Mangalam Campus
Mangalam Hills, Vettimukal P.O
Ettumanoor, Kottayam
Kerala-686631

MANGALAM
COLLEGE OF ENGINEERING

Inspire | Imbibe | Innovate

Ph :+91-481-2710120, +91-481-2537053
+91-481-2533711, Fax: +91-481-2533700
Web : www.mangalam.ac.in
E-mail : info@mangalam.in

(Approved by AICTE, Affiliated to MGU / APJ Abdul Kalam Technological University, NAAC Accredited & ISO Certified Institution)

3.3.2 Number of research papers per teachers in the Journals notified on UGC website during the last five years (10)

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 /Digita Object Identifier (doi) number		
						Link to website	Link to article/pape	Is it listed i UGC Car
Improval AQUAPRO	Preethi Sebastian	EEE	IJCSE	Sep-17			https://www.ijcseonline.org/archive_is	UGC
Improval AQUAPRO	Susan V Nainan	EEE	IJCSE	Sep-17			https://www.ijcseonline.org/archive_issue.php?pub_id=52	UGC
Improval AQUAPRO	,Jeneesh Scaria	EEE	IJCSE	Sep-17			https://www.ijcseonline.org/archive_issue.php?pub_id=53	UGC
Improved Analysis of EAHE and the effect of Pipe Material in its Performance	Jishnu	ME	IJCSE	Nov-17			https://www.ijcseonline.org/archive_issue.php?pub_id=53	UGC
Improved Analysis of EAHE and the effect of Pipe Material in its Performance	Arun Jose	ME	IJCSE	Nov-17			https://www.ijcseonline.org/archive_issue.php?pub_id=53	UGC

PRINCIPAL
MANGALAM COLLEGE OF ENGINEERIN
Ettumanoor

Improved Analysis of EAHE and the effect of Pipe Material in its Performance	Harikrishnan	ME	IJCSE	Nov-17			https://www.ijcseonline.org/archive_issue.php?pub_id=53	UGC
Improved Analysis of EAHE and the effect of Pipe Material in its Performance	Leneesh N Gopal	ME	IJCSE	Nov-17			https://www.ijcseonline.org/archive_issue.php?pub_id=53	UGC
IMPROVING CUSTOMER SATISFACTION CRITERIA IN E - COMMERCE PLATFORM BEFORE AND DURING COVID PANDEMIC	Jishnu M	ME	IJCSE	Nov-17			https://www.ijcseonline.org/archive_issue.php?pub_id=53	UGC
IMPROVING CUSTOMER SATISFACTION CRITERIA IN E - COMMERCE PLATFORM BEFORE AND DURING COVID PANDEMIC	Arun Jose	ME	IJCSE	Nov-17			https://www.ijcseonline.org/archive_issue.php?pub_id=53	UGC
IMPROVING CUSTOMER SATISFACTION CRITERIA IN E - COMMERCE PLATFORM BEFORE AND DURING COVID PANDEMIC	Harikrishnan	ME	IJCSE	Nov-17			https://www.ijcseonline.org/archive_issue.php?pub_id=53	UGC
IMPROVING CUSTOMER SATISFACTION CRITERIA IN E - COMMERCE PLATFORM BEFORE AND DURING COVID PANDEMIC	Lenish	ME	IJCSE	Nov-17			https://www.ijcseonline.org/archive_issue.php?pub_id=53	UGC

PRINCIPAL
MANGALAM COLLEGE OF ENGINEERING
Ettumanoor

IoT based Precision Agriculture	Reshma Chandrn	ECE	IJCSE	Dec-17			https://www.ijcseonline.org/archive_issue.php?pub_id=54	UGC
IoT based Precision Agriculture	Siml P Thomas	ECE	IJCSE	Dec-17			https://www.ijcseonline.org/archive_issue.php?pub_id=55	UGC
IoT based Precision Agriculture	Neethan Elizabeth Abraham	ECE	IJCSE	Dec-17			https://www.ijcseonline.org/archive_issue.php?pub_id=56	UGC
IoT based Precision Agriculture	,Anu Philip	ECE	IJCSE	Dec-17			https://www.ijcseonline.org/archive_issue.php?pub_id=57	UGC
Privacy protection on cloud computing with auditing scheme	Nimmymol Manuel	CSE	IJCSE	Dec-17			https://www.ijcseonline.org/archive_issue.php?pub_id=58	UGC
Privacy protection on cloud computing with auditing scheme	Simy Mary Kurian	CSE	IJCSE	Dec-17			https://www.ijcseonline.org/archive_issue.php?pub_id=59	UGC
Privacy protection on	Neena	CSE	IJCSE	Dec-17			https://www	UGC
Privacy protection on	Neema	CSE	IJCSE	Dec-17			https://www	UGC
Time Table	Vinodh P	CSE	IJCSE	Dec-17			https://www	UGC
Time Table	Neena	CSE	IJCSE	Dec-17			https://www	UGC
Time Table	Neema	CSE	IJCSE	Dec-17			https://www	UGC
Time Table	Simy Mary	CSE	IJCSE	Dec-17			https://www	UGC
Improving Image	Nimmy Mol	CSE	IJCSE	Jan-18			https://www	UGC
Improving Image	Neena	CSE	IJCSE	Jan-18			https://www	UGC
Improving Image	Neema	CSE	IJCSE	Jan-18			https://www	UGC
IoT Enabled Sensor	Neena	CSE	IJCSE	Mar-18			https://www	UGC
IoT Enabled Sensor	nodh P Vijay	CSE	IJCSE	Mar-18			https://www	UGC

PRINCIPAL
IANGALAM COLLEGE OF ENGINEERIN
Ettumanoor

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		
						Link to website of the Journal	Link to article/paper/abstract of the article	Is it listed in UGC Care list/Scopus/Web of Science/other, mention
IoT Enabled Sensor Network and Machine Learning	Neema George	CSE	IJCSE	Mar-18			https://www.ijcseonline.org/archive_issue.php?pub_id=57	UGC
IoT Enabled Sensor Network and Machine Learning	Nimmymol Manue	CSE	IJCSE	Mar-18			https://www.ijcseonline.org/archive_issue.php?pub_id=57	UGC
Multiple parameter analysis on wireless network using spatial reusability	Athira Manikuttan, Vinodh P Vijayan, Neena Joseph	Computer Science and Engineering	International Journal Of Creative Research Thoughts (IJCRT)	2018	ISSN: 2320-2882		https://ijcrt.org/papers/IJCRT1892182.pdf	Google Scholar
Improving End-to-End Throughput in Wireless Network using Spatial Reusability	Athira Manikuttan, Vinodh P Vijayan, Neena Joseph	Computer Science and Engineering	International Journal of Advance Research, Ideas and Innovations in Technology (IJARIIT)	2018	ISSN: 2454-132X		https://www.ijariit.com/manuscripts/v4i1/V4I1-1375.pdf	Google Scholar
Multiple parameter analysis on wireless network using spatial reusability	Athira Manikuttan, Vinodh P Vijayan, Neena Joseph	Computer Science and Engineering	International Journal Of Creative Research Thoughts (IJCRT)	2018	ISSN: 2320-2882		https://ijcrt.org/papers/IJCRT1892182.pdf	Google Scholar

PRINCIPAL
MANGALAM COLLEGE OF ENGINEERING
Ettumanoor

Improving End-to-End Throughput in Wireless Network using Spatial Reusability	Athira Manikuttan, Vinodh P Vijayan, Neena Joseph	Computer Science and Engineering	International Journal of Advance Research, Ideas and Innovations in Technology (IJARIIT)	2018	ISSN: 2454-132X		https://www.ijariit.com/manuscripts/v4i1/V4I1-1375.pdf	Google Scholar
An Efficient Security Key for Practical Requirement of PIN Entry Protection Section Authentication	Kiren Vijai, Neena Joseph	Computer Science and Engineering	International Journal of Advance Research, Ideas and Innovations in Technology (IJARIIT)	2018	Corpus ID: 54219107		https://www.semanticscholar.org/paper/An-Efficient-Security-Key-for-Practical-Requirement	Google Scholar
Automatically mining query facet from search results using text mining algorithm	Soniya Joy , Neena Joseph	Computer Science and Engineering	International Journal of Advance Research, Ideas and Innovations in Technology (IJARIIT)	2018	ISSN:2454-132X		https://www.ijariit.com/manuscripts/v4i3/V4I3-1775.pdf	Google Scholar
An efficient framework security model of sharing data for privacy protection and performance-based outsource data sharing on cloud	Kiren Vijai, Syamamol T, Merlin Mary James	Computer Science and Engineering	International Journal of Advance Research, Ideas and Innovations in Technology (IJARIIT)	MARCH-APRIL 2018	Corpus ID: 53689568 /ISSN: 2454-132X		https://www.semanticscholar.org/paper/An-Efficient-Framework-Security-Model-of-Sharing-on	Google Scholar

PRINCIPAL
MANGALAM COLLEGE OF ENGINEERIN
Ettumanoor

An efficient framework security model of sharing data for privacy protection and performance-based outsource data sharing on cloud	Kiren Vijai, Syamamol T, Merlin Mary James	Computer Science and Engineering	International Journal of Advance Research, Ideas and Innovations in Technology (IJARIIT)	MARCH-APRIL 2018	Corpus ID: 53689568		https://www.semanticscholar.org/paper/An-Efficient-Framework-Security-Model-of-Sharing-on	Google Scholar
High Efficient Z-Source DC Dc Boost Converter	Susan V Ninan	EEE	International Journal of Advance Research, Ideas and Innovations in Technology	2017-18	ISSN: 2454-132X Impact factor: 4.295 (Volume 4, Issue 3)			Google Scholar
Control of Grid-Connected Photovoltaic Systems to Improve the Voltage Profile of a Distribution Feeder	Preethi Sebastian	EEE	International Journal of Science & Engineering Development Research	2017-18	ISSN:2455-2631		http://www.ijsdr.org/papers/IJSDR1706047.pdf	Google Scholar
A Study on the Impact of Brand Loyalty for Cosmetic Products among Female Customers in selected Districts of Kerala	Dr. Sibu C. Chithran	Management Studies	Journal of Management and Innovative Information Technology	2017	2395-4981			Google Scholar

PRINCIPAL
MANGALAM COLLEGE OF ENGINEERIN
Ettumanoor

A Study on the Impact of Voluntary Labour Standards on Coir Industry in Kerala	Dr. Sibu C. Chithran	Management Studies	Journal of Management and Innovative Information Technology	2017	2395-4981			Google Scholar

PRINCIPAL
MANGALAM COLLEGE OF ENGINEERIN
Ettumanoor

Control of Grid-Connected Photovoltaic Systems to Improve the Voltage Profile of a Distribution Feeder

[1]ATHIRA SASANKAN, [2]PREETHY SEBASTIAN

Mangalam College of Engineering
Ettumanoor, Kottayam Kerala

***Abstract*: This paper presents a photovoltaic system interconnecting 15 bus radial distribution feeder for the finding the variation of bus voltage and line current. It consists of a PV array in addition to a power conditioning system for grid interfacing purposes. The power conditioning system is composed of a DC-DC boost converter, followed by a current controlled Voltage Source Inverter (VSI)). An analysis of bus voltage and line current is made with the simulated model. By connecting PV to the loaded line its voltage profile can be improved.**

***Index terms:* MPPT, Voltage source inverter, photovoltaic, reverse saturation current**

I. INTRODUCTION

The present energy production has mainly been based on energy sources like oil, gas and coal, which until today was looked upon as close to inexhaustible. As the global energy consumption is growing with a drastically high rate and the fossil fuels reserves are shrinking, the urge for renewable energy resources has attained more focus [1]. Both renewable and non-renewable energy resources are mostly created by the sun rays hitting the surface of the earth. The sun is a non-polluting resource responsible for the sustained life on earth. Among the renewable energy resources are hydro power, wind power and solar energy. While hydro power has been a well-known technology for a long time, there is a lot of research going on with wind and solar power today. Solar energy as a source of energy has a large theoretical potential, and can be utilized both directly and indirectly. In a grid connected Photovoltaic (PV) inverter system the PV system utilize the solar energy as the power source and transfer the power into the grid through power electronics conditioning.

The strategy behind Maximum Power Point Tracking (MPPT) results in appreciable increase in the efficiency of the Photovoltaic System. The MPPT algorithm thus proposed identifies the suitable duty ratio in which the DC/DC converter should be operated to obtain maximum power output. However the solar radiation never remains constant. The main objective is to track the maximum power point (MPP) of the solar array by modulating the DC-DC converter's duty cycle, thereby, optimizing the power output of the panel. The Perturb and Observe (P&O) algorithm is utilized here which performed with a higher overall efficiency capable of tracking the MPP quickly[2].

II. EVALUATION OF THE BASIC BLOCKS

The major components of a grid connected PV system are shown in figure 1. It consists of a PV array, DC–DC Boost converter, and a voltage source inverter. The module making solar array converts sun's energy to direct current (DC). This output has to be converted to AC for interfacing with the grid. The mounting system supports the solar array at different angles to the sun. Output of a PV array varies with temperature and irradiation. Irradiation is the amount of radiation both direct and diffused that can be received at any given location. MPPT method is used to track maximum power from the solar array. The switching of DC-DC converter is based on MPPT.

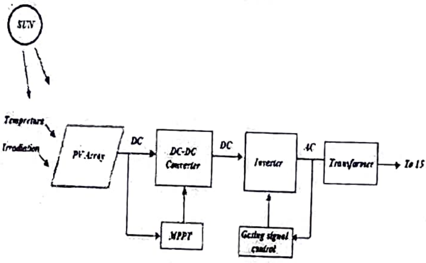


Fig.1. Block diagram of grid connected photovoltaic system

The DC–DC boost converter extracts maximum power from the solar array and increases the terminal voltage to a level suitable for interfacing with the 15 bus.The voltage source inverter converts DC to AC. For the switching of inverter gating signals are provided. The transformer increases the voltage and the system is interfaced to the 15 bus.

The equivalent circuit model of a PV cell is needed in order to simulate its real behavior. Using the physics of p-n junctions, a PV cell can be modeled as a DC current source in parallel with a diode that represents currents escaping due to diffusion. Two resistances, R_s and R_p, are included to model which are the contact resistances and the internal PV cell resistance respectively. PV cell equivalent circuit model is shown in Fig.2.

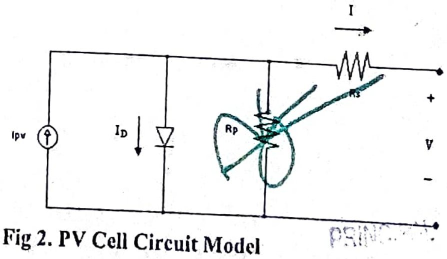


Fig 2. PV Cell Circuit Model

IJARIIT

INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume 4, Issue 3)

Available online at: www.ijariit.com

Highly efficient Z source inverter

Mithun Manohar
mithunmanohar.eee@gmail.com
Mangalam College of Engineering,
Kottayam, Kerala

Susan V Ninan
susan.ninan@mangalam.in
Mangalam College of Engineering,
Kottayam, Kerala

Jeepa K J
jeepa.kj@mangalam.in
Mangalam College of Engineering,
Kottayam, Kerala

ABSTRACT

This project deals with the design, analysis, simulation, and development of Highly Efficient Boost Inverter using Z Source Network. The boost capabilities of the traditional Z-source networks are limited; the proposed converters are composed of combined traditional Z-Source networks in different ways to enhance the boost abilities of the traditional Z-source networks. The proposed converter are satisfied the traditional benefits of Z-source networks with stronger voltage boost abilities which can also be applied to dc-ac, ac-ac, and ac-dc power conversions. Analysis, MATLAB Simulation, and the Experimental result were illustrated in this paper.

