby increasing the Frequency.

### II. EXISTING SYSTEM

#### A. Booth Multiplication Algorithm for radix 2

Booth algorithm gives a procedure for multiplying binary integers in signed -2's complement representation.

#### Step 1: Making the Booth table

- From the two numbers, pick the number with the smallest difference between a series of consecutive numbers, and make it a multiplier. i.e., 0010 -- From 0 to 0 no change, 0 to 1 one change, 1 to 0 another change ,so there are two changes on this one 1100 -- From 1 to 1 no change, 1 to 0 one change, 0 to 0 no change, so there is only one change on this one. Therefore, multiplication of  $2 \times (-4)$ , where 2 ten (0010 two ) is the multiplicand and (-4) ten (1100 two ) is the multiplier.
- Let X = 1100 (multiplier) Let Y = 0010 (multiplicand)  
Take the 2's complement of Y and call it  $-Y -Y = 1110$
- III. Load the X value in the table.
- IV. Load 0 for X-1 value it should be the previous first least significant bit of X
- V. Load 0 in U and V rows which will have the product of X and Y at the end of operation.
- VI. Make four rows for each cycle; this is because we are multiplying four bits numbers.

#### Step 2: Booth Algorithm

Booth algorithm requires examination of the multiplier bits, and shifting of the partial product. Prior to the shifting, the multiplicand may be added to partial product, subtracted from the partial product, or left unchanged according to the following rules: Look at the first least significant bits of the multiplier "X", and the previous least significant bits of the multiplier "X - 1". I 0 0 Shift only 1 1 Shift only. 0 1 Add Y to U, and shift 1 0 Subtract Y from U, and shift or add (-Y) to U and shift II Take U & V together and shift arithmetic right

## Facial Feature Identification and Matching using Face Sketch Synthesis by Modified Sparse Technique

KASA RAJESH<sup>1</sup>, P. KAVYA SRI<sup>2</sup>

<sup>1</sup>Assistant Professor, Dept of ECE, PBR Visvadaya Institute of Technology And Science, Kavali, AP, India.

<sup>2</sup>PG Scholar, Dept of ECE, PBR Visvadaya Institute of Technology And Science, Kavali, AP, India.

**Abstract:** Face sketch synthesis has wide applications in digital entertainment and law enforcement. Although there is much research on face sketch synthesis, most existing algorithms cannot handle some nonfacial factors, such as hair style, hairpins, and glasses if these factors are excluded in the training set. In addition, previous methods only work on well controlled conditions and fail on images with different backgrounds and sizes as the training set. To this end, this project presents a novel method that combines both the similarity between different image patches and prior knowledge to synthesize face sketches. Given training photo-sketch pairs, the proposed method learns a photo patch feature dictionary from the training photo patches and replaces the photo patches with their sparse coefficients during the searching process. For a test photo patch, by obtaining its sparse coefficient via the learnt dictionary and then search its nearest neighbors (candidate patches) in the whole training photo patches with sparse coefficients. After purifying the nearest neighbors with prior knowledge, the final sketch corresponding to the test photo can be obtained by Bayesian inference. The contributions of this project are as follows: 1) Relaxing the nearest neighbor search area from local region to the whole image without too much time consuming and 2) This method can produce non-facial factors that are not contained in the training set and is robust against image backgrounds and can even ignore the alignment and image size aspects of test photos. This experimental results show that the proposed method outperforms several state of-the-arts in terms of perceptual and objective metrics.

**Keywords:** Face Sketch Synthesis, Sparse Matrix, Markov Random Fields.

### I. INTRODUCTION

Face sketch is useful in applications such as face recognition and digital entertainment. Compared with face photos, face sketches have the following advantages.

- In many cases, especially in law enforcement, when the face photo of a suspect is not available, photo based face recognition methods cannot be used. An artist's drawing based on the depiction of the witness is needed.
- Face sketches are more concisely and discriminatively than face photos. Usually, artists can capture the most distinctive characteristics of human faces by observation

and human being can recognize their depictions very well. In face sketch-based applications, sketch synthesis is usually used to construct the sketch database. In the last decade, several studies have been conducted on sketch synthesis. They developed an eigen transform based algorithm, in which the transformation between photos and sketches is assumed to be linear.

In this project, a face sketch synthesis method with sparse representation is proposed. Given a test face photo, initially obtain its corresponding sketch image by solving an  $\ell_1$ - norm minimization problem with Lasso. Firstly, the training photos and sketches are divided into overlapped regions. Since the used face photo and sketch images have been aligned that the same face components in different images roughly at the same region, photo and sketch patch pairs within the corresponding photo and sketch regions are used to built a coupled dictionary with much succinct elements using sparse coding. Secondly, for each image patch in the test photo, one can compute its sparse representation coefficient with respect to the photo elements in coupled dictionary. The sketch patch can be recovered with the same coefficient and the sketch elements in coupled dictionary. Finally, the face sketch can be constructed with the obtained sketch patches. Compared with previous approaches, our method has advantages in three aspects. Firstly, the computed sparse representation adaptively selects the most relevant patches which give best representations to the test face image. It can avoid the parameter selection of traditional neighbor-based methods. Secondly, former methods require dictionaries containing all the sampling image patches from the training set, while our method requires a much smaller dictionary using sparse coding; Thirdly, instead of adopting a global dictionary for training, our method is performed on local dictionaries over small regions, which makes good use of the alignment of face and sketch images. The sketch synthesis with local dictionaries is efficient and effective both theoretically and numerically. Experiment results on public data set show the superiority of our method.

### A. Existing System

Existing methods about face sketch synthesis could be sorted into three categories: the subspace learning

## Non-Uniform Templates for Near Duplicate Image Matching

D. VIJAYA KUMAR<sup>1</sup>, K. RAJESH<sup>2</sup>

<sup>1</sup>PG Scholar, Dept of ECE, PBR Visvodaya Institute of Technology & Science, Kavali, Nellore (Dt), AP, India.