Keywords: *DC-DC Converters; Z Source; Inverter; Voltage Boosting.*

1. INTRODUCTION

A system involving power converters are being often used in applications like alternative energy sources and hybrid electric vehicle (HEV). A major objective for power electronics designers is efficiency, low cost & reliability. In a PV power system, the output voltages of the PV panels are usually low and vary widely under the influences of climate and environment, therefore, a step-up stage is required.An Z-source inverter can perform buck-boost functions, as compared to the traditional voltage–source inverter. An additional shoot-through zero state is added to the switching states in order to boost the voltage. The design of the step-up dc-dc converters is very important to the PV power systems[2]. The unregulated low dc voltage of PV panels, which cannot be provided for inverters, must be boosted and regulated through the high-gain converters[1]. Then, the step-up converters output regulated high dc voltage to the grid-connected inverters. The application of Z-source networks in dc-dc power conversion is a fastest growing area for research. Therefore, this paper applies the Z-source networks to dc-dc converters with their boost abilities and proposes a family of hybrid Z-source boost dc-dc converters, which are obtained by combining the traditional Z-source/quasi-Z-source networks in different ways[1].The Z-Source inverter(ZSI) has been introduced in order to overcome the limitations of the traditional converter.The ZSI has the unique buck-boost capability which ideally gives an output voltage range from zero to infinity regardless of the input voltage. The additional functionality of ZSI over the traditional inverter can be stated not only in terms of boost for DC to AC power conversion but a short circuit across any phase leg is allowed & dead band is not required[11]. The second order filter is provided which is more efficient in suppressing output voltage ripples. The inrush current and harmonics can be reduced.

In this paper, operating principle of Z-source dc-dc Converter is explained, at present, the studies on Z-source networks mainly focus on the field of dc-ac power conversion, while the application of Z-source networks in dc-dc power conversion is essentially required. Therefore, this paper applies the Z-source networks to dc-dc converters with their boost abilities and proposes highly efficient Z-source boost dc-dc converters [10-13].

The proposed converter is very suited for PV power systems, where the dc-dc converter with the high step-up ability is required.
The remainder of this paper is structured as follows. The operating principles and parameters design are presented in Sections II. The design Parameter is Presented in III. Finally, the simulation results are given in Sections V and Experimental results are given in section VI to verify the features of the proposed Inverter.

2. OPERATING PRINCIPLES OF THE PROPOSED CONVERTER

The following Conditions are assumed for the operating principles.

- All the components are ideal.
- All Capacitor Voltages are treated as constant.
- The proposed converter operates in CCM.

3.3.2 Number of research papers per teachers in the Journals notified on UGC website during the last five years (10)

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 /Digital		
						Link to website of the Journal	Link to article/paper/abstract of the article	Is it listed in UGC Care list/Scopus/Web of Science/other, mention
Multiple parameter analysis on wireless network using spatial reusability	Athira Manikuttan, Vinodh P Vijayan, Neena Joseph	Computer Science and Engineering	International Journal Of Creative Research Thoughts (IJCRT)	2018	ISSN: 2320-2882		https://ijcrt.org/papers/IJCRT1892182.pdf	Google Scholar
Improving End-to-End Throughput in Wireless Network using Spatial Reusability	Athira Manikuttan, Vinodh P Vijayan, Neena Joseph	Computer Science and Engineering	International Journal of Advance Research, Ideas and Innovations in Technology (IJARIIT)	2018	ISSN: 2454-132X		https://www.ijariit.com/manuscripts/v4i1/V4I1-1375.pdf	Google Scholar
Multiple parameter analysis on wireless network using spatial reusability	Athira Manikuttan, Vinodh P Vijayan, Neena Joseph	Computer Science and Engineering	International Journal Of Creative Research Thoughts (IJCRT)	2018	ISSN: 2320-2882		https://ijcrt.org/papers/IJCRT1892182.pdf	Google Scholar
Improving End-to-End Throughput in Wireless Network using Spatial Reusability	Athira Manikuttan, Vinodh P Vijayan, Neena Joseph	Computer Science and Engineering	International Journal of Advance Research, Ideas and Innovations in Technology (IJARIIT)	2018	ISSN: 2454-132X		https://www.ijariit.com/manuscripts/v4i1/V4I1-1375.pdf	Google Scholar
An Efficient Security Key for Practical Requirement of PIN Entry Protection Section Authentication	Kiren Vijai, Neena Joseph	Computer Science and Engineering	International Journal of Advance Research, Ideas and Innovations in Technology (IJARIIT)	2018	Corpus ID: 54219107		https://www.semanticscholar.org/paper/An-Efficient-Security-Key-for-Practical-Requirement	Google Scholar
Automatically mining query facet from search results using text mining algorithm	Soniya Joy , Neena Joseph	Computer Science and Engineering	International Journal of Advance Research, Ideas and Innovations in Technology (IJARIIT)	2018	ISSN:2454-132X		https://www.ijariit.com/manuscripts/v4i3/V4I3-1775.pdf	Google Scholar
An efficient framework security model of sharing data for privacy protection and performance-based outsource data sharing on cloud	Kiren Vijai, SyamamolT, Merlin Mary James	Computer Science and Engineering	International Journal of Advance Research, Ideas and Innovations in Technology (IJARIIT)	MARCH-APRIL 2018	Corpus ID: 53689568/ISSN: 2454-132X	http://www.ijariit.com/	https://www.semanticscholar.org/paper/An-Efficient-Framework-Security-Model-of-Sharing-on	Google Scholar
An efficient framework security model of sharing data for privacy protection and performance-based outsource data sharing on cloud	Kiren Vijai, SyamamolT, Merlin Mary James	Computer Science and Engineering	International Journal of Advance Research, Ideas and Innovations in Technology (IJARIIT)	MARCH-APRIL 2018	Corpus ID: 53689568		https://www.semanticscholar.org/paper/An-Efficient-Framework-Security-Model-of-Sharing-on	Google Scholar

HEAD OF DEPARTMENT
Department of Computer Science & Engineering
Mangalam College of Engineering
Ettumanoor 686 631

Internal Quality Assurance Cell (IQAC)
Mangalam College of Engineering
Kottayam, Kerala - 686 631

PRINCIPAL
MANGALAM COLLEGE OF ENGINEERING
Ettumanoor

PRINCIPAL
MANGALAM COLLEGE OF ENGINEERING

17-18
Jour

MULTIPLE PARAMETER ANALYSIS ON WIRELESS NETWORK USING SPATIAL REUSABILITY

Athira Manikuttan, Vinodh P Vijayan, Neena Joseph
P G Scholar, Assoc. Professor, Asst. Professor
Computer Science and Engineering
Mangalam College of Engineering, Ettumanoor, Kottayam

Abstract: The selection of optimal route from source node to destination node that guarantees a high end-to-end throughput, is the main issue of routing in multi hop wireless network especially in a multi objective and heterogeneous scenario. As the environment is heterogeneous and various parameters affect the system performance in varying scale, the issue seems to be much complex, most of the solutions end with local optimum because those algorithms mostly fail to ensure not only end to end throughput, but also other parameters of routing like delay, congestion control, energy of nodes etc. By considering spatial reusability of wireless networks, all these parameters of wireless multi hop remote systems can be enhanced significantly. To achieve the expected performance, Spatial-reusability Aware Single-path Routing (SASR) algorithm is proposed and to analyze the performance the same is compared with existing single path routing protocol. Assessment shows that proposed protocol shows significant improvement in comparison with existing protocols.

Index Terms: **Wireless network, spatial reusability, routing**

I. INTRODUCTION

Because of the constrained limit of wireless communication media, and lossy wireless connection [16], it is imperative to a great degree to choose a path that augment the end-to-end throughput, particularly in multi hop wireless network. A principle issue with existing wireless routing protocol is that limiting number of transmission to convey a single packet from source node to destination node does not rely augment the end-to-end throughput [4].

This paper examines routing protocol in single path routing. The goal of single path routing is to choose a cost limiting path along which the packets are conveyed from the source node to destination node. Large portion of existing protocols, link quality aware routing. They just select the path that limit the overall transmission count or transmission time for transmitting the packet.

An important property of wireless communication media which differentiate it from wired communication media is the spatial reusability. Wireless signal loses its energy through each hop[2]. Therefore, two links can be used at same time, if they in far distance. But existing protocols do not take this into consideration.

II. RELATED WORK

In this area a quick review on related work is done. And also compare our work with these and briefly review other works that consider reusability.

There is various work on wireless routing metrics. For single path routing a few link equality aware measurements [1][6][7][9] are proposed. RTT [1] measured the cost of single wireless link by the round trip delay of probe packets. ETX [6] allocated the link cost with its normal number of transmission to effectively convey a packet. Based on ETX the author in [9] outlined ETOP metric considering the connection genuine position on the way.

The early single path routing protocols [3] [10] [17] [18] applied Dijikstra's algorithm for selecting route. Some current cross-layer approaches mutually consider routing and also link scheduling eg [11] [19] [20]. Zhang et al [20] detailed joint routing and planning into an enhancement issue and tackled the issue with a segment age technique. Skillet et al [16] managed to the joint issue in subjective ratio systems considering the opening of authorized groups.

The calculations proposed in this work don't require any scheduling and the SASR calculations can be actualized in disseminated way. In [21] the authors consider the exchange between spatial reuse and information rate, proposed a decentralized power and rate control calculation for higher system limit Zhai and Fany [22] researched the ideal bearer detecting range for throughput augmentation.

III.SYSTEM MODEL

Consider a static multi-hop wireless network with N nodes. Assume that the nodes have same transmission rate and do not have any power control constraint in this work.

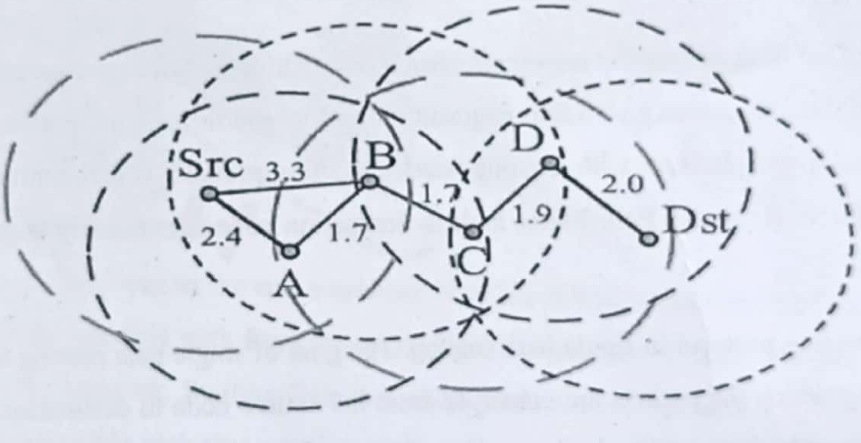


Fig 1. Importance of spatial reusability

Fig 1 shows a network with 6 nodes and each node's range is also shown. Each node's range is denoted by the circle with the node in its center. Each link is given an arbitrary cost. As wireless signal losses its energy in its prorogation, two wireless links can be worked at same time, if they are far away from each other [13] [14]. If any pair of the nodes are out of the interfacing range of each other, we call it non-interfacing set I and a non-interfacing set can work at same time [15].

Let's use an example from Fig 1. to represent significance of spatial reusability of the correspondence media in single-path directing in wireless system. Here we have four middle nodes (A, B, C, D) between source and destination. The dashed circle around each node demonstrate the range of the node. The cost is set apart close to each of the wireless link. There are two ways to reach destination (Dst) from the source (Src).

First Path: Src – B – C – D – Dst

Second Path: Src – A – B – C – D – Dst

First Path Cost = 8.9 (3.3+1.7+1.9+2.0) Equation 1

Second Path Cost = 9.7 (2.4+1.7+1.7+1.9+2.0) Equation 2

Since First Path have lower cost it is likely to select it as the best path.

But considering the spatial reusability, we can see in Second Path, the link Src – A and link D – Dst are out of range of each other and can work at the same time. It is important to combine spatially non-interfacing links while doing the path determination. By combine cost, we imply that cost of non-interfacing set can be considered as single. On selecting a path with Src – A and D – Dst together, instead of adding both the cost, we select the one with higher cost only. So now the total cost of Second Path can be lower to 7.7 which is less than total cost of First Path i.e.; 8.9.

IV. SPATIAL REUSABILITY AWARE SINGLE PATH ROUTING

We initially consider the spatial reusability-aware path cost assessment for single-path routing. Given each of the paths found by a current source routing algorithm (e.g., DSR [10]), our SASR calculation ascertains the spatial reusability aware path cost of it. At that point, the way with the small cost can be chosen.

The total SASR algorithm is proposed in two parts.

1. SASR-MIN algorithm
2. SASR-FF algorithm

4.1 SASR-MIN algorithm

This algorithm takes the input as the entire network. Number of nodes, links and the cost of each node is its input. It finds all the possible path from the source node to destination node. And also finds all the non-interfacing set in the network. Starting from the source node it traverses each node to find the destination node. Finds all the possible path that connects the source node and destination node. Outputs of this part of SASR algorithm are paths from source to destination, their cost and all the possible non-interfacing sets.

```
SASR-MIN
    1. Start from the source node.
    2. Traverse through the network to find the destination node.
    3. Save all possible path along with their cost.
```

4. Considering the range of each node find possible non-interfacing sets and save it.
5. Output the paths from source to destination, its cost and the non-interfacing set.

4.2 SASR-FF algorithm

This algorithm takes the output of the SASR-MIN algorithm to find the path with lowest cost on considering the concept of spatial reusability. It takes each path and traverse through it to find any element in non-interfacing set in it. If it finds a pair of non-interfacing nodes in the path, it combines the cost by only considering the highest cost among the non-interfacing nodes. Thus, it finds the new cost for all possible paths from source node to destination node. And compare the total cost of each path to find the new path with minimum cost.

SASR-FF

1. Take output from SASR-MIN algorithm.
2. Traverse through each path from source node to destination node to find if they have any pair from the non-interfacing set that obtained as the output of SASR-MIN algorithm.
3. On finding any pair of non-interfacing nodes in the path, combine the link costs of non-interfacing sets.
4. For that, find the highest link cost link cost from the non-interfacing set and include only that cost while calculating the total cost of the path.
5. Exclude the one with minimum link cost in non-interfacing set of nodes.
6. Compare between the new cost and select the one with minimum cost as the right path from source node to destination node.

V. EXPERIMENT AND RESULT

Here evaluated the performance of SASR_MIN and SASR_FF algorithm by using java as the front end and WampServer as the back end. Evaluation is done on the assumption that all the nodes use same transmission rate. Comparison between traditional Dijikstra's algorithm and proposed SASR algorithm is done here.

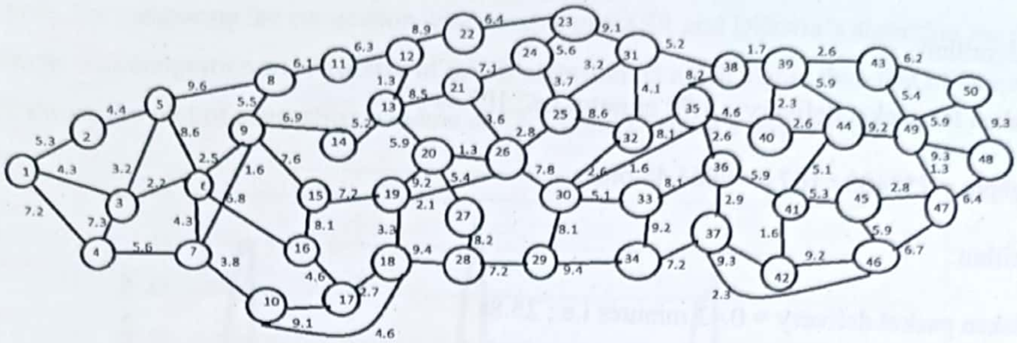


Fig 1. Typical network model

A network model of 50 nodes, Fig 1, is taken as the system model to execute the algorithms and evaluate its performance for different network parameters

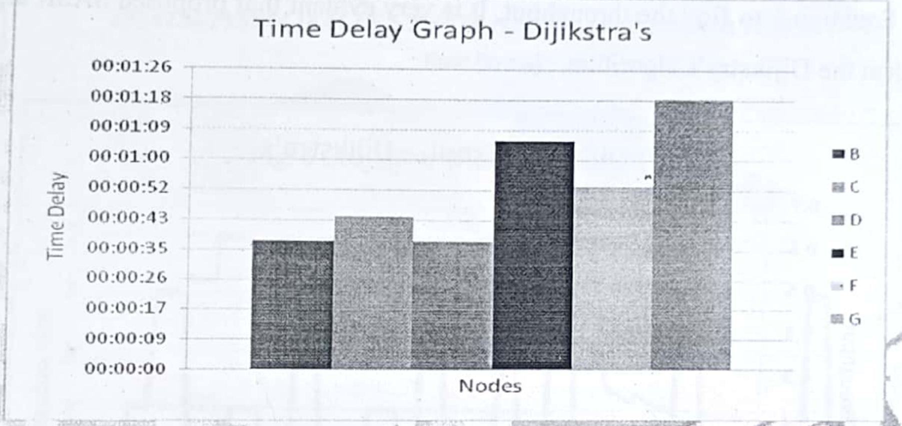


Fig 2. Packet delay measurement in Dijikstra's algorithm

Fig 2 and Fig 3 shows the graph plotted for Dijikstra's and SASR algorithm. Comparison is done on considering that both the algorithm transmits the same data from source to destination. The graphs are a plot of nodes in the X axis and delivery time in Y axis. As the same packet is being transferred from source to destination, the packet size become constant.

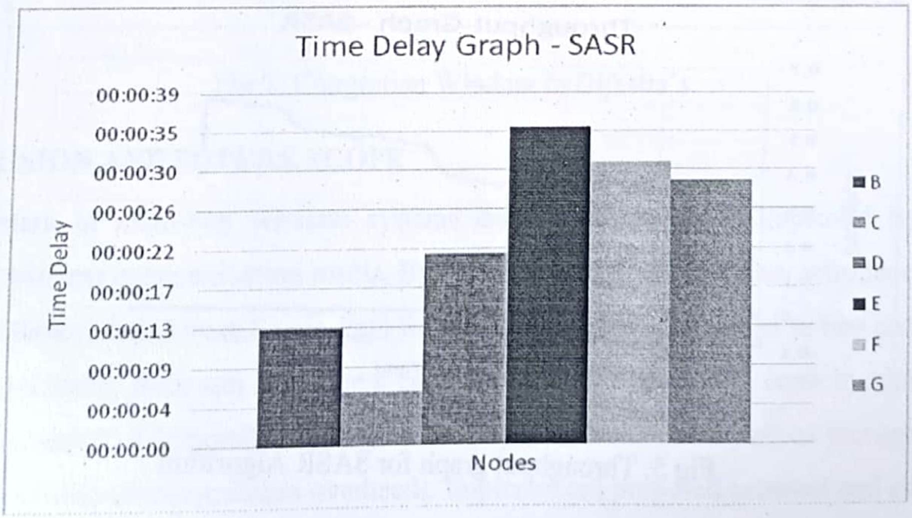


Fig 3. Packet delay measurement in SASR algorithm

Throughput = received size / time Equation 1

In Dijikstra's algorithm:

Time taken for packet delivery = 1.79 minutes i.e.; 107.4s

Throughput = 758400 / 107.4= 7061.45 bits/s

In SASR algorithm:

Time taken packet delivery = 0.43 minutes i.e.; 25.8s

Throughput = 758400 / 25.8 = 29395.34 bits/sec

For the above calculation same packet is transferred from source node to destination node. Node G is considered as the destination node. Packet size is 94.8 kb i.e.; 758400 bits. Packet delivery time is obtained from the Y axis of both graphs, as the value is in minutes it is converted to seconds. Then both the values are substituted to Equation 1 to find the throughput. It is very evident that proposed SASR algorithm yields high throughput than the Dijikstra's algorithm.

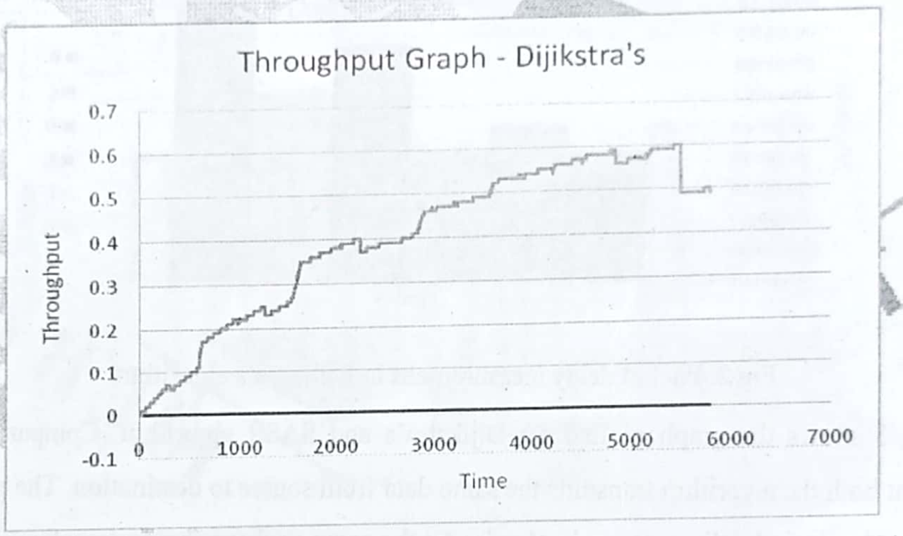


Fig 4. Throughput graph for Dijikstra's Algorithm

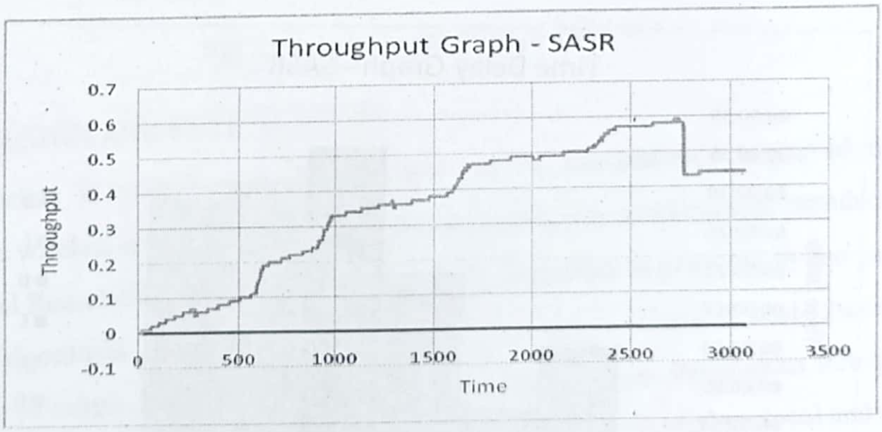


Fig 5. Throughput graph for SASR Algorithm

Congestion window size of a routing algorithm refers to number of packets that can be send simultaneously through a path. By comparing the congestion window size of SASR and Dijkstra's algorithm the result obtained shows that congestion window size of SASR algorithm is much higher than that of Dijkstra's. Fig. 6 and Fig.7 shows the plot of congestion window of SASR and Dijkstra's respectively.

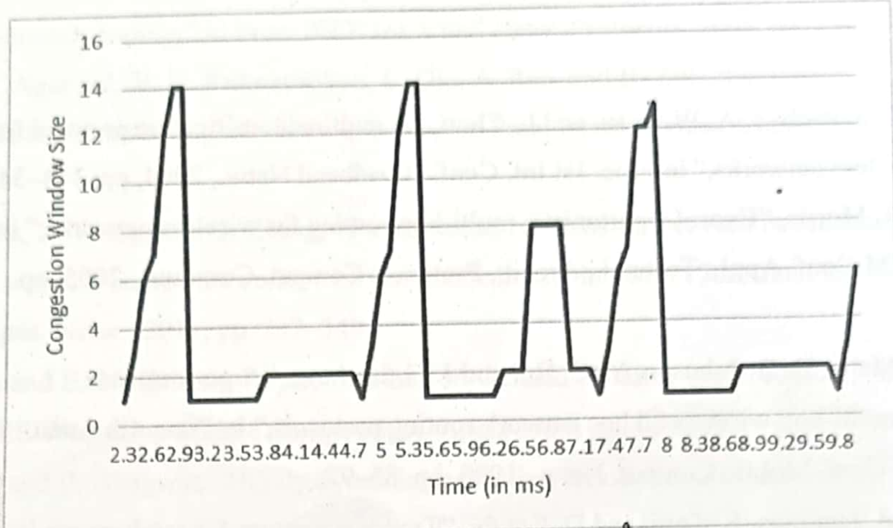


Fig. 6 Conjestion Window in SASR

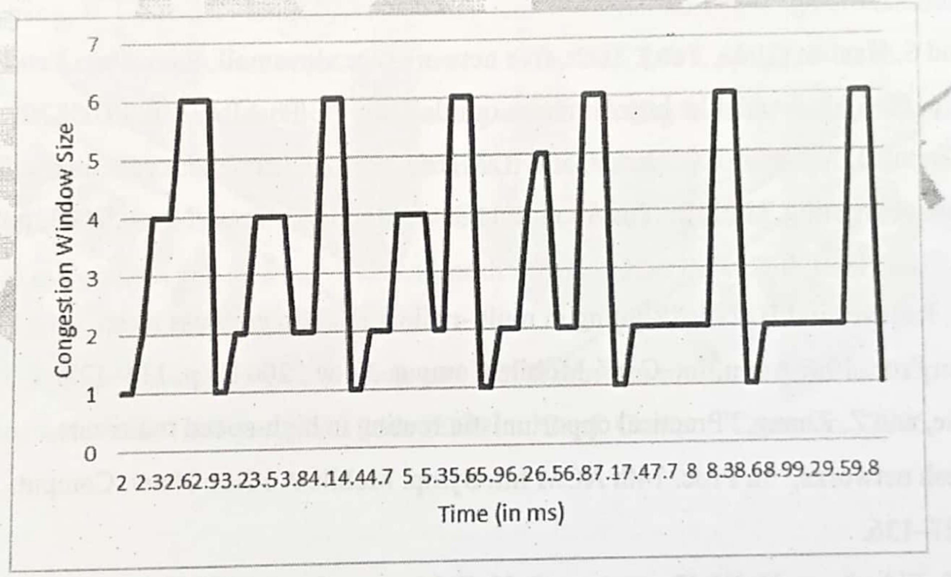


Fig 7. Congestion Window in Dijkstra's

VI. CONCLUSION AND FUTURE SCOPE

Different parameters in multi-hop wireless systems can be tremendously improved by using spatial reusability of the wireless communication media. By taking this into consideration, introduced an algorithm, SASR for Spatial Reusability-Aware Single-Path Routing. Algorithm is proposed in two parts: SASR_MIN and SASR_FF algorithms. Both sub algorithms combine to give a minimum cost- maximum end-to-end throughput path as output. Additional advantage of this system is that, tremendous throughput gains only require acceptable additional transmission overheads. Implemented proposed protocol and compared it with existing routing protocols. Assessment demonstrated that SASR algorithm achieved tremendous performance under higher data rates. As a future work, proposed system will be implemented in different constellation size and then evaluate and compare results with exiting protocols. Another direction is to incorporate selection of path with AI to get a more optimized path.

REFERENCES

[1] A. Adya, P. Bahl, J. Padhye, A. Wolman, and L. Zhou, "A multiradiounification protocol for IEEE 802.11 wireless networks," in Proc. 1st Int. Conf. Broadband Netw., 2004, pp. 344–345.

[2] S. Biswas and R. Morris, "Exor: Opportunistic multi-hop routing for wireless networks," in Proc. SIGCOMM Conf. Appl., Technol., Archit., Protocols Comput. Commun., 2005, pp. 133-144

[3] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. G. Jetcheva, "A performance Comparison of multi-hop wireless ad hoc network routing protocols," in Proc. 4th Annu. ACM/IEEE Int. Conf. Mobile Comput. Netw., 1998, pp. 85–97.

[4] S. Chachulski, M. Jennings, S. Katti, and D. Katabi, "Trading structure for randomness in wireless opportunistic routing," in Proc. SIGCOMM Conf. Appl., Technol., Archit. Protocols Comput. Commun., 2007, pp. 169–180.

[5] R. Cohen, and S. Havlin, (2003, Feb.). Scale-free networks are ultrasmall. Phys. Rev. Lett. [Online] 90, p. 058701. Available: http://link.aps.org/doi/10.1103/PhysRevLett.90.058701

[6] D. S. J. D. Couto, D. Aguayo, J. C. Bicket, and R. Morris, "A highthroughput path metric for multi-hop wireless routing," in Proc. 9th Annu. Int. Conf. Mobile Comput. Netw., 2003, pp. 134–146.

[7] R. Draves, J. Padhye, and B. Zill, "Routing in multi-radio, multihop wireless mesh networks," in Proc. 10th Annu. Int. Conf. Mobile Comput. Netw., 2004, pp. 114–128.

[8] W. Hu, J. Xie, and Z. Zhang, "Practical opportunistic routing in high-speed multi-rate Wireless mesh networks," in Proc. 14th ACM Int. Symp. Mobile Ad Hoc Netw. Comput., 2013, pp. 127–136.