<sup>2</sup>Assistant Professor, Dept of ECE, PBR Visvodaya Institute of Technology & Science, Kavali, Nellore (Dt), AP, India.

**Abstract:** We propose a variable-length signature for close duplicate image coordinating in this paper. An image is represented by a signature, the length of which differs concerning the quantity of patches in the image. Another visual descriptor, viz., probabilistic focus symmetric nearby paired example, is proposed to portray the presence of each image fix. Past every individual fix, the spatial connections among the patches are caught. With a specific end goal to register the likeness between two images, we use the earth mover's separation which is great at dealing with variable-length signatures. The proposed image signature is assessed in two unique applications, i.e., close duplicate record image recovery and close duplicate common image discovery. The promising trial comes about exhibit the legitimacy and adequacy of the proposed variable-length signature.

**Keywords:** Variable-Length Image Signature, Near-Duplicate Image Detection, Near-Duplicate Image Retrieval.

### I. INTRODUCTION

Close duplicate images are produced by taking independent photographs of a similar protest under various conditions in enlightenments, resolutions, et cetera. Moreover, they can be made by changing the first images utilizing a few changes, e.g. image turn and scaling. Recognizing close duplicate images assumes an imperative part in numerous applications, for example, postal computerization, copyright security, and so forth. Two key issues are engaged with image coordinating: image portrayal and image likeness estimation. Image portrayal specifies how a machine "sees" an image. It is vital since a capable image portrayal can facilitate the coordinating procedure. Additionally, unique image representations involve diverse comparability measures. We first give a short survey on the image portrayals and likeness measures received in the writing.

### A. Literature Review

The basic practice is to first venture images to some component spaces and after that speak to them as vectors, in view of which the closeness between two images can be computed by a great deal of scientific apparatuses, e.g. Euclidean separation. Kim utilized the ordinal measures of the discrete cosine change coefficients to speak to an image. At that point the L1 standard was used for image likeness calculation. In Liu and Yang assembled a shading

distinction histogram for an image, which encoded the shading and edge introductions of the image in a uniform structure. Consequently, the closeness of two images was figured as far as the upgraded Canberra separate. Aksoy and Haralick proposed line-point proportion measurements and co-event fluctuations to speak to an image which was sorted out into an element vector of 28 measurements. At that point diverse similitude measures were looked at in the image recovery situation. As per their tests, it was smarter to consider the element dispersions in planning likeness measures. In Meng et al. first spoke to an image by a 279D component vector. For likeness computation, the upgraded Dynamic Partial Function was proposed which adaptively initiated an alternate number of highlights in a pair wise way to suit the attributes of each image match. Mate et al. spoke to an image in view of its shading histograms and after that utilized Locality Sensitive Hashing (LSH) for quick recovery. For computational efficiency, the vectorial portrayals were first implanted into paired codes in a few works. In this unique situation, a key issue was to guarantee that the images that were comparative in the first vector space ought to be reduced in the paired code space. At that point the image closeness can be efficiently ascertained by the Hamming separation between the double codes.

In spite of the straightforwardness, speaking to an image by a solitary vector for the most part neglects to adapt to the varieties among the close duplicate images as exhibited. In addition, the measurement of the highlights must be resolved from the earlier, paying little mind to the image's attributes. What's more, the vectors are bad at displaying the connections among a few sections of the image. To handle the issue, some effective information structures past vectors were utilized for image portrayal, for example, diagrams or trees. Zhang and Chang used the credited social chart to speak to an image, which changed the image closeness calculation issue into diagram coordinating. To dorovic and Ahuja spoke to an image by a tree of recursively implanted image locales. To defeat imaging clamor, the tree was increased with new hubs created by blending nearby kin hubs, delivering coordinated non-cyclic charts (DAGs) thusly. Transitive terminations of the DAGs were then developed, planning the tree coordinating issue as finding a bijection between the two transitive terminations. As a rule, more discriminative image portrayals can be rendered utilizing charts or trees.

## Efficient Approaches for Designing Quantum Costs of Various Reversible Gates

M. Surekha

*Assistant professor, Department of ECE  
Visvodaya Engineering College, Kavali, India.*

### Abstract

Over the last few decades, research in reversible logic has increasingly become very popular and it is gaining greater momentum in the present word. Reversible logic has started finding concert applications in quantum computing, optical computing, nano-technology based system, low-power CMOS design, VLSI design. The principal objective of this work is to argue for quantum implementation of various reversible logic gates by using C-NOT, Controlled-V and Controlled-V<sup>+</sup> gates. The present work presents parallel adder/subtractor (with over flow detection), as well as Binary coded decimal adder (BCD) in terms of number of gates, garbage outputs, quantum cost, delay and hardware complexity compared to existing design.

**Keywords:** Parallel adder/subtractor, Quantum cost, Reversible logic, and Reversible BCD adder.

### INTRODUCTION

The process of moving forward in high-level integration and fabrication process has emerged in superior logic circuits and energy loss has also been significantly reduced over the last decades. This inclination of decrease of heat in computation as well has its physical limit are achieved. According to Landauer [1, 2], in logic computation all bits of information loss generates  $KT\ln 2$  joules of heat energy where K is Boltzmann's constants of  $1.38 \times 10^{-23} \text{ J/K}$  and T is absolute temperature of the environment. At room temperature, the dissipating heat is around  $2.9 \times 10^{-21} \text{ J}$ . Energy loss due to Landauer limit is also important as it is probable that the increase of heat production causing information loss will be perceptible in future.

# Design of Area Efficient High-Performance 2-4 and 4-16 Mixed-Logic Line Decoders

G. KIRAN<sup>1</sup>

kiran17793@gmail.com<sup>1</sup>

<sup>1</sup>PG Scholar, VLSI, PBR Visvodaya Institute of Technology and Science, Kavali, Nellore, Andhra Pradesh.