[9] G. Jakllari, S. Eidenbenz, N. W. Hengartner, S. V. Krishnamurthy, and M. Faloutsos, "Link. positions matter: A noncommutative routing metric for wireless mesh network," in Proc. IEEE 27thConf. Comput. Commun., 2008, pp. 744–752

[10] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," Mobile Comput., vol. 353, pp. 153–181, 1996.

[11] N. M. Jones, B. Shrader, and E. Modiano, "Optimal routing and scheduling for a simple network coding scheme," in Proc. INFOCOM, 2012, pp. 352–360.

[12] T.-S. Kim, J. C. Hou, and H. Lim, "Improving spatial reuse through tuning transmit power, carrier sense threshold, and data rate in multihop wireless networks," in Proc. 12th Annu.

Int. Conf. Mobile Comput. Netw., 2006, pp. 366–377.

[13] R. P. Laufer, H. Dubois-Ferri_ere, and L. Kleinrock, "Multirate anypath routing in wireless mesh networks," in Proc. INFOCOM, 2009, pp. 37–45.

[14] Y. Lin, B. Li, and B. Liang, "Codeor: Opportunistic routing in wireless mesh networks with segmented network coding," in Proc. IEEE Int. Conf. Netw. Protocols, 2008, pp. 13–22.

[15] J. Padhye, S. Agarwal, V. N. Padmanabhan, L. Qiu, A. Rao, and B. Zill, "Estimation of link interference in static multi-hop wireless networks," in Proc. Internet Meas. Conf., 2005, p. 28

[16] S. Zhao, L. Fu, X. Wang, and Q. Zhang, "Fundamental relationship between nodedensity and delay in wireless ad hoc networks with unreliable links," in Proc. 17th Annu. Int. Conf. Mobile Comput. Netw., 2011, pp. 337–348.

[17] C. E. Perkins and E. M. Belding-Royer, "Ad-hoc on-demand distance vector routing," in Proc. 2nd IEEE Workshop Mobile Comput.Syst. Appl., 1999, pp. 90–100.

[18] C. E. Perkins and P. Bhagwat, "Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers," in Proc. Conf. Commun. Archit., Protocols Appl., 1994,pp. 234–244.

[19] M. Pan, C. Zhang, P. Li, and Y. Fang, "Joint routing and link scheduling for cognitive radio networks under uncertain spectrum supply," in Proc. INFOCOM, 2011, pp. 2237–2245.

[20] J. Zhang, H. Wu, Q. Zhang, and B. Li, "Joint routing and scheduling in multi-radio multi-channel multi-hop wireless networks," in Proc. BROADNETS, 2005, pp. 678–687.

[21] K. N. Ramachandran, E. M. Belding, K. C. Almeroth, and M. M. Buddhikot, "Interference-aware channel assignment in multiradiowireless mesh networks," in Proc. 25th IEEE Int. Conf. Comput. Commun., 2006, pp. 1–12.

[22] H. Zhai and Y. Fang, "Physical carrier sensing and spatial reuse in multirate and multihop wireless ad hoc networks," in Proc. IEEE 25th IEEE Int. Conf. Comput. Commun., 2006, pp. 1–12.

IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 1)
Available online at www.ijariit.com

Improving End-to-End Throughput in Wireless Network Using Spatial Reusability

Athira Manikuttan
athiramanikuttan01@gmail.com
Mangalam College of Engineering, Ettumanoor, Kottayam, Kerala

Vinodh P Vijayan
vinodh.pvijayan@mangalam.in
Mangalam College of Engineering, Ettumanoor, Kottayam, Kerala

Neena Joseph
neena.joseph@mangalam.in
Mangalam College of Engineering, Ettumanoor, Kottayam, Kerala

ABSTRACT

The optimal route from the source node to the destination node that guarantees a high end-to-end throughput is the main issue of routing in multi-hop wireless network. As the environment is heterogeneous the issue seems to be much complex, most of the solutions end with local optimum because those algorithms mostly fail to ensure an end to end throughput. By considering spatial reusability of wireless media, the end-to-end throughput in wireless multi-hop remote systems can be enhanced massively. To support the argument, Spatial-reusability Aware Single-path Routing (SASR) algorithm is proposed and compared with existing single path routing protocol. The assessment showed that proposed protocol show significant improvement in end-to-end throughput in comparison with existing protocols.

Keywords: *Wireless Network, Spatial Reusability, Routing.*

1. INTRODUCTION

Because of the constrained limit of wireless communication media, and lossy wireless connection [16], it is imperative to a great degree to choose a path that augments the end-to-end throughput, particularly in multi-hop wireless network. A principle issue with existing wireless routing protocol is that limiting the number of transmissions to convey a single packet from source node to destination node does not rely on augmenting the end-to-end throughput [4].

This paper examines routing protocol in single path routing. The goal of single path routing is to choose a cost-limiting path along which the packets are conveyed from the source node to destination node. A large portion of existing protocols links quality aware routing. They just select the path that limits the overall transmission count or transmission time for transmitting the packet.
An important property of wireless communication media which differentiate it from wired communication media is the spatial reusability. Wireless signal loses its energy through each hop [2]. Therefore, two links can be used at same time, if they in the far distance. But existing protocols do not take this into consideration.

2. RELATED WORK

In this area, a quick review of related work is done. And also compare our work with these and briefly review other works that consider reusability.

There is various work on wireless routing metrics. For single path routing a few link equality aware measurements [1][6][7][9] are proposed. RTT [1] measured the cost of the single wireless link by the round trip delay of probe packets. ETX [6] allocated the link cost with its normal number of transmission to effectively convey a packet. Based on ETX the author in [9] outlined ETOP metric considering the connection genuine position on the way.

The early single path routing protocols [3] [10] [17] [18] applied Dijikstra's algorithm for selecting a route. Some current cross-layer approaches mutually consider routing and also link scheduling eg [11] [19] [20], Zhang et al [20] detailed joint routing and planning into an enhancement issue and tackled the issue with a segment age technique. Skillet et al [16] managed to the joint issue in subjective ratio systems considering the opening of authorized groups.

PRINCIPAL
MANGALAM COLLEGE OF ENGINEERING
Ettumanoor

The calculations proposed in this work don't require any scheduling and the SASR calculations can be actualized in a disseminated way. In [21] the authors consider the exchange between spatial reuse and information rate, proposed a decentralized power and rate control calculation for higher system limit Zhai and Fany [22] researched the ideal bearer detecting range for throughput augmentation.

3. SYSTEM MODEL

Consider a static multi-hop wireless network with N nodes. Assume that the nodes have same transmission rate and do not have any power control constraint in this work.

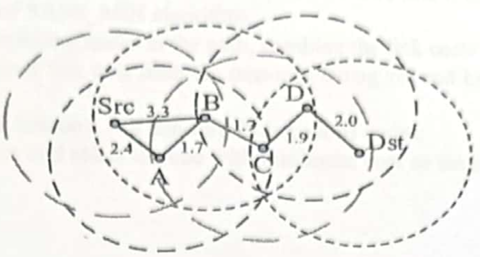


Fig 1. Importance of Spatial Reusability

Fig 1 shows a network with 6 nodes and each node's range is also shown. Each node's range is denoted by the circle with the node in its center. Each link is given an arbitrary cost. As wireless signal losses its energy in its prorogation, two wireless links can be worked at the same time, if they are far away from each other [13] [14]. If any pair of the nodes is out of the interfacing range of each other, we call it non-interfacing set I and a non-interfacing set can work at the same time [15].

Let's use an example from Fig 1. To represent the significance of spatial reusability of the correspondence media in single-path directing in a wireless system. Here we have four middle nodes (A, B, C, D) between source and destination. The dashed circle around each node demonstrate the range of the node. The cost is set apart close to each of the wireless link. There are two ways to reach the destination (Dst) from the source (Src).

Way 1: Src – B – C – D – Dst
Way 2: Src – A – B – C – D – Dst
In Way 1 cost is: 3.3+1.7+1.9+2.0 = 8.9
In Way 2 cost is: 2.4+1.7+1.7+1.9+2.0 = 9.7

Since Way 1 has lower cost it is likely to select it as the best path.

But considering the spatial reusability, we can see in Way 2, the link Src – A and link D – Dst are out of range of each other, and can work at the same time. It is important to combine spatially non-interfacing links while doing the path determination. By combine cost, we imply that cost of the non-interfacing set can be considered as single. On selecting a path with Src – A and D – Dst together, instead of adding both the cost, we select the one with higher cost only. So now the total cost of Way 2 can be lower to 7.7 which is less than the total cost of Way 1 i.e.; 8.9.

4. SPATIAL REUSABILITY AWARE SINGLE PATH ROUTING

We initially consider the spatial reusability-aware path cost assessment for single-path routing. Given each of the paths found by a current source routing algorithm (e.g., DSR [10]), our SASR calculation ascertains the spatial reusability aware path cost of it. At that point, the way with the small cost can be chosen.

The total SASR algorithm is proposed in two parts.

- SASR_MIN Algorithm
- SASR_FF Algorithm

4.1 SASR_MIN Algorithm

This algorithm takes the input of the entire network. A number of nodes, links and the cost of each node are its input. It finds all the possible path from the source node to destination node. And also finds all the non-interfacing set in the network. Starting from the source node it traverses each node to find the destination node. Finds all the possible path that connects the source node and destination node. Outputs of this part of SASR algorithm are paths from source to destination, their cost, and all the possible non-interfacing sets.

Algorithm

- Start from the source node.
- Traverse through the network to find the destination node.
- Save all possible path along with their cost.
- Considering the range of each node find possible non-interfacing sets and save it.
- Output the paths from source to destination, its cost and the non-interfacing set.

4.2 SASR_FF Algorithm

This algorithm takes the output of the SASR_MIN algorithm to find the path with the lowest cost of considering the concept of spatial reusability. It takes each path and traverses through it to find any element in non-interfacing set in it. If it finds a pair of non-interfacing nodes in the path, it combines the cost by only considering the highest cost among the non-interfacing nodes. Thus it finds the new cost for all possible paths from the source node to destination node. And compare the total cost of each path to find the new path with minimum cost.

Algorithm

- Take the output from SASR_MIN algorithm.
- Traverse through each path from source node to the destination node to find if they have any pair from the non-interfacing set that obtained as the output of SASR_MIN algorithm.
- On finding any pair of non-interfacing nodes in the path, combine the link costs of non-interfacing sets.
- For that, find the highest link cost link cost from the non-interfacing set and include only that cost while calculating the total cost of the path.
- Exclude the one with minimum link cost in a non-interfacing set of nodes.
- Compare between the new costs and select the one with minimum cost as the right path from source node to destination node.

5. EVALUATION

Here evaluated the performance of SASR_MIN and SASR_FF algorithm by using Java as the front end and wampserver as the back end. Evaluation is done on the assumption that all the nodes use same transmission rate. Comparison between traditional Dijikstra's algorithm and proposed SASR algorithm is done here.

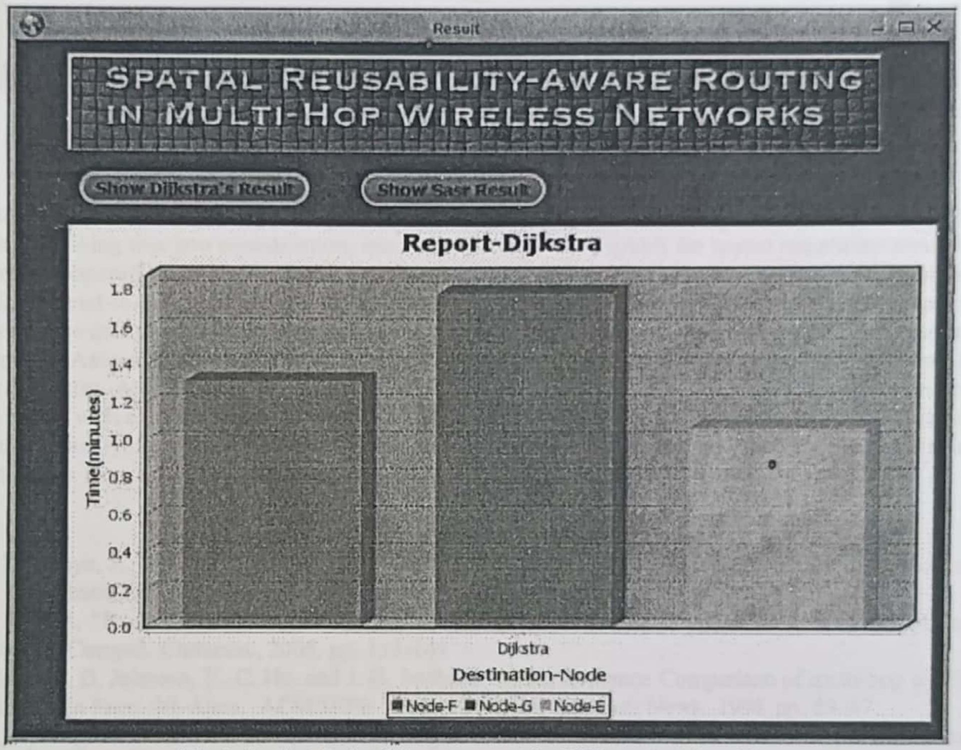


Fig 2. Packet Delay Measurement in Dijikstra's Algorithm

Fig 2 and Fig 3 shows the graph plotted for Dijikstra's and SASR algorithm. The comparison is done by considering that both the algorithm transmits the same data from source to destination. The graphs are a plot of nodes in the X-axis and delivery time in Y-axis. As the same packet is being transferred from source to destination, the packet size becomes constant.

Throughput = received size / time Equation 1

In Dijikstra's algorithm:

Time taken for packet delivery = 1.79 minutes i.e.; 107.4s

Throughput = 758400 / 107.4= 7061.45 bits/s

In SASR algorithm:

Time taken packet delivery = 0.43 minutes i.e.; 25.8s

Throughput = 758400 / 25.8 = 29395.34 bits/sec

For the above calculation same packet is transferred from source node to destination node. Node G is considered as the destination node. Packet size is 94.8 kb i.e.; 758400 bits. Packet delivery time is obtained from the Y-axis of both graphs, as the value is in minutes it is converted to seconds. Then both the values are substituted by Equation 1 to find the throughput. It is very evident that proposed SASR algorithm yields high throughput than he Dijikstra's algorithm.

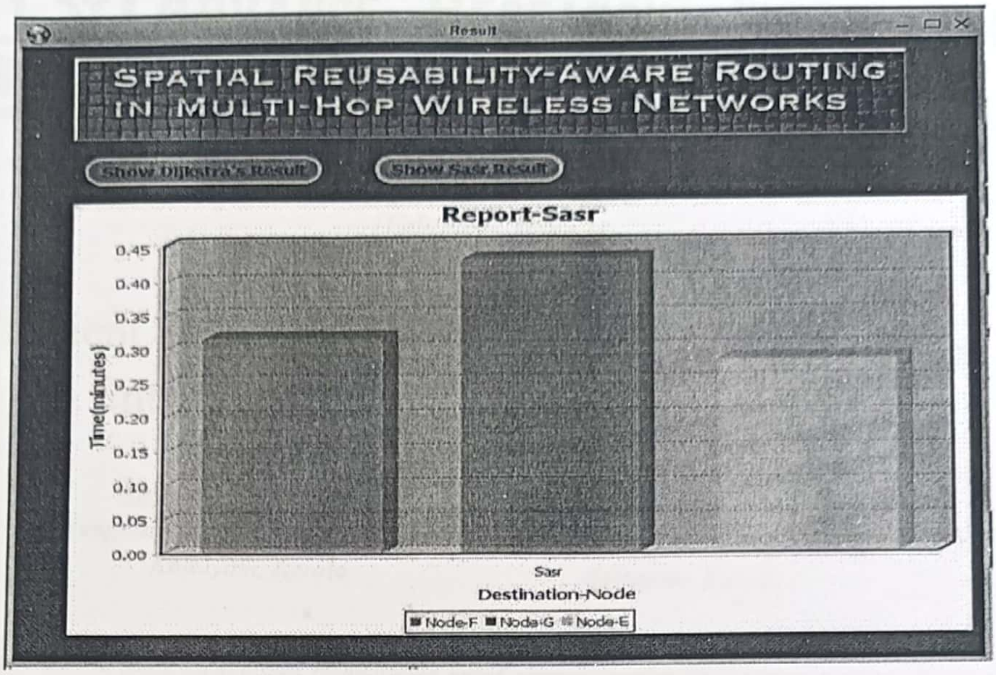


Fig 3. Packet Delay Measurement in SASR Algorithm

6. CONCLUSION AND FUTURE SCOPE

End-to-end throughput in multi-hop wireless systems can be tremendously improved by using spatial reusability of the wireless communication media. By taking this into consideration, introduced an algorithm, SASR for spatial reusability-aware single-path routing. The algorithm is proposed in two parts: SASR_MIN and SASR_FF algorithms. Both sub-algorithms combine to give a minimum cost- maximum end-to-end throughput path as output. An additional advantage of this system is that tremendous throughput gains only require acceptable additional transmission overheads. Implemented proposed protocol and compared it with existing routing protocols. Assessment demonstrated that SASR algorithm achieved more noteworthy end-to-end throughput increase under higher data rates. As a future work, the proposed system will be implemented in different constellation size and then evaluate and compare results with exiting protocols. Another direction is to further explore opportunities to improve the performance of our routing algorithms by analyzing special underperforming cases identified in the evaluation. Another direction is to incorporate a selection of path with AI to get a more optimized path.

7. REFERENCES

[1] A. Adya, P. Bahl, J. Padhye, A. Wolman, and L. Zhou, "A multi-radio unification protocol for IEEE 802.11 wireless networks," in Proc. 1st Int. Conf. Broadband Netw., 2004, pp. 344–345.

[2] S. Biswas and R. Morris, "Exor: Opportunistic multi-hop routing for wireless networks," in Proc. SIGCOMM Conf. Appl., Technol., Archit., Protocols Comput. Commun., 2005, pp. 133-144

[3] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. G. Jetcheva, "A Performance Comparison of multi-hop wireless ad hoc network routing protocols," in Proc. 4th Annu. ACM/IEEE Int. Conf. Mobile Comput. Newt., 1998, pp. 85–97.

[4] S. Chachulski, M. Jennings, S. Katti, and D. Katabi, "Trading structure for randomness in wireless opportunistic routing," in Proc. SIGCOMM Conf. Appl., Technol., Archit. Protocols Comput. Commun., 2007, pp. 169–180.

[5] R. Cohen, and S. Havlin, (2003, Feb.). Scale-free networks are ultrasmall. Phys. Rev. Lett. [Online] 90, p. 058701. Available: http://link.aps.org/doi/10.1103/PhysRevLett.90.058701

[6] D. S. J. D. Couto, D. Aguayo, J. C. Bicket, and R. Morris, "A high throughput path metric for multi-hop wireless routing," in Proc. 9th Annu. Int. Conf. Mobile Comput. Netw., 2003, p 134–146.

[7] R. Draves, J. Padhye, and B. Zill, "Routing in multi-radio, multihop wireless mesh networks," in Proc. 10th Annu. Int. Conf. Mobile Comput. Netw., 2004, pp. 114–128.

[8] W. Hu, J. Xie, and Z. Zhang, "Practical opportunistic routing in high-speed multi-rate Wireless mesh networks," in Proc. 14th ACM Int. Symp. Mobile Ad Hoc Netw. Comput. 2013, pp. 127–136.

[9] G. Jakllari, S. Eidenbenz, N. W. Hengartner, S. V. Krishnamurthy, and M. Faloutsos, "Link. Positions matter: A noncommutative routing metric for a wireless mesh network," in Proc. IEEE 27thConf. Comput. Commun., 2008, pp. 744–752

[10] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," Mobile Comput., vol. 353, pp. 153–181, 1996.

[11] N. M. Jones, B. Shrader, and E. Modiano, "Optimal routing and scheduling for a simple network coding scheme," in Proc. INFOCOM, 2012, pp. 352–360.

IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 1)
Available online at www.ijariit.com

An Efficient Security Key for Practical Requirement of PIN Entry Protection Section Authentication

Kiren Vijai
kiren.vijai@gmail.com
Mangalam College of Engineering,
Kottayam, Kerala

Neena Joseph
neena.joseph@mangalam.in
Mangalam College of Engineering,
Kottayam, Kerala

ABSTRACT

Clients regularly reuse the same customized recognizable proof numeric system for various sessions. Coordinate numeric sections can be profoundly powerless for the bear to break assaults and assailants can successfully watch PIN section with covered cameras. Backhanded PIN passage techniques proposed as countermeasures are seldom conveyed on the grounds that they request a heavier subjective workload for clients. To accomplish security and ease of use and display a useful aberrant PIN section technique called SteganoPIN. It has two main numbered systems, first is the secured, the second one is unclosed. Intended objectively for looking someone's shoulder's over direct observation of the hidden cameras. In the wake of finding a long haul PIN in the more run of the mill design, secured numeric system, client produces an OTP to securely come on the display assailants. The test control utilized an inside subject factorial outline with two autonomous factors- PIN section framework, recognized proof numeric write. The slow passage of distinguishing numeric system time however approved. The disguised numeric system is flexible to the direct observation over looking someone's shoulder through unseen camera assaults by different confirmation class.

Keywords: *Security, Shoulder-Surfing, Human – Machine Interface, Personalized Identification Number, OTP.*

1. INTRODUCTION

Individual ID numbers (PINs), normally developed also, remembered, and are generally utilized as numerical passwords for client verification or different opening purposes. Their application is expanding on the grounds that advanced touchscreens can encourage helpful usage for numeric key passage boundary, an assortment of item devices, gadgets, smart phones, computerized entryway machine lock, cell phones, and PCs with locking system. Shockingly, client straightforwardly used mystery numeric number system frameworks, to ensure more protection is effortlessly bargained, especially out in the open spots. Close-by individuals can watch PIN section by a bear attack through covered cameras [1], [2], [28]. Unseen cameras are placed by the assailant is characterized as a frail enemy who has no programmed account gadget, however, may utilize manual instruments [3].

The conceptual and subjective abilities of human-just assailants are restricted for some people [4]. Hidden cameras are placed at the top of the building by the assailant can be characterized for more grounded foe helped by a programmed recording device, for example, a camera is used to placed for tap someone's individual id number and dissect whole exchanges viably through large distance [2]. In addition, enemies can be effectively attacked through assaults, gathered various numeric individual numbers of the applicants to endeavor through mimic a client. Dynamic speculating aggressors are the enemy whose endeavors surmise through the numeric individual numbered applicants. Includes the aggressor be turn out to be all the more capable and rehashes camera-based perception of a similar client and framework [5]. Remotely associated perception is additionally turning into a worry since high-determination cameras are being circulated and arranged out in the open spots [6], [7].

The current pattern of focusing on assaults through appearance to tap PCs allows rehashed direct observation of the shoulder surfing assaults an undeniably sensible risk to the PIN client interface. The quantity of numeric individual number system hopefuls allows stable adequately extensive through decrease data spillage regardless of whether a client's PIN passages are more than once saw by foes. Indeed, even incomplete data spillage could be destructive in light of the fact that clients regularly reuse indistinguishable or if nothing else comparable PINs for different frameworks. Moreover, a token or potentially ID frequently joined through the numeric individual number be hacked by the attackers then again enemies utilizing the numeric individual number of the applicants [8], [9]. Accordingly, the mystery of numeric individual numbered system can be bargained, the client would present the numerous ruptures of protected applicant's individual numeric numbers.

2. RELATED WORKS

To manage the nontechnical assaults [1], one successful mediation by UI [10]. Primary angle can consolidate backhanded numeric section scales isolated through noticeable numeric passage over the mystery of the PIN. Prior the mystery of the PIN examined subjective validation inside the restrictions of people. BinaryPIN has utilized twice hues over backhanded numeric passage through strategy [3]. Every step, framework hued an irregular portion of the numbered system would be dark, another one is for the clients would move the shade over numeric individual number through squeezing different shading numeric number. Different steps are move on the solitary numeric number system, what's more, rehashed until the point that the numeric number systems are move on to exist. Introduced curved frame touch is used in unique keys [11]. Here, large haul mystery will move the symbols, an arbitrary test utilized various irregular found symbols including both pass and phony symbols. For confirmation, clients made a psychological picture of a curved body connecting pass-symbols and entered inner side amid various steps. Psychological validation conspires over the numeric individual numbered system is used [12]. An arbitrary test has an arrangement over graphical images such as watchword, arbitrarily masterminded over the PCs. Clients followed the virtual way in view of the secret word such as graphical images placed in the PC's, move on the goal esteem in numerous steps. Here, exhibited Color PIN can utilize an arrangement of hued characters as an irregular test doled out of the numbered system to be used [13]. Every cycle, thrice diverse shaded strings and symbols are allowed through the individual numbered system was copied thrice individual numbered id can be used various hues. The Color PIN, the mystery of the numeric numbered system were really shading numbered mixes. Clients have moved mystery hued strings on the numeric numbered id utilizing different strings console over and again until the point when the entire numeric keys are used. Significant worries whose strategies are longer confirmation issues are provided and larger keys are used to recall. Additionally, various problems are raised [4], [14] - [16].

The previous job is utilized over utilization through the assistant undetectable network, constrain information accessible to shoulder surfers [16]. Uncovered isolating (imperceptible) material difficulties and (noticeable) graphical difficulties and depending on people's various tactile contributions for a graphical secret word presented Sasamoto et al. [17]. A particular haptic gadget was outlined: a client set one hand on a power criticism trackball to detect the material test and, in view of it, utilized another one is, enter a brief description to identify mystery picture through phony pictures through the visual test. The attributes of the system which utilized varieties of signs an arbitrary test move on a client's confided in cell phone [18]. A client move on the numeric identical system is used in a different system without a vibration sign however a phony (arbitrary) system is used to prompt the cell phone [19] - [21] contemplated a few numeric numbered passage techniques over the assistant network. Fundamental UI was a vacant numeric number cushion has not been imagining the numbered esteems. For locking the phone, clients have unfilled numbers for the cushion is used to see the numeric numbered an incentive to sound digits, material checks. Clients rehashed this choice advance until the point that seeing a numeric individual number to entered every stage. The mystery of the numeric individual id bearing number blends. Clients continued turning the wheel cushion in mystery headings until the point that seeing the PIN key by checking sound or material signals. At that point, they discharged the hand for the move on the individual numbers in every step. Clients have shading numbers, requesting numbers foreordained request the numeric keys to see options. Bianchi et al. talked about the clockwise amplifier, the comparative gadget is the reasonable risk for the helper network plans [22] revealed the absence of the problems of the channel misusing the client's character attributes, conceivable convergences over numerous arbitrary difficulties.

3. EXISTING SYSTEM

A Leakage Resilient Password System is basically a test reaction convention between human and PC and is represented as an individual called the client, PC called the owner. Client, owner concur the main mystery, for the most part, alluded to the secret word. The main problem of this is to someone who guesses the PIN. Client mainly makes to produce reactions demonstrate the personality to guess the PIN by the attackers. Mocking someone's individual id number. Not at all like customary watchword frameworks, a reaction in LRPS is a muddled message got from the root mystery, as opposed to the plaintext of the root mystery itself. With the direct observation of someone who is looking shoulders through the unseen cameras. Thinking about the restricted intellectual abilities of unaided people, a usable confusion work is typically an individual that mocks to take someones individual numeric id number. Appropriate response test expands achievement over speculating assault the enemy endeavors go for confirmation over arbitrarily mocking the right PIN appropriate response test. Hence, a verification of these frequently makes different stages of test reaction system keeping in mind the end goal to achieve a normal validation quality. The security quality of an LRPS is characterized as the protection against these two nonexclusive assaults given a similar achievement rate of irregular speculating. The foe continues evacuating insignificant competitors when an ever-increasing number of prompts are accessible. Its technique can be depicted as takes after. List every conceivable possibility for the secret key in the objective framework. Every attack is a type of assault has stick whenever, anyplace individuals, innovation. Over the long haul, our lives will turn out to be increasingly digitized. Despite everything have a name yet an uncommon mark, numeric, id been likewise decidedly recognize the problems. More mechanical developments have gradually been brought the present society. Expansive larger parts of individuals are grasping new contraptions, a large problem that arises to the society. It helps winding up many advantageous, little tedious. Be that as it may, it likewise realizes an expansion of problems. Shoulder surfers are people whose choose helpless result endeavor data got through individual looking over shoulders in the direct observation. Possibly take somebody's character or upset somebody's personality or appropriate to protection. Mechanical advancements can be awesome anyway, one must be additional careful while using them. For every free perception of a test reaction state, looks legitimacy over every hopeful to present applicant confirmation calculation utilized, expel fake competitors over applicant test. The above methodology demonstrates that the productivity of candidate in the spillage versatility dependent just constrained to measure over applicant test. Acquaint twice articulations with additionally portray the energy of savage power assault. These announcements apply to root mystery, as well as to round insider facts when the enemy can dependably aggregate the perceptions for individual round mystery.

4. PROPOSED SYSTEM

Inscribe the attacks of assaults by different validation class, furthermore relocate clients officially acquainted with the standard PIN section framework, a new numeric identification individual passage strategy is utilized. Framework expands over the idea to test reaction through UI [10], [25], [28], protecting the security and privacy [23], [24], [28] for propelling through accompanying objectives over Stick aimed verification. Many of utilize general individual identification number section and cause restricted increments to the numeric identification number section and occur incorrect mistakes. Exceed to expand the large length of the haul customized identification number and remain inside transient prerequisites over customer's constraints, [26], [27], [28]. More versatile for shoulder surfing assaults by numerous validation class and oppose dynamic speculating assaults without permitting more preferred standpoint than arbitrary speculating. Tricky Numeric Keys are used and an essential UI first is the individual numbered identification keys a normal format, the second one represents little an irregular design. Irregular design numeric key known as test numeric keys. The client must utilize this test keypad to determine a new OTP, the client initially finds a long haul PIN in customary format and in this manner checks the numeric numbered areas for the test system to password determination. A client at that point to move on the password to consistent format system implies the reaction system. Here two keypad systems are used. One is a normal design another one is an irregular design. UI of the test system cannot show up quickly, just the reaction keypad shows up in its consistent format. This framework rather shows the little circle of 20 mm (0.787) width. It demonstrates the test keypad just when a client glasses a finger over hover to hold like circle shut to the shape of ρ. The test keypad at that point appears after a little postponement and vanishes instantly when the client discharges the measured hand. Utilizing this method, the human client and the machine framework can intelligently ensure the test keypad by outwardly impeding to foes. Little test size over the system could likewise add graphical impediment through influencing client. By and large, SteganoPIN fulfills solid security objectives. That is, it is more useful for the protection of the security and is more capable to protect the individual identification number to be secured. When the PIN is entered in the irregular pattern system suddenly send a message to the owner's smartphone and also send a mail to the owner's mail id. It is more useful to the society if the framework is legitimately introduced and utilized. It is secure against dynamic speculating assaults.