LML.NARAYANA REDDY<sup>2</sup>

narayananareddy.lml@gmail.com<sup>2</sup>

<sup>2</sup>Associate Professor, Dept of ECE, PBR Visvodaya Institute of Technology and Science, Kavali, Nellore, Andhra Pradesh.

**Abstract:** This project involves a mixed-logic design method for line decoders, combining transmission gate logic, pass transistor dual-value logic and static CMOS. Two novel topologies are presented for the 2-4 decoders: a 14-transistor topology aiming on minimizing transistor count and power dissipation and a 15-transistor topology aiming on high power delay performance. Both a normal and an inverting decoder are implemented in each case, yielding a total of four new designs. Furthermore, four new 4-16 decoders are designed, by using mixed-logic 2-4 pre-decoders combined with standard CMOS post-decoder. All proposed decoders have full swinging capability and reduced transistor count compared to their conventional CMOS counterparts. Finally, a variety of comparative spice simulations at the 32 nm shows that the proposed circuits present a significant improvement in power and delay, outperforming CMOS in almost all cases.

**Index Terms**—line decoder, mixed logic, pass transistor logic, transmission gate logic.

## I. INTRODUCTION

The concept of digital data manipulation changes the society in attractive way even all the electronic gadgets are in digital formats. Due to invention of various digital IC technologies we are in VLSI era. These digital technologies have their own advantages and disadvantages. Due to invention of Bipolar Junction Technology (BJT) the first IC had been implemented that is TTL (Transistor- Transistor Logic). TTL logic provides higher packing density but slow turn off process. A new technology had been developed called ECL (emitter coupled logic) which is fastest logic but provides higher power dissipation. But

unfortunately, in VLSI era, BJT is defeated by MOS technology. MOS provides lower power dissipation and high packing density than BJT. But again CMOS beat the MOS technology as it provides excellent static characteristics like lowest static power dissipation and highest Noise margin. But the problem with the CMOS ICs is their dynamic power dissipation and digital switching noise.

This problem is solved if we use differential amplifier. Because these amplifiers are not only less sensitive to noise but also enable us to bias amplifier and couple the amplifier stage together without the requirement for bypass and coupling capacitor. This born various technologies like SCL (source coupled logic), FSCL (folded Source Coupled Logic), MCML (MOS current Mode Logic). Static CMOS logic provides several advantages in designing digital circuit, that are low sensitivity to noise, good performance, low power consumption, etc. But it show some disadvantages while designing mixed mode ICs. In VLSI circuit, several logic gates switches simultaneously and resulting current causes switching noise. The mixed mode IC has both analog and digital circuit on single semiconductor die so this noise affect analog circuit through substrate coupling. This reduces speed and accuracy of mixed mode ICs. Various methods are used to reduce this noise in mixed mode ICs like separate analog and digital supply line, diffuse guard band, bonding pads etc. Source coupled logic(SCL) was developed to reduce this digital switching noise and it is most successful methods among all the constant current source technique.

Now a day's power reduction is a major issue in the technology world. The low power design is major issue in high performance digital system, such as microprocessors, digital signal processors (DSPs) and

## **Transferring the Health Details of Animal using Zigbee Module**

**POLEPALLI NAGA LAKSHMI<sup>1</sup>, K. ASHOK KUMAR<sup>2</sup>**

<sup>1</sup>PG Scholar, Dept of ECE, PBR VITS, Kavali, AP, India.

<sup>2</sup>Assistant Professor, Dept of ECE, PBR VITS, Kavali, AP, India.

**Abstract:** In this paper present an animal health monitoring system (AHMS) for monitoring the physiological parameters such as rumination, body temperature, and heart rate with surrounding temperature and humidity has been developed. The developed system can also be analyzing the stress level corresponding to thermal humidity index (THI). The ZIGBEE device and Microcontroller are used in the implementation of sensor module. It controls every component of the system. The LCD monitor displays the if the animal has been detected. The device is very helpful of inexpensive health care of livestock. A prototype model is developed and tested with high accuracy results.

**Keywords:** Sensors, Animal Health Monitoring, Animal Disease.

### **I. INTRODUCTION**

The present patient screen frameworks in doctor's facilities permit ceaseless observing of patient fundamental signs, which require the sensors to be hardwired to adjacent, bedside screens or PCs, and basically bind the patient to his clinic bed. Indeed, even subsequent to associating these frameworks to a specific patient, a paramedical right hand need to constantly screen and note down all the crucial parameters of a given patient by monitoring the majority of his/her records physically. Receiving such a technique is blunder inclined and may prompt debacle on account of a human mistake. In the current proposed framework the patient wellbeing is persistently checked by the Mobile multi tolerant observing framework and the obtained information is transmitted to a brought together ARM server utilizing Wireless Sensor Networks. A ZigBee hub is associated with each patient screen framework that expends low power and is to a great degree little in measure. These are particularly intended for low power utilization, with insignificant circuit segments expected for little bundle, long separation go applications and ordinarily comprise of a low power processor with negligible assets and interface capacities. They additionally have a preservationist handset that is equipped for transmitting 8 bytes of information at once and has a direct transmitting scope of around 130 m. Hence, WPANs appear to be an ideal fit for remote patient observing. To enhance the precision and to expand the proficiency of the above procedures a continuous patient observing framework in light of Wireless Sensor Networks (utilizing IEEE 802.15a) and a unified ARM Server incorporated with GSM module is composed. This paper portrays a free framework that consequently logs essential parameters of patients for simple get to. The information is open to specialists through cell phone for accommodation if necessary.

### **II. INTRODUCTION ON ZIGBEE**

ZigBee is an IEEE 802.15.4 standard for data communications with business and consumer devices [2]. It is designed around low-power consumption batteries with long battery life which last forever. The ZigBee standard provides network, security, and application support services operating which works on top of the IEEE 802.15.4 Medium Access Control (MAC) and Physical Layer (PHY) wireless standard. It works a set of technologies to enable scalable, self-organizing, self-healing networks that can manage various data traffic patterns. ZigBee is a low-cost, low-power, wireless mesh networking standard. The low cost allows the technology to be widely deployed in wireless control and monitoring applications, the low power-usage allows longer life with smaller batteries, and the mesh networking provides high reliability and larger range.