5. RESULT

Numeric individual identification passage is more fruitful for authentication, section frameworks to blend in an irregular (framework picked) or client picked customized id number. Standard passage of the framework is fundamentally quicker. Found no other noteworthy principle or collaboration impacts. In general, the standard Stick framework outflanked SteganoPIN in PIN section time paying little heed to PIN composes, as anticipated. When the PIN is entered in irregular pattern system immediately send a message to the owner's smartphone and a mail is also sent to the owner emailed. In the more drawn out term, irregular utilize instance of client the picked numeric identification id number, cannot huge distinction to the numeric identification numbered section of these network channel.

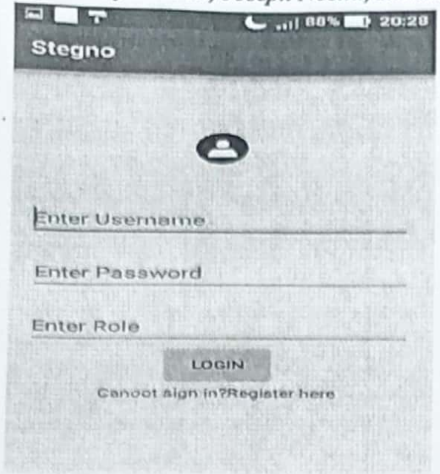


Chart 1: Home Page

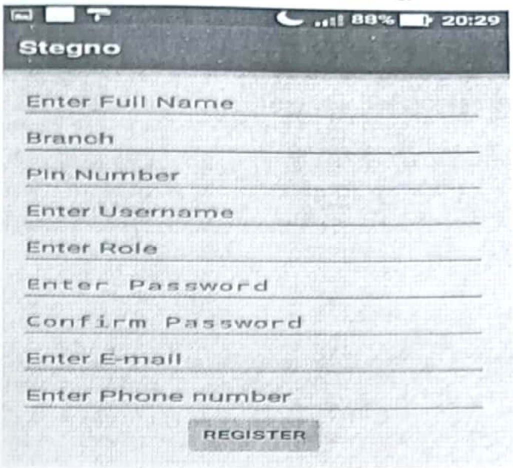
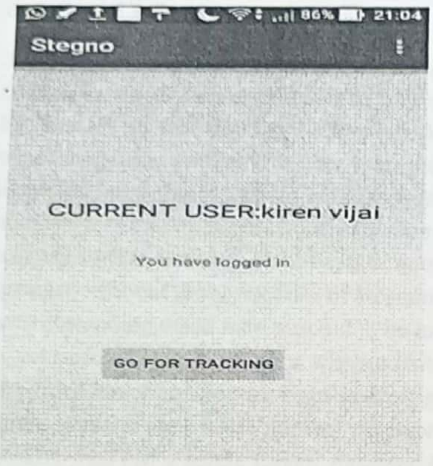


Chart 2: Registration Page



CURRENT USER:kiren vijai

You have logged in

Chart 3: Tracking the User

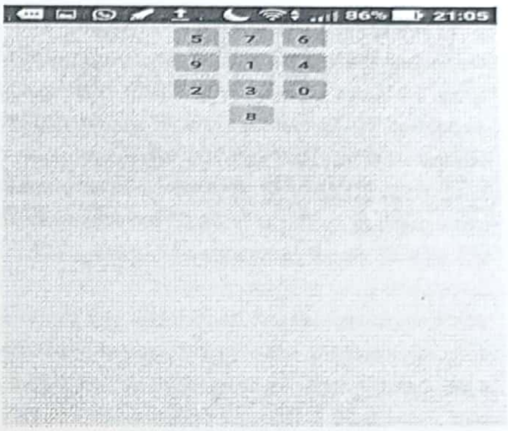


Chart 4: Irregular Pattern Numeric Key

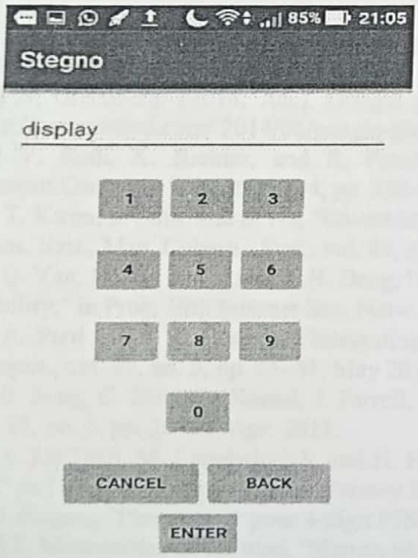
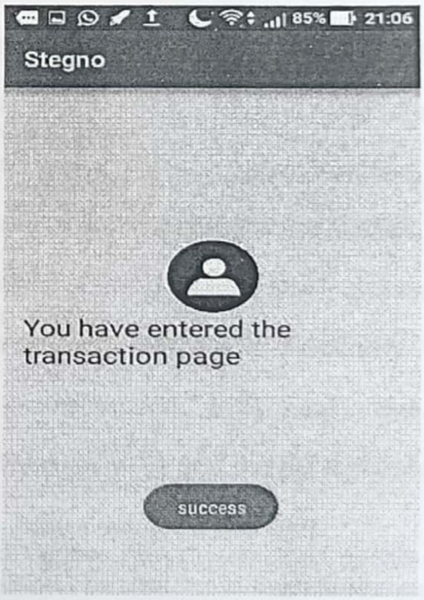
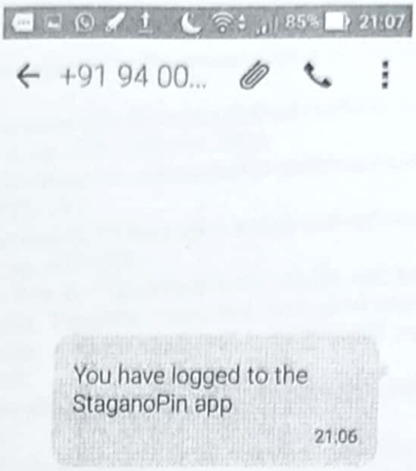


Chart 5: Normal Numeric Key Pattern



You have entered the transaction page

Chart 6: Entered the Transaction Page



You have logged to the StaganoPin app

21:06

Chart 7: A Message is Send to the Owners Mobile

6. CONCLUSION

The PIN section strategy ready to accomplish both great security and down to earth ease of use. The investigation and client contemplate both delivered comes about supporting the theories. In particular, it can assault by different verification class, the client legitimately utilized through the framework. The usability, simplicity for learning, and simplicity for control among OTP deduction were altogether evaluated higher than direct. The mistake rate in Stegano PIN was essentially not the same as the numeric identification number technique in discontinuous utilize work. Comprehended the outcome in originating to common sense over numeric identification password induction for contribution to entire numeric individual password endeavor. Thus provide more security for the numeric identification number and also provide more protection to the society. The outcomes firmly bolster the speculation about the ease of use of SteganoPIN. There was input from one member that senior individuals ought to favor this stance notwithstanding when they turn out to be more experienced. Casually, replayed this stance and understood that the test keypad was as yet undetectable to enemies without irritating the user. By and by, the client might have imperative give the alternative to pick one-sided hover position for right-and left-gave clients. Another fascinating conduct was that one right-gave member utilized just a single numeric individual number password to get more determination, passage. The conduct infers through a framework that worked with just a single finger. Assessed the decent conduct over the protection. These are mainly used to improve the security, protection of the system and also used for user authentication. Hence, by and large, the SteganoPIN framework is more proper to stationary frameworks, despite the fact that it can be given as a promising choice to versatile.

7. REFERENCES

[1] J. Long and J. Wiles, No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Boston, MA, USA: Syngress, 2008.

[2] A. Greenberg. (2014, Jun.). Google glass snoopers can steal your passcode with a glance," Wired. [Online]. Available: http://www.wired.com/ 2014/06/google-glass-snoopers-can-steal-your-passcode-with-a-glance/

[3] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," in Proc. ACM Comput.Common. Security, 2004, pp. 236–245.

[4] T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surfing: Human adversaries are more powerful than expected," IEEE Trans. Syst., Man, Cybern., Syst., vol. 44, no. 6, pp. 716–727, Jun. 2014.

[5] Q. Yan, J. Han, Y. Li, and R. H. Deng, "On limitations of designing leakage-resilient password systems: Attacks, principles and usability," in Proc. 19th Internet Soc. Netw. Distrib. Syst. Security Symp., 2012, pp. 1–16.

[6] A. Parti and F. Z. Qureshi, "Integrating consumer smart cameras into camera networks: Opportunities and obstacles," IEEE Comput., vol. 47, no. 5, pp. 45–51, May 2014.

[7] B. Song, C. Ding, A. Kamal, J. Farrell, and A. Roy-Chowdhury, "Distributed camera networks," IEEE Signal Process. Mag., vol. 28, no. 3, pp. 20–31, Apr. 2011.

[8] A. De Luca, M. Langheinrich, and H. Hussmann, "Towards understanding ATM security—A field study of real-world ATM use," in Proc. ACM Symp. Usable Privacy Security, 2010, pp. 1–10.

[9] J. Rogers, "Please enter your 4-digit PIN," Financial Services Technology, U.S. Edition, vol. no. 4, Mar. 2007.

[10] T. Matsumoto and H. Imai, "Human identification through an insecure channel," in Proc. Adv. Cryptol., 1991, pp. 409–421.

[11] S. Wiedenbeck, J. Waters, L. Sobrado, and J. C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in Proc. ACM Int. Working Conf. Adv. Visual Interfaces, 2006, pp. 177–184.

[12] D. Weinshall, "Cognitive authentication schemes safe against spyware," in Proc. IEEE Symp. Security Privacy, 2006, pp. 295–300.

[13] A. De Luca, K. Hertzschuch, and H. Hussmann, "Color PIN–Securing PIN entry through the indirect input," in Proc. ACM CHI Conf. Human Factors Comput. Syst., 2010, pp. 1103–1106.

[14] H. J. Asghar, S. Li, J. Pieprzyk, and H. Wang, "Cryptoanalysis of the convex hull click human identification protocol," in Proc. 13th Int. Conf. Inf. Security, 2010, pp. 24–30.

[15] P. Golle and D. Wagner, "Cryptanalysis of a cognitive authentication scheme," in Proc. IEEE Symp. Security Privacy., 2007, pp. 66–70.

[16] T. Kwon and J. Hong, "Analysis and improvement of a PIN entry method resilient to shoulder-surfing and recording attacks," IEEE Trans. Inf. Forensics Security, vol. 10, no. 2, pp. 278–292, Feb. 2015.

[17] H. Sasamoto, N. Christin, and E. Hayashi, "Undercover: authentication usable in front of prying eyes," in Proc. ACM SIGCHI Conf. Human Factors Comput. Syst., 2008, pp. 183–192.

[18] A. De Luca, E. von Zezschwitz, and H. Hussmann, "Vibrapass – secure authentication based on shared lies," in Proc. ACM CHI Conf. Human Factors Comput. Syst., 2009, pp. 913–916.

[19] A. Bianchi, I. Oakley, V. Kostakos, and D. Kwon, "The Phone Lock: Audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices," in Proc. 5th Int. Conf. Tangible, Embedded, Embodied Interaction, 2011, pp. 197–200.

[20] A. Bianchi, I. Oakley, and D. Kwon, "Spinlock: A single-cue haptic and audio PIN input technique for authentication," in Proc. Haptic Audio Interaction Design, 2011, pp. 81–90.

[21] A. Bianchi, I. Oakley, and D. S. Kwon, "Counting clicks and beeps: Exploring numerosity based haptic and audio pin entry," Interacting Comput., vol. 24, pp. 409–422, 2012.

[22] T. Perkovic, A. Mumtaz, Y. Javed, S. Li, S. A. Khayam, and M. Cagalj, "Breaking undercover: Exploiting design flaws and nonuniform human behavior," in Proc. 7th Symp. Usable Privacy Security, 2011, pp. 1–15.

[23] D. Kim, P. Dunphy, P. Briggs, J. Hook, J. W. Nicholson, J. Nicholson, and P. Olivier, "Multi-touch authentication on tabletops," in Proc. ACM SIGCHI Conf. Human Factors Comput. Syst., 2010, pp. 1093–1102.

[24] Q.Yan, J. Han,Y. Li, J. Zhou, and R.H.Deng, "Designing leakage-resilient password entry on touchscreen mobile devices," in Proc. 8th ACMSIGSAC Symp. Inform., Comput. Commun. Security, 2013, pp. 37–48.

[25] T. Kwon and S. Na, "SwitchPIN: Securing smartphone PIN entry with switchable keypads," in Proc. IEEE Int. Conf. Consumer Electron., 2014, pp. 27–28.

[26] N. Cowan, "The magical number 4 in short-term memory: A reconsideration of mental storage capacity," Behavioral Brain Sci., vol. 24, no. 1, pp. 87–114, 2001.

[27] G. A. Miller, "The magical number seven, plus or minus two: Some limits on our capacity for processing information," Psychol. Rev., vol. 101, no. 2, pp. 343–352, 1956.

[28] Taekyoung Kwon and Sarang Na, "SteganoPIN: Two-Faced Human–Machine Interface for Practical Enforcement of PIN Entry Security" IEEE Transactions on Human-Machine Systems, vol. 46, NO. 1, February 2016

BIOGRAPHIES

	Kiren Vijai **Student** Kiren Vijai is a post graduate student from Mangalam College of Engineering, affiliated to APJ Abdul Kalam Technological University, Kerala. She received her B.Tech from Mahatma Gandhi University in 2014.Her research interest includes Network Security, Data Mining, Cloud Computing.
	Neena Joseph **Assistant Professor** Neena Joseph is an Assistant Professor at Mangalam College of Engineering, affiliated to APJ Abdul Kalam Technological University, Kerala.She received her M.Tech from Manonmanian Sundaranar University, Tirunelveli in 2012.She is a researcher since 2012.Her main research interest is Data mining, Cloud Computing, Security, and Optimization in Compilers.

IJARIIT
INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 3)
Available online at: www.ijariit.com

Automatically mining query facet from search results using text mining algorithm

Soniya Joy
soniyajoy15395@gmail.com
Mangalam College of Engineering, Ettumanoor, Kerala

Neena Joseph
neena.joseph@mangalam.in
Mangalam College of Engineering, Ettumanoor, Kerala

ABSTRACT

A query facet can be considered as a single word or multiple words which summarize and describe that query. Query facets may provide direct information that users are seeking. The existing algorithms for generating query facet can be used by extracting the frequent list in search results. The coverage of facet item must be limited because the only small number of search results can be used. In order to solve this kind of problem in the proposed system uses the format of the list is more user-friendly. Query facet is analyzing the text query the query facet provides useful knowledge about a query. In existing algorithms are used the coverage of facet item must be limited in order to solve this kind of problem propose an algorithm text mining and use the knowledge base to improve the quality and the coverage of facet item. Text Mining algorithms are used to extract the relevant information from available text.

Keywords— Query facets, Text mining, Multi-faceted queries, Knowledgebase

1. INTRODUCTION

Query facet is a collection of items which summarized the content of a query. In conventional method the user can browse a webpage user can view many documents for the information they are seeking, this takes a lot of time and confused the user [6]. Here use an automatic summarization of search result will produce it will help the user to know about the query they are searching without browsing many web pages. Mining query facets is an approach to solve the above-explained problem using text mining algorithms to mine the query facet. Table 1 shows an example of query facet the query is "Beijing subway," is a place in a European country. Its query facets cover aspects of related country lines temple, important city etc. These query facets help users learn about the topic "Beijing subway" without browsing so many web pages.

Query facets are good summaries of a query and are useful for users to understand the query and help them explore information [1]. Existing algorithm like QD Miner, QF-I, QF-J has used automatically mine query facets by aggregating frequent lists contained in the results. The facet item is extracted as a top search result from a search engine. One problem can arise by using this kind of methods the coverage of facet mined can be limited [6].

Table 1. Example of query facet

Query	Beijing subway
1	line 1, line 2, line 4, line 5, line 10, line 13, batong line
2	xizhimen, jianguomen, dongzhimen chongwenmen
3	forbidden city, the temple of heaven, Tiananmen square

To solve this problem use a knowledge base as a data source to improve the quality of query facet. Knowledgebase contains structured information such as entities and properties of the related query [6]. A text mining algorithm can be used to mine the query facet. Text mining is also known as text analytics, is the process of deriving high-quality information from text. Text mining is a process to extract interesting and significant patterns to explore knowledge from textual data sources [4]. Text mining is a multi-disciplinary field based on information retrieval, data mining, machine learning, statistics, and computational linguistics [4].

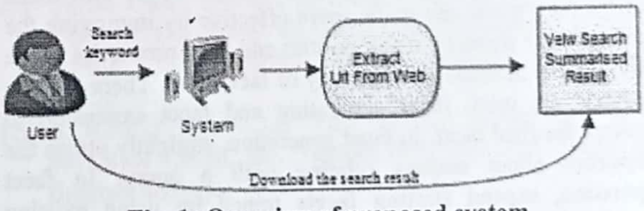


Fig. 1: Overview of proposed system

Figure 1 shows the overview of the proposed system. The user can search for a keyword by using the system. Then the URL of the search result is retrieved from the web and finally view the summarised search result and the user can download the search result. There are two methods are used to construct the final facet namely Facet Generation and Facet Expansion.

2. RELATED WORKS

Nowadays, search engines like Google have evolved to include in their results information from structured data sources along with text documents. These search engines provide a keyword search capability to their user. But, users are mainly interested in exploring a structured collection of information than a query for a specific item. A commonly used interaction for structured information is faceted search. Faceted search provides a more user-friendly visual alternative to keywords for the user to explore the structured results. Faceted search is a technique for accessing information organized according to a faceted classification system [3].

The search engine is an important tool for the user to search for information. Query facet a set of items which summarise the important aspects of a query. Query facets may provide direct information that users are seeking. Direct access to digital information has completely changed the rules, users can directly browse the information, without consulting any complex systems. The spread of digital access to information has been a sudden increase in the volume of information available about any given query. Many websites now provide even more refined tools to help users find information. Filters are one such tool to find information [1].

Search queries are multi-faceted, which makes a simple ranked list of results. To finding information for such faceted queries, browse a technique that explicitly represents the facets of a query using groups of semantically related terms. Query facets can help users to find topics of the search results by applying multiple faceted. Construct a supervised method based on a graphical model for query facet extraction. The graphical model learns how a candidate term is to be a facet term as well as how likely two terms are to be grouped together in a query facet and captures the dependencies between the two factors [7].

3. PROPOSED SYSTEM

Search engines currently have become the vital tools for web users to locate information [1]. A knowledge base use as a data source to improve the quality of query facets [6]. Knowledge bases hold numerous prominent organized majority of the data for, such as   their properties. In the proposed system, the user can search a keyword the search result are retrieved from the web. Then check the URL of search keywords if the URL is valid then extract the URL and then extract the search result. Apply the facet generation and facet expansion method to construct the final facet.The facet candidates are constructed by facet generation and expansion are further merged, because there might be duplicate items within these candidates. Then apply the facet grouping and facet weighting and finally produce the final facet. Our focus will be the system can made more effective by improving the recall of facet items by using entities and their properties of the query and at increase the accuracy of facet item. There are two methods are used, facet generation and facet expansion to produce the final facet. In facet generation, straightly utilize the properties about entities relating with a query. In facet expansion, expand starting facets mined by using existing algorithm. Those facets constructed using this two techniques would further consolidated and positioned should produce last query facets. Facet grouping can done in the system is all the facet candidates constructed by facet generation and expansion might have duplicate entities cluster them into the final facets by grouping similar candidates together. Facet Weighting can be done to weight each final facet.

The text mining algorithm is used, Text mining is the method of extracting meaningful information or knowledge or patterns from the available text documents from various sources [5]. Text mining is also referred as text data mining deriving high-quality information from text. Text mining usually involves the process of structuring input text deriving patterns from structured data finally evaluate the output. Text mining has a higher economic value than data mining. Text mining tasks consist of three steps: text preprocessing, text mining operations, text post-processing. Text preprocessing includes data selection text categorization and feature extraction. Text mining operations are the core part of text mining that includes association rule discovery, text clustering, and pattern discovery. Post-processing tasks modify the data after text mining operations are completed such as selecting, evaluating and visualization of knowledge [2].

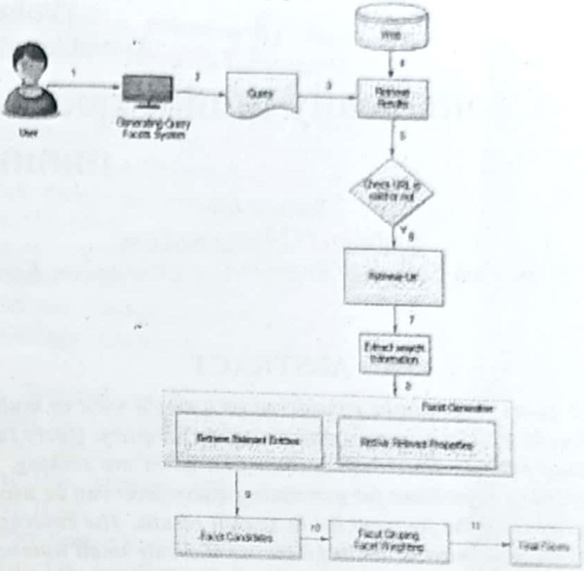

Web
User
1
Generating Query Facets System
2
Query
3
4
Retrieve Results
5
Check URL is valid or not
Y
6
Retrieve Url
7
Extract search information
8
Facet Generation
Retrieve Relevant Entities
Retrieve Relevant Properties
9
Facet Candidates
10
Facet Grouping Facet Weighting
11
Final Facets

Fig. 2: System Architecture

Text Mining is finding unknown hidden information. The information extracted from different written resources is done automatically. Text mining is a process that employs a set of algorithms for converting unstructured text into structured data items. Generic process of text mining performs the following steps [4]. (Figure 3)

1. Collecting unstructured data from different sources available in different file formats such as plain text, Web pages, pdf files etc.
2. Pre-processing and cleansing operations are performed to detect and remove anomalies. The cleansing process makes sure to capture the real essence of text available and is performed to remove stop words stemming (the process of identifying the root of the certain word) and indexing the data.
3. Processing and controlling operations are applied to audit and further clean the data set by automatic processing.
4. Pattern analysis is implemented by Management Information System (MIS).
5. Information processed in the above steps are used to extract valuable and relevant information for effective and timely decision making and trend analysis.

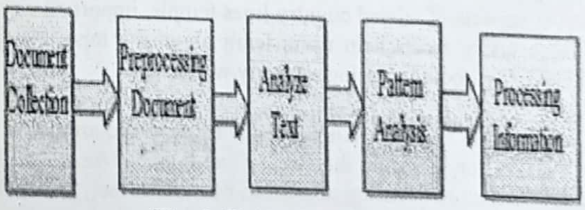


Fig. 3: Text mining process

Text mining deals with natural language text which is stored in semi-structured and unstructured format. The selection of an appropriate technique for mining text reduces the time and effort to find the relevant patterns for analysis and decision making [4].There are some basic text mining technologies they are Information Retrieval, Information Extraction, Categorization, Clustering, Summarization.

4. EXPERIMENTAL RESULTS

4.1 Comparison of QDMiner and Text Mining Algorithm

QDMiner extracts lists from free text, HTML tags, and repeat regions contained in the top search results, groups them into clusters based on the items they contain, then ranks the clusters and items based on how the lists and items appear in the top results [8]. To summarize the information contained in the query to find a list of related queries. QDMiner, to automatically mine query aspects by way of extracting and grouping common lists from loose textual content, HTML tags, and repeat areas inside top search effects [9]. The facets in QDMiner are generated using four essential phases such as List extraction, list weighting, list clustering and list ranking [9].

Text mining is extracting meaningful information from the available text document. Text mining usually involves the process of structuring the input text deriving patterns from structured data and finally evaluation and interpretation of the output. There are different tasks performed in text mining algorithm, Text categorization, Text clustering, Concept mining, Information retrieval, Information Extraction. .Text mining generally consists of the analysis of text documents by extracting key phrases, concepts, etc. and the preparation of the text processed in that manner for further analyses with numeric data mining techniques[10].

From the figure 4 shows the comparison of QDMiner algorithm i.e., the traditional method used and web data i.e., proposed algorithm it is text mining algorithm. Here we can clearly conclude that by using a traditional method different search keys are used the number of the search result can decrease. By using the proposed method the number of the search result can be increased rapidly. So by using the proposed method we can improve the system efficiency and at the same time improve the accuracy of facet item.

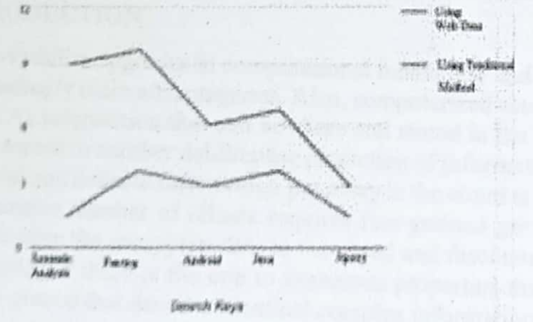


Fig. 4: Comparision Results of QDMiner and Text Mining Algorithm

5. CONCLUSION

In this paper, we can automatically generate query facet by using text mining algorithm. Query Facet is a set of items which describe and summarize one important aspect of a query. Text mining is extracting meaningful information from the available text document. The user can search for a keyword by using the system. Then the URL of the search result is retrieved from the web and finally view the summarised search result and the user can download the search result. There are two methods are used to construct the final facet namely Facet Generation and Facet Expansion.

In future, the system can be made more effective by improving the recall of facet items by utilizing entities and their properties contained in knowledge bases, and at the same time, make sure that the accuracy of facet items.

6. REFERENCES

[1] Survey on Query Facets Mining Approaches, Sheetal Sonwane, Nilam Patil.

[2] Feature Extraction and Duplicate Detection for Text Mining: A Survey, Ramya R S, Venugopal K R, Iyengar S S, Patnaik L M.

[3] Facet Discovery for Structured Web Search: A Query-log Mining Approach, Jeffrey Pound University of Waterloo Waterloo, Canada, Stelios Paparizos Microsoft Research Mountain View, CA, USA, Panayiotis Tsaparas Microsoft Research Mountain View, CA, USA.

[4] Text Mining: Techniques, Applications and Issues, Ramzan Talib, Muhammad Kashif Hanify, Shaeela Ayeshaz, and Fakeeha Fatimax, Department of Computer Science, Government College University, Faisalabad, Pakistan.

[5] A Review on Various Text Mining Techniques and Algorithms, R. Balamurugan, Dr. S. Pushpa.

[6] Generating Query Facets using Knowledge Bases, Zhengbao Jiang, Zhicheng Dou, Member, IEEE, and Ji-Rong Wen, Senior Member, IEEE.

[7] Extracting Query Facets from Search Results, Weize Kong and James Allan Center for Intelligent Information Retrieval School of Computer Science University of Massachusetts Amherst Amherst, MA 01003.

[8] Automatically Mining Facets for Queries from Their Search Results, Zhicheng Dou, Member, IEEE, Zhengbao Jiang, Sha Hu, Ji-Rong Wen, and Ruihua Song.

[9] Useful Query Facets Extracting Automatically from Top Retrieved Documents by Using QDMiner System, Bhagya Varsha S, Y. Sucharitha, Dr. D. Baswaraj, Dr.M.Janga Reddy.

[10] A tutorial review on Text Mining Algorithms, Mrs. Sayantani Ghosh, Mr. Sudipta Roy, and Prof. Samir K. Bandyopadhyay.

17-18

IJARIIT

INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume 4, Issue 2)

Available online at: www.ijariit.com

An Efficient Framework Security Model of Sharing Data for Privacy Protection and Performance-Based Outsource Data Sharing on Cloud

Kiren Vijai
kiren.vijai@gmail.com
Mangalam College of Engineering, Kottayam, Kerala

Syamamol T
syamamol.t@mangalam.in
Mangalam College of Engineering, Kottayam, Kerala

Merlin Mary James
merlin.james@mangalam.in
Mangalam College of Engineering, Kottayam, Kerala

ABSTRACT

One of the most efficient cryptanalysis systems of elegant data is stored and more data sharing file to be cached through the cloud. Be the part of the unusual weakness is the pivotal administration block of notoriety over the appliances. One of the main disadvantages is the pivotal pledge complication. While transferring the confidential file from one system to another there is a chance to leak the data from the system and can lose the privacy. The front-end gadgets of customers like advanced mobile phones by and large have constrained security assurance, the personal pivotal exist completely maintained and customers hazard pivotal introduction especially not really seen however inalienably existed in past research. Besides, gigantic customer decoding overhead constrains the handy utilization of ABE. The proposed system is that a shared key administration convention in CP-ABE. The development acknowledges disseminated age, drawback along with capacity over personal pivotal left out including some additional framework. The efficient information prompt trait disavowal is accommodated vital pivotal refresh. A synergistic instrument successfully takes care of key escrow issue as well as a key introduction. In the interim, it helps extraordinarily decrease customer unscrambling overhauls. The correlation thus alternative delegate the plans exhibits the plan made to some degree better execution as far as cloud-construct outsourced information partaking in light of cell phones and thus enhance the security and privacy protection. At last, we give evidence of security to the proposed convention.