### **III. HARDWARE AND SOFTWARE DESCRIPTION**

Hardware specification gives a specification of hardware details used to implement in the system.

#### **A. PIC16F877A**

This powerful (200 nanosecond instruction execution) which easy-to-program CMOS FLASH-based 8-bit microcontroller is heart of system, which packs Microchip's powerful PIC architecture into an 40- or 44-pin package and is upwards compatible with the PIC16C5X, PIC12CXXX and PIC16C7X devices. The PIC16F877A features include 256 bytes of EEPROM data memory, self-programming, an ICD, 2 Comparators, 8 channels of 10-bit Analog-to-Digital (A/D) converter, two capture/compare/PWM functions, the synchronous serial port can be configured as either 3-wire. The other parts are Serial Peripheral Interface (SPI™) or the 2-wire Inter-Integrated Circuit (I<sup>2</sup>C™) bus and a Universal Asynchronous Receiver Transmitter (USART). All of these

## **An Approach to Control and Monitor Environmental Parameters in Greenhouse using ARM**

**B. SREELEKHA<sup>1</sup>, K. ASHOK KUMAR<sup>2</sup>**

<sup>1</sup>PG Scholar, Dept of ECE, PBR VITS, Kavali, AP, India.

<sup>2</sup>Assistant Professor, Dept of ECE, PBR VITS, Kavali, AP, India.

**Abstract:** The work is implemented for remote monitoring and control of greenhouse parameters with the help of sensors and GSM communication. It overcomes the disadvantages of wired and wireless constraints such as complicated wiring, difficult maintenance and distance, to monitor and control the applications. The application will have embedded system which consists of ARM7 microcontroller, real time operating system, sensors, GSM modem and control devices to monitor the environmental parameters condition namely temperature, humidity, CO<sub>2</sub> concentration and light intensity in greenhouse.. By this, environmental parameters in greenhouse can be monitored and controlled remotely and the user can be able to know the status of the greenhouse using IOT server. The hardware and software modules of the application system are discussed in detail. This embedded application is implemented and tested for its correct functionality. The experimental results show that the developed monitoring system has the following features, such as simple structure, high reliability, good extensibility and flexible configuration. It will control automatically the environmental parameters in every greenhouse and has project practicality and vendibility.

**Keywords:** Greenhouse, GSM, ARM7, Temperature, Humidity, Light intensity, CO<sub>2</sub>, PIR.

### **I. INTRODUCTION**

A greenhouse is a building in which plants are grown. These structures range in size from small sheds to very large buildings. For the large rural distract, the greenhouse production has become a way of being rich. The growth of crop in greenhouse depends on temperature, CO<sub>2</sub>, humidity, light intensity and other parameters in greenhouse. So it is important to real-time and properly measure and adjust the temperature, CO<sub>2</sub>, humidity, light intensity and other parameters in the greenhouse. With the continued expansion of production scale, the disadvantages of traditional wire monitoring system are more and more prominent, such as complicated arrangement, difficult maintenance and so on. Then the Remote monitoring system is developed, which based on wireless communication technology, does not need cables, adds or reduces configuration at random, possess simple system construction. Moreover, it is characterized by

its low power consumption. Therefore, it proves to be simple and of practical significance.

### **A. Back Ground**

In greenhouse more number of the parameters is to be control because, the varieties of the crops are large. They are increasing day by day because of the development in agriculture technology. The automation is possible with simple hardware by using microcontroller where only the controlling is possible but user (farmer) will not get information about the greenhouse. On progress towards the improvement to monitor and control, an attempt was made using wireless technology. There are many technologies can be used for wireless application. It was tried to adopt the wireless communication like Infrared, Bluetooth, Zigbee and RF technology. But the attempt has failed because of technology constraints. In this situation, the wireless sensor network with additional hardware and software is a solution for greenhouse control. If parameters still increase, then for WSN technology bandwidth may not be sufficient [1]. A Control System of Environment Parameters of Greenhouse based on CAN Bus is existing and requires wired system. The Wireless Measurement and Control System for Environmental Parameters in Greenhouse [3], overcomes the disadvantages of wired monitoring system, such as as complicated wiring & difficult maintenance. This project is designed to overcome the above mentioned disadvantages, using which the environmental parameters in every greenhouse can be measured and controlled by microcontroller remotely. The Parameters settings can be made in two modes i.e. by using push button keys or by GSM communication mode remotely. A user can know the greenhouse status by connecting to the IOT server which will get updated for every 30 seconds.

### **II. OVERVIEW**

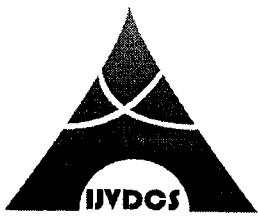
The Fig1 shows the block diagram of ARM based Monitoring and Control system architecture. It contains two modules, namely monitoring unit and controlling unit.

Where T u: Upper Threshold Temperature

T L: Lower Threshold Temperature

Hu: Upper Threshold Humidity

HL: Lower Threshold Humidity



## **Design And Implementation of FM0/Manchester Encoder Using Sols Technique**

**D. PRASANNA KUMAR<sup>1</sup>, K. ASHOK KUMAR<sup>2</sup>**

<sup>1</sup>PG Scholar, Dept of ECE, PBR Visvodaya Institute of Technology & Science, Kavali, SPSR Nellore(Dt), AP, India.

<sup>2</sup>Assistant Professor, Dept of ECE, PBR Visvodaya Institute of Technology & Science, Kavali, SPSR Nellore(Dt), AP, India.