Keywords: *Efficiency, Security, Data Sharing, Cloud Data Sharing, CP-ABE.*

1. INTRODUCTION

The cost-viability upgrades in computational innovation and expansive scale systems, offering information to others turns out to be correspondingly more advantageous. Also, computerized assets are all the more effortlessly acquired through distributed evaluation, capacity. As information that can be share and stored in the framework such a few associations mutually held, remote stockpiling is by one means or another debilitating protection of information proprietors. Along these lines, upholding the assurance of personal, confidential and delicate information put away in the cloud is to a great degree urgent [23], [25], [26], [36]. The synchronous interest of an extensive number of clients requires fine-grained get to authority while information splitting. One of the most promising security to store the encrypted data to the cloud and fascinating talent for secure and exible information splitting. One of the main characteristics of these is the one to numerous properties that implies the solitary pivotal are unscrambling diverse complex data distinctive pivotal that decodes identical complex information. The Attribute-Based Encryption is known as ciphertext strategy. The confidential data's are stored in the cloud and while transferring the data from one system to another, there is a chance to leak the file details and also chance to hack the files by the attackers. The data entrances strategies are implanted over the personal pivotal, property maintains to insert to the complex information and enables information proprietors over the data sharing technique is used to maintain the system [2], [36]. Any individual who needs to acquire information must first coordinate the entrance strategy with a property set. Because of the matter, protect the information while sharing the data during the transferring of the file from one system to another [27], [28], [36].

In any case, the considerable measure unenclosed difficulties of data sharing concerning useful acknowledge the data while particularly as far as private key administration. For huge quantities of past ABE plans [2] - [7], pivotal specialist can totally reliable, the unscramble data, the complex information that can be utilize to create personal pivotal after authorization. Getting the data or information without the permission of data from the owner generally known as key escrow issue, the innate disservice helps to debilitates client protection. Development of data sharing over versatile operation, portable data administrations [24], [31], [36] that are presented in the virtual pattern over distributed data flowing. Flow examine job scarcely sees that versatile front-end gadgets, for example, cell phones, are significantly more powerless than servers regarding security assurance [20]. In this way, the helplessness in private key insurance may effectively prompt the presentation of keys to unapproved clients [30], [5] - [29], [36]. The encrypted datas are keep to cloud and protect the file from hacking from attackers and provide more security and authentication to the system.

2. RELATED WORKS

An unique characteristic form entry limitation to an elegant pivotal refresh instrument through presenting trait aggregate pivotal to the overall system [2], [14]. The productive plan underpins much exible quality disavowal also the client repudiation that upgraded in the system also provides to store the data. The complex information capacity also the unscrambling rate i.e. real downsides to pragmatic over the system appliances [5]. To conquer these issues, a unique characteristics of the decoding system is placed an intermediary system is used a large portion through unscrambling data storage of the system to encode the data. While executing decoding, an information collector exchanges a change pivotal also complex information to be an intermediary system also gets an ciphertext. In this way, the plaintext can be extricated through extremely straightforward calculation by the information recipient. With the potential pattern of portable cloud benefit, applying outsourced unscrambling plan notably streamlines client encounter. A fluffy character based encryption (FIBE) in light of great personality based encryption [1].The character of a collector is spoken to by an arrangement of allocate the data, i.e. installed the personal pivotal. In the event that and just separation between quality arrangement over the recipient, another is the owner is encrypt the data through the limitation of the information, collector could remove the ordinary information effectively. A few numerous pivotal highlights over Attribute-Based Encryption, it established hypothetical framework over resulting testing towards Attribute-Based Encryption [21]. The examination effort showed additional development of the pivotal strategy of the Attribute base encryption, that implies every personal pivotal related along the entrance arrangement, every complex information i.e. related to the arrangement over data qualities [6], [25]. An idea over various levels summed up properties in light of the worldwide property accumulation, and proposed a progressive multiauthority system for CP-ABE. At the point when a client characterizes an entrance structure and demands information encryption, each key age focus (KGA) produces relating access arrangement and personal pivotal for the protection over the pivotal administration are ensured [10], [32]. An Attribute Based Encryption disavowal includes a proposal, cross breed irregular quality build encryption along, mix over immediate data also roundabout renouncement. While executing encryption, every datum sender is permitted to choose which revocable plan is utilized that consolidate points of interest of the two strategies. Nothing that its half and half renouncement has no impact on decoding albeit every datum beneficiary has just a single private key [3], [9]. A solid development where the system information of the owner could adaptably characterized entrance arrangement instead of the information being scrambled [21], [2]. Subsequently, ensures information confidentiality as well as acknowledgment of independent entry constraint. Oualha et al. [35] showed that notwithstanding gigantic calculation assets are required in ABE, heaps of overwhelming calculation should be possible ahead of time. Thinking about constraint of vitality and calculation of hubs over the data utilization presenting calculation procedure that processes also be securing any basic components previously encoding happens [7], [8]. Despite the fact that ongoing calculation overhead is especially diminished, their plan requires confided in substances to store components. Facilitate many, committed network likewise need safely exchange of components wanted to store the data in the hubs. The encode rate, also the decrypt rate increment directly through multifaceted nature over entry strategy makes the complex information to the system [4].

3. EXISTING SYSTEM

Past plans of key administration in quality based information sharing framework basically centers around key refresh, intermediary re-encryption and outsourced decoding. Some examination showed untrusted key specialist may prompt key escrow issue and gave relating arrangements. In any case, challenges are facing to safeguard the data. In the event that personal pivotal totally put away including the systems like cell phone gadgets, more regrettable issue known pivotal introduction happens debilitating secrecy of private keys. In expansion, the greater part of property based information sharing plans improved protection over the system administration rate over the unscrambling reduction through information recipients. With cost-viability changes in computational innovation and expansive scale systems, offering information to others turns out to be correspondingly more helpful. Moreover, computerized assets are all the more effortlessly acquired through distributed evaluation and capacity. Since the information splitting the data framework are held with few associations together, remote stockpiling are some way or another undermining security of information proprietors. Accordingly, implementing the assurance of personal, confidential and delicate information put away in the cloud is amazingly critical [23], [25], [26], [36]. The synchronous interest of an extensive number of clients requires fine-grained get to authority while information splitting. One of the most promising security to store the encrypted data to the cloud and fascinating talent for secure and exible information splitting. One of the main characteristic of these is the one to numerous properties that implies the solitary pivotal are unscrambling diverse complex_data distinctive pivotal that decodes identical complex information. The Attribute-Based Encryption known as ciphertext strategy. The confidential data's are stored in the cloud and while transferring the data from one system to another, there is chance to leak the file details and also chance to hack the files by the attackers. The data entrances strategies are implanted over the personal pivotal, property maintain to insert to the complex information and enables information proprietors over the data sharing technique is used to maintain the system [2], [36]. Any individual who needs to acquire information must first coordinate the entrance strategy with a property set. Because of the matter, protect the information while sharing the data during the transferring of file from one system to another [27], [28] [36]. In any case, the considerable measure unenclosed difficulties of data sharing concerning useful acknowledge the data while particularly as far as private key administration. For huge quantities of past ABE plans [2]-[7], [36], pivotal specialist can totally reliable, the unscramble data, the complex information that can be utilize to create personal pivotal after authorization. Getting the data or information without the permission of data from the owner generally known as key escrow issue, the innate disservice helps to debilitates client protection. Development of data sharing over versatile operation, portable data administrations [24], [31] [36] that are presented in the virtual pattern over distributed data flowing. Flow examine job scarcely sees that versatile front-end gadgets, for example, cell phones, are significantly more powerless than servers regarding security assurance [20]. In this way, the helplessness in private key insurance may effectively prompt the presentation of keys to unapproved clients [30], [5] - [29], [36]. The encrypted data is keep to the cloud and protect the files from hacking by attackers and provide more security and authentication to the system.

4. PROPOSED SYSTEM

A novel synergistic key administration convention in ciphertext arrangement trait model is used, improve protection of data and enhance the security for the system model, productivity over pivotal administration of data information model. Fundamental commitments have compressed to takes after: The model communitarian convention are displayed. The data owner can create or upload the file in the system. While uploading the file, the data is encrypted. The encrypted file are kept on cloud server. If the owner wants data, the file is decrypted and the data owner can access the file. In this manner, the protection of pivotal administration are ensured including some additional external foundation. If the client accesses the data from the data owner he / she send a request for the acquire file to the owner. Owner immediately sends three keys i.e. private key, master key, secret key to the client. If clients gets the keys then, the client can access the file also data owner sends a time limit to the client. Within the time limit the client, acquire data from the data owner. If time limit exceeds then again the client sends a request to the data owner. A one of a kind trait assemble key is distributed to each quality gathering that contains customers who share a similar trait. Through refreshing trait bunch pivotal, quick quality denials are given. Demonstrate the key escrow issue as well as key introduction is undermining the classification of personal pivotal, that are not really seen past system model. Contrasted with past key administration conventions for quality based information sharing framework, the convention adequately makes twice issues over the community pivotal administration. Thus, provides more security and protection of files to the whole system. Provides the privacy of the data or files and also provides a key update function to the model.

4.1 System Framework

In the system framework mainly consist of 5 components are engaged with information splitting. One of the main component is the Data Owner. An information proprietor are approved client through framework whose informations are created and uploaded. DOs define their own particular express entry approaches with the goal that lone alluring CLs are allowed authorization to acquire plaintext. Another main component is the Key Authority. The pivotal specialists are crucial segment to framework. Key Authority are in charge of more ascertaining undertakings, especially pivotal age, pivotal refresh, and so on and accept that the KA is semi-confided in the framework, which means i.e. interested regarding estimation through ordinary information however have the goal of altering off. Another important component is the Cloud Server. In the cs, complete information or files can be stored to cs also encrypted file are kept over cs. Another main component is the Decryption Server, an unscrambling system of data have effective registering abilities. It attempts and confines the more data, however completely inadequate all errand unscrambling. Decryption Server gets the network be unreliable, on the grounds i.e. adequate to ensure information security. Finally an important component is the Client, customer i.e. a client whose means of getting the information through distributed network store through system gadgets. The client is collected the data / information through the owner. With the permission of the owner, client can access the data or information. A chance of getting the CL's property set fulfills an entrance approach related to the complex information, client should permitted the data, acquire procure ordinary information and get the decrypted data to the client.

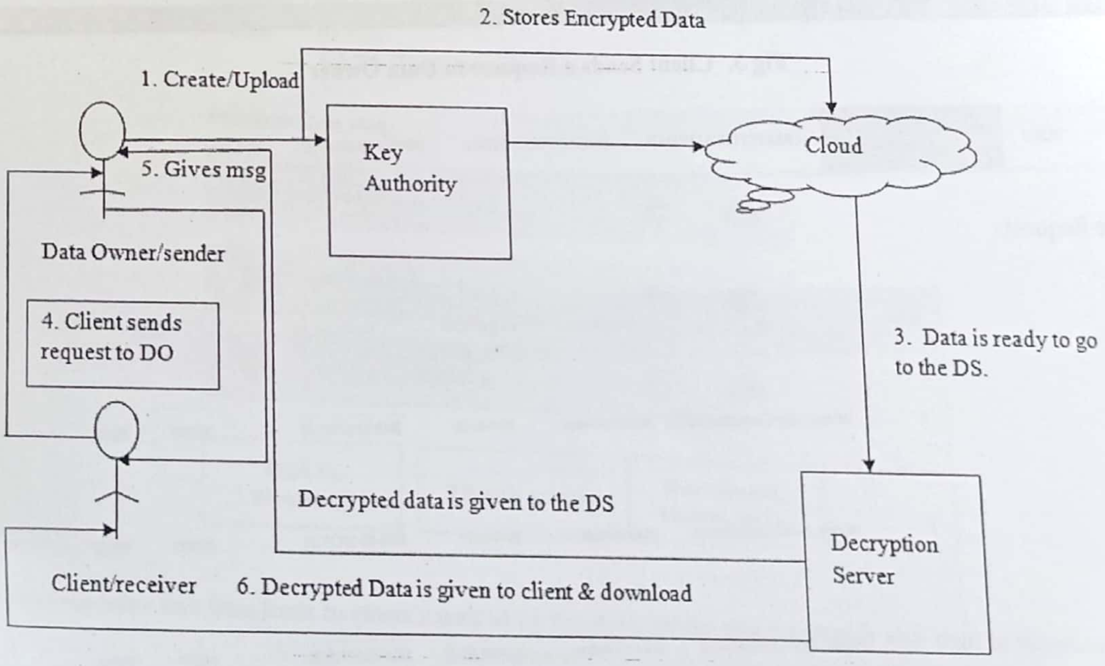
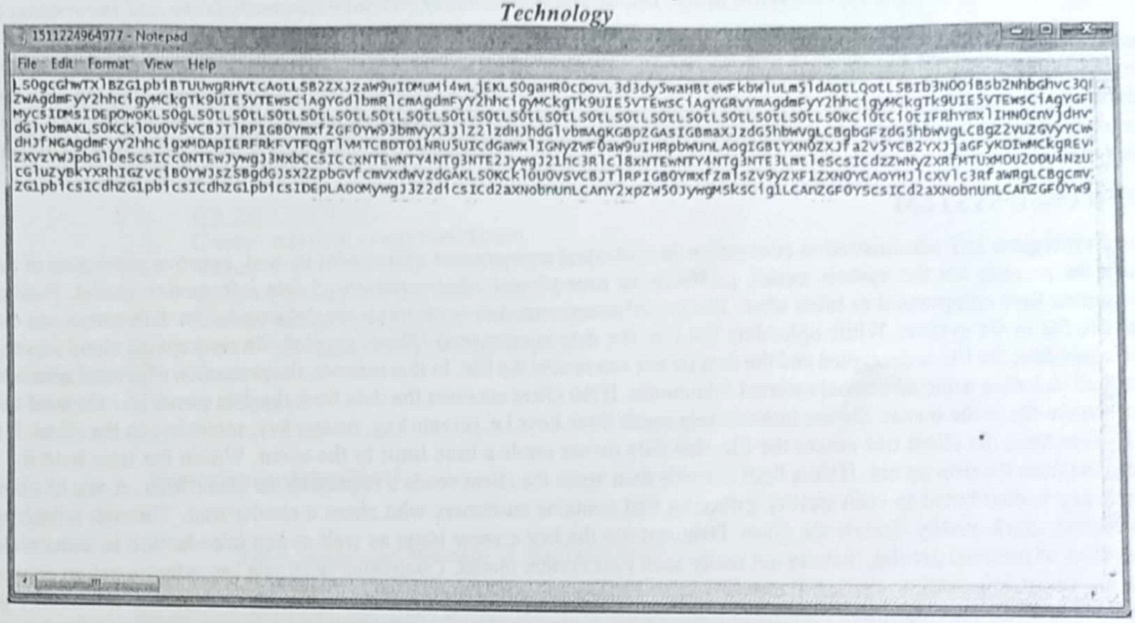