**Abstract:** The dedicated short-range communication (DSRC) is a developing procedure to drive the canny transportation framework into our every day life. The DSRC models for the most part embrace FM0 and Manchester codes to achieve dc-adjust, enhancing the flag dependability. In any case, the coding-decent variety between the FM0 and Manchester codes genuinely constrains the possibility to plan a completely reused VLSI design for both. In this paper, the likeness situated rationale rearrangements (SOLS) method is proposed to beat this restriction. The SOLS system enhances the equipment usage rate from 57.14% to 100% for both FM0 and Manchester encodings.

**Keywords:** Dedicated Short-Range Communication (DSRC), FM0, Manchester, VLSI.

### I. INTRODUCTION

The dedicated short-range communication (DSRC) [1] is a convention for maybe a couple way medium range communication particularly for shrewd transportation frameworks. The DSRC can be quickly arranged into two classes: vehicle to-car and car to-roadside. In vehicle to-car, the DSRC empowers the message sending and broadcasting among cars for security issues and open data declaration [2], [3]. The security issues incorporate blind side, crossing point cautioning, entomb autos separation, and crash alert. The DSRC principles have been built up by a few associations in various nations. These DSRC gauges of America, Europe, and Japan are appeared in Table I. The information rate independently focuses at 500 kb/s, 4 Mb/s, and 27 Mb/s with bearer recurrence of 5.8 and 5.9 GHz. The modulation strategies fuse amplitude shift keying, phase shift keying, and orthogonal recurrence division multiplexing. For the most part, the waveform of transmitted flag is required to have zero mean for heartiness issue, and this is additionally alluded to as dc-adjust. The transmitted flag comprises of subjective parallel succession, which is hard to acquire dc-adjust. The reasons for FM0 and Manchester codes can give the transmitted flag dc-adjust. Both FM0 and Manchester codes are broadly received in encoding for downlink. The VLSI models of FM0 and Manchester encoders are investigated as takes after.

### II. CODING PRINCIPLES OF FM0 CODE AND MANCHESTER CODE

In the following discussion, the clock signal and the input data are abbreviated as CLK, and X, respectively. With the above parameters, the coding principles of FM0 and Manchester codes are discussed as follows.

#### A. FM0 Encoding

As appeared in Fig2, for every X, the FM0 code comprises of two sections: one for previous half cycle of CLK, An, and the other one for some other time half cycle of CLK, B. The coding rule of FM0 is recorded as the accompanying three principles.

- If X is the rationale 0, the FM0 code must display a change amongst An and B.
- If X is the rationale 1, no progress is permitted amongst An and B.
- The progress is designated among each FM0 code regardless of what the X is.

A FM0 coding case is appeared in Fig3. At cycle 1, the X is rationale 0; hence, a change happens on its FM0 code, as indicated by manage 1. For straightforwardness, this change is at first set from rationale 0 to -1. As indicated by manage 3, a progress is distributed among each FM0 code, and in this manner the rationale 1 is changed to rationale 0 in the start of cycle 2. At that point, as per govern 2, this rationale level is hold with no change in whole cycle 2 for the X of rationale 1. In this manner, the FM0 code of each cycle can be inferred with these three guidelines said before.

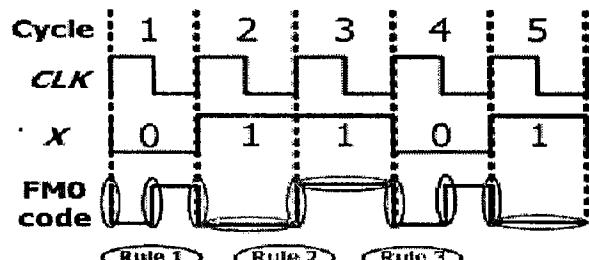


Fig.1. Illustration of FM0 coding example.

## A Novel High Speed Memory Solution using TCAM

P. POOJITHA<sup>1</sup>, ASHOK KUMAR<sup>2</sup>

<sup>1</sup>PG Scholar, Dept of ECE, PBR Visvodaya Institute of Technology and Science, Kavali, Nellore(Dt), AP, India.  
<sup>2</sup>Associate Professor, Dept of ECE, PBR Visvodaya Institute of Technology and Science, Kavali, Nellore(Dt), AP, India.

**Abstract:** Ternary content addressable memories (TCAMs) perform fast inquiry errand yet when differentiated and static random access memories (SRAMs), TCAMs have certain obstructions, for instance, low amassing thickness, for the most part direct access time, low adaptability, complex hardware, and are uncommonly exorbitant. In like manner, would we have the capacity to use the upsides of SRAM by planning it (with additional justification) to engage it to act like TCAM? This short proposes a novel memory architecture, named Z-TCAM, which impersonates the TCAM hardiness with SRAM. Z-TCAM wisely portions the conventional TCAM table along areas and columns into cream TCAM sub tables, which are then dealt with to depict their relating memory pieces. Two case gets ready for Z-TCAM of sizes  $512 \times 36$  and  $64 \times 32$  have been executed on Xilinx Virtex-7 field-programmable gate array.

**Keywords:** Application Particular Incorporated Circuit (ASIC), Memory Architecture, Priority Encoder, Static Random Access Memory(SRAM)- Based TCAM, Ternary Content Addressable Memory (TCAM).

### I. INTRODUCTION

Ternary content addressable memory (TCAM) empowers its memory to be looked by contents rather than by an address and a memory territory among matches is sent to the yield in a reliable time. A customary TCAM cell has two static random access memory (SRAM) cells and a relationship equipment and can store three states – 0, 1, and x where x is a couldn't mind less state. The x state is always seen as facilitated paying little mind to the data bit. The unfaltering time quest for TCAM makes it a fitting rival in different applications, for instance, mastermind switches, data pressure, progressing illustration planning in contamination recognizable proof, and picture preparing [1]. TCAM gives single clock inquiry; in any case, it has a couple of damages differentiated and SRAM. TCAM isn't subjected to the genuine business contention found in the RAM grandstand [2]. TCAM is less thick than SRAM. The comparator's equipment in TCAM cell adds multifaceted nature to the TCAM architecture. The extra reason and capacitive stacking due to the tremendous parallelism extend the access time of TCAM, which is 3.3 times longer than the SRAM access time [3]. Common basic obstacles in like manner confine the total chip breaking point of TCAM. Complex joining of memory and method of reasoning moreover sets aside a couple of minutes consuming

[1]. With the potential great conditions of SRAM over CAM, and common sense of FPGA development, we propose a memory architecture called Z-TCAM that mirrors TCAM value with SRAM and has been adequately completed on Xilinx Virtex-7 FPGA and moreover arranged using OSUcells library for  $0.18 \mu\text{m}$  advancement. We ensure that the proposed TCAM offers comparative request execution, flexibility, and lower cost than set up TCAM contraptions, gave that SRAM devices are denser, more affordable, and work snappier than TCAM devices.

### A. Related Work

We gather RAM-based responses for CAM in this fragment. The methods proposed in [2] and [12] use hashing to collect CAM from RAM however these methodologies encounter the evil impacts of crashes and holder surge. If various records have been placed in a surge zone, by then a question may not finish until the point that the moment that various bowls are looked for. In [12], when secured keys contain couldn't mindless bits in the bit positions used for hashing, by then such keys must be replicated in different buckets, which require extended utmost. On the other hand, if the interest scratch contains couldn't mindless bits which are taken by the hash work, different bowls must be accessed that results in execution defilement. In [2], the execution of the method ends up being easily degradable as the amount of set away segments increases. Additionally, it duplicates matched CAM, not TCAM. Thusly, hashing can't give deterministic execution inferable from potential crashes and is inefficient in dealing with extraordinary case. Standard algorithmic chase courses of action take different clock cycles [11] and besides result in inefficient memory use [10]. Strikingly, Z-TCAM has a deterministic request execution that is free of data, viably handles the trump cards, and has better memory utilize.

The technique proposed in [13] merges RAM and CAM to develop the CAM helpfulness. This approach makes packages of the customary TCAM table using some perceiving bits in CAM sections. In any case, making allocations of totally random data is a greatly dull and monotonous occupation. Since the methodology uses TCAM as a bit of the general architecture, it brings the inherent TCAM downsides in the general architecture of [13] however Z-TCAM is non particular and has a straightforward dividing. Crush based CAMs showed in [6] and [14] have an

# Construction and Design of Microcontroller Embedded Based Viscometer

P. Seshu Mani, Prof. S. Vijaya Bhaskara Rao, D. Uma Maheswara Reddy

## ABSTRACT

Ostwald Viscometer with Photo – Detector system is developed by using Light Emitting Diode and Light Dependent Resistor. The flow time is measured with Microcontroller and output displayed on Liquid Crystal Display. Software is written in computer for the measurement of flow time in embedded ‘c’ and hardware designing is described. The accuracy of the newly designed instrument is in milliseconds.

## 1. INTRODUCTION

Viscosity is the property of the fluid arising from collisions between neighboring particles that are moving at different velocities. Viscosity is measured with different types of viscometers. In conventional Ostwald Viscometer, flow time is measured between two fiducial marks with stop watch. By reducing human errors we are developed a newly designed Ostwald Glass Capillary Viscometer with a photo - Detector System [ 1 ]. The flow time measured by using hardware and software explained in the next sections.

## 2. HARDWARE DESIGNING

The block diagram of experimental set up for the measurement of viscosity is shown in fig. 1. The function of each block is explained below.

### 5V D. C. POWER SUPPLY

One of output of computer is taken as input to the ARDUINO BOARD. It gives 5V D. C. power supply constantly.

### VISCOMETER

Now we are using Ostwald Capillary Viscometer shown in Fig. 2. It consists of two wider bulbs A

and B having different capacities. Bulb A is called reservoir with more capacity and bulb B with less capacity. In between these bulbs there is a U – tube possess capillary E and F below bulb B. There are two fiducial marks U and L one above the bulb B and one lower the bulb B. A fixed mark G is placed above the bulb A to maintain constant volume.

### PHOTO DETECTOR SYSTEM FOR UPPER MARK 'U'

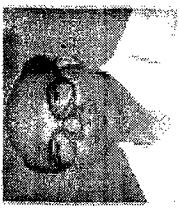
This system consists of Light Emitting Diode ( LED ) L 1 and a Light Dependent Resistor ( LDR ) R 1. These two are placed exactly in opposite direction, because the light coming from LED is exactly falling on LDR. These LED and LDR are placed in small glass tubes fixed with araldite to the upper fiducial mark of the viscometer. The power of LED is taken from ARDUINO BOARD Supply Out. Hence bidirectional arrows are used at Photo - Detector System for upper mark 'U'.

### PHOTO DETECTOR SYSTEM FOR LOWER MARK 'L'

Lower mark Photo Detector System also consists of one Light Emitting Diode ( LED ) L 2 and one Light Dependent Resistor ( LDR ) R 2 exactly in opposite direction placed in glass tubes. These two glass tubes are fixed with viscometer by araldite. The power of LED L 2 is taken from ARDUINO BOARD Supply Out, so bidirectional arrow marks are used.

### THERMISTOR

Thermistor means Thermal Resistor, having negative temperature coefficient of temperature. Thermistor is highly sensitive to temperature variations and gives correct temperature. The power of Thermistor is taken from ARDUINO BOARD Supply Out. Therefore bidirectional arrows are used.



**PARVATHAREDDY BABU REDDY**  
**VISVODAYA INSTITUTE OF TECHNOLOGY & SCIENCE**  
 (Affiliated to J.N.T.U.A, Approved by AICTE and Accredited by NAAC with 'A' Grade)  
**KAVALLI – 524201, S.P.S.R Nellore Dist., A.P. India. Ph: 08626-243930**

## **DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING**

### **List of Publications**

**Academic Year: 2018-19**

S.No	Title of paper	Name of the author/s	Department of the teacher	Name of journal	Year of publication	ISSN number	Link to the recognition in UGC enlistment of the Journal
1	A novel fan shaped UWB antenna with band notch for WLAN using a simple parasitic slit	Dr.A.Maheswara Rao	ECE	International Journal of Electronics Letters	Sep,2018	ISSN:2168-1724 (Print) 2168-1732 (Online) Journal.	<a href="https://www.tandfonline.com/doi/abs/10.1080/21681724.2018.1519854">https://www.tandfonline.com/doi/abs/10.1080/21681724.2018.1519854</a>
2	IOT BASED AUTO METRO TRAIN SHUTTLE BETWEEN STATIONS	Dr.A.Maheswar Rao	ECE	Journal of Emerging Technologies and Innovative Research (JETIR)	June,, 2019	ISSN-2349-5162	<a href="http://www.jetir.org">www.jetir.org</a>
3	Compact UWB monopole antenna with quadruple band notched characteristics	Dr.A.Maheswar Rao	ECE	International Journal of Electronics	May,2019	ISSN: 0020-7217 (Print) 1362-3060 (Online)	<a href="https://www.tandfonline.com/doi/ten20">https://www.tandfonline.com/doi/ten20</a>
4	A Novel Fan Shaped UWB Antenna with BandNotch for WLAN Using a Simple Parasitic Slit	Dr. A.Maheswara Rao	ECE	International Journal of Electronics Letters.	Sep,2018	ISSN: 2168-1724 (Print) 2168-1732 (Online)	<a href="https://doi.org/10.1080/21681724.2018.1519854">https://doi.org/10.1080/21681724.2018.1519854</a>
5	Arduino Based Oil Tank Truck Alarm System for Illegal Fuel Hoarding Using GSM Module	R.Pratap Singh	ECE	International Journal of Advanced Technology and Innovative Research	July,2018	ISSN 2348-2370	<a href="http://ijatir.org/uploads/136425IJATIR17020-141.pdf">http://ijatir.org/uploads/136425IJATIR17020-141.pdf</a>
6	An Adaptive Resource Allocation and Management in Full Duplex Heterogeneous Network	R.Pratap Singh	ECE	International Journal of Advanced Technology and Innovative Research	Mar, 2019	ISSN 2348-2370	<a href="http://www.ijatir.org/issue.php?issue=203&amp;volume=Volume11">http://www.ijatir.org/issue.php?issue=203&amp;volume=Volume11</a>
7	Image Watermarking using QR Decomposition	V.Phani Bhushan	ECE	International Journal of Advanced Technology and Innovative Research	July, 2018	ISSN 2348-2370	<a href="http://ijatir.org/uploads/452631IJATIR17018-139.pdf">http://ijatir.org/uploads/452631IJATIR17018-139.pdf</a>

8	NonLocal Centralized and Adaptive PCA Based Denoising Technique for color images	V.Phani Bhushan	ECE	International Journal of Advanced Technology and Innovative Research	Aug, 2018	ISSN 2348-2370	<a href="http://www.ijati.org/issue.php?issue=Volume10&amp;page=3">http://www.ijati.org/issue.php?issue=Volume10&amp;page=3</a>
9	Power Monitoring System For Automatic Metering And Billing	A.Suman Kumar Reddy	ECE	International Journal of Advanced Technology and Innovative Research	Dec, 2018	ISSN 2348-2370	<a href="http://www.ijardcs.org/backissues/article ISSUE%208&amp;volume=Volume10&amp;page=2">http://www.ijardcs.org/backissues/article ISSUE%208&amp;volume=Volume10&amp;page=2</a>
10	Improved Adaptive Multipath Routing for Congestion Control	N.Krishna Chaitanya	ECE	Journal of Advanced Research in Dynamical and Control Systems (JARDCS),	Aug, 2018	ISSN: 1943-023X	<a href="http://link.springer.com/article/10.1007/s11277-018-6003-z">http://link.springer.com/article/10.1007/s11277-018-6003-z</a>
11	Traffic Aware Congestion Control Priority based Efficient Adaptive Multipath Routing in wired networks with new queuing Technique	N.Krishna Chaitanya	ECE	Wireless Personal Communication, Springer Publications,	Dec, 2018	ISSN: 0929-6212.	<a href="https://doi.org/10.1007/s11277-018-6003-z">https://doi.org/10.1007/s11277-018-6003-z</a>
12	Design and implementation of 64 bit parallel self time adder(PASTA)	M.Pavitra	ECE	IJPRES International Journal of Professional Engineering studies	Dec, 2018	ISSN 2348-2370	<a href="http://www.ijpres.com/pdf40/12.pdf">http://www.ijpres.com/pdf40/12.pdf</a>
13	A Fire Alarming System For Monitoring Environmental Fire Issues Based On YCbCr Method	N.V.Sai Chand	ECE	International Journal of Advanced Technology and Innovative Research	Nov,2018	ISSN 2348-2370	<a href="http://www.ijatir.org/issue.php?issue=Volume10">http://www.ijatir.org/issue.php?issue=Volume10</a>
14	Environment Pollution Awareness through Vehicle Tracking System Using IOT	Ch.Amarnath Sharma	ECE	International Journal of Scientific Research and Review	Nov,2018	ISSN 2279-543x	<a href="http://www.dynamiccpublisher.org/gallery/83-ijstr-1115.f.pdf">http://www.dynamiccpublisher.org/gallery/83-ijstr-1115.f.pdf</a>
15	FPGA Implementation of Reconfigurable FIR Filter using Carry Bypass Adder	Sk.Rasool	ECE	International Journal of Advanced Research in Computer and Communication Engineering and	Nov,2018	ISSN (Online) 2278-1021 ISSN (Print) 2319-5940	<a href="https://ijarce.com/papers/fpga-implementation-of-reconfigurable-fir-filter-using-carry-bypass-adder/">https://ijarce.com/papers/fpga-implementation-of-reconfigurable-fir-filter-using-carry-bypass-adder/</a>
16	Environment Pollution Awareness through Vehicle Tracking System Using IOT	A.Srinivasa Rao	ECE	International Journal of Scientific Research and Review	Nov,2018	ISSN 2279-543x	<a href="http://www.dynamiccpublisher.org/gallery/83-ijstr-1115.f.pdf">http://www.dynamiccpublisher.org/gallery/83-ijstr-1115.f.pdf</a>

  
Faculty Incharge

Head of the Department  
Electronics & Communication Engineering  
OB Visvadharan Institute of  
Technology & Science  
KAVALI - 524 201

## A novel fan shaped UWB antenna with band notch for WLAN using a simple parasitic slit

V. N. Koteswara Rao Devana & A. Maheswara Rao

To cite this article: V. N. Koteswara Rao Devana & A. Maheswara Rao (2018): A novel fan shaped UWB antenna with band notch for WLAN using a simple parasitic slit, International Journal of Electronics Letters, DOI: [10.1080/21681724.2018.1519854](https://doi.org/10.1080/21681724.2018.1519854)

To link to this article: <https://doi.org/10.1080/21681724.2018.1519854>



Accepted author version posted online: 10  
Sep 2018.  
Published online: 22 Sep 2018.



Submit your article to this journal 



Article views: 30



View Crossmark data 

# IOT BASED AUTO METRO TRAIN SHUTTLE BETWEEN STATIONS

<sup>1</sup>A.Suman Kumar Reddy,<sup>2</sup>A.Maheswar Rao

<sup>1</sup>Associate Professor, <sup>2</sup>Professor,Dept. Of E.C.E

<sup>1,2</sup>PBR Visvodaya Institute of Technology & Science, Kavali , Nellore (Dt), AP, India.

## ABSTRACT

This paper proposes the equipment utilized in metro train movement which are utilized in a large portion of the advanced nations. In this automatic metro train, we have given raspberry pi controller that encourages the modified stopping of the train starting with one station then onto the next station. This work introduces the upgrade procedure of a structure for a driverless train incited utilizing raspberry pi based controller. The equipment circuit's plan, which are based on circuit sheets, are furnished with different sensors for computerization purposes. The equipment is amassed in a toy-like train structure. Driverless trains are equipped with a control framework, which is modified to cause them to pursue an exact way. Stations on such a way, timings of the train and separations between stations are all predefined. Messages and admonitions are automatically created and reported to the passengers.

This embedded application for the most part centers around conquering escape conditions in the present structure. It is progressed to meet the cost and power use necessities.

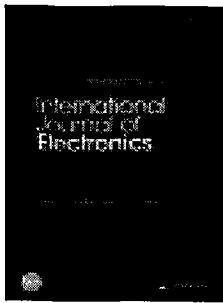
## I.INTRODUCTION

Later innovative advancements are being acclimatized in practically all purpose of our life including travel transportation, where a ton of upgradation has been made. Railroad transport, for actuality, has experienced an enormous change, beginning with the early steam worked motors to the latest shot train. Numerous advancements in travel transport has used the current framework, where the current metro framework is being modernized and outfitted with automatic train control and security framework so as to make them increasingly beneficial. Driverless robotized ideas have been received, The goal of this task is to drive the train automatically with the assistance of sensors and security of passengers is the essential worry of our model-based model metro train. In this work, some portion of this mechanization assignments is considered, and an

Arduino-based model is created. work, for example, going through a given way with predefined stations, and detecting the landing in the station and henceforth, appropriate stopping are executed in the structure. Data that are synced with the train's development through its way are reported to passengers by means of a LCD display. Additionally, alarm sign are delivered as fitting. Controlling of the entryways as far as open and close and timings of such activities are considered.

## II.LITERATURE SURVEY

In present day days metro train transportation has transformed into the most down to earth and safe strategy for open transportation system. It interfaces two significant urban networks and gives a quick transportation organizations to individuals by and large. The unmanned metro train (Driverless) licenses an incredibly secure and prevalent techniques for transportation. The model makes use of microcontroller to control the train advancements. It similarly controls traveler checking and makes a notice banner including customized opening and closing of doors. The train continues running between two predefined stations. It in like manner gives an office of effect evading if there ought to be an event of two trains being on a comparative track. The partition between two stations are moreover predefined. The train continues running between two stations without human intervention. It gives a reset change to the traveler which goes about as an emergency stopping instrument to stop the train if there ought to be an event of emergency. The crucial idea of the methodology is to allow customized metro train structure which is completely unmanned and is careful and errorless in its assignment. Counting of passengers happens by using bidirectional revelation by IR and photo diode plan.



## Compact UWB monopole antenna with quadruple band notched characteristics

V N Koteswara Rao Devana & A. Maheswara Rao

To cite this article: V N Koteswara Rao Devana & A. Maheswara Rao (2019): Compact UWB monopole antenna with quadruple band notched characteristics, International Journal of Electronics, DOI: [10.1080/00207217.2019.1636311](https://doi.org/10.1080/00207217.2019.1636311)

To link to this article: <https://doi.org/10.1080/00207217.2019.1636311>



Accepted author version posted online: 25 Jun 2019.  
Published online: 02 Jul 2019.



Submit your article to this journal 



Article views: 13



View Crossmark data 

## A Novel Fan Shaped UWB Antenna with Band Notch for WLAN Using a Simple Parasitic Slit

V N Koteswara Rao Devana & Dr. A. Maheswara Rao

To cite this article: V N Koteswara Rao Devana & Dr. A. Maheswara Rao (2018): A Novel Fan Shaped UWB Antenna with Band Notch for WLAN Using a Simple Parasitic Slit, International Journal of Electronics Letters, DOI: [10.1080/21681724.2018.1519854](https://doi.org/10.1080/21681724.2018.1519854)

To link to this article: <https://doi.org/10.1080/21681724.2018.1519854>



Accepted author version posted online: 10 Sep 2018.



Submit your article to this journal



View Crossmark data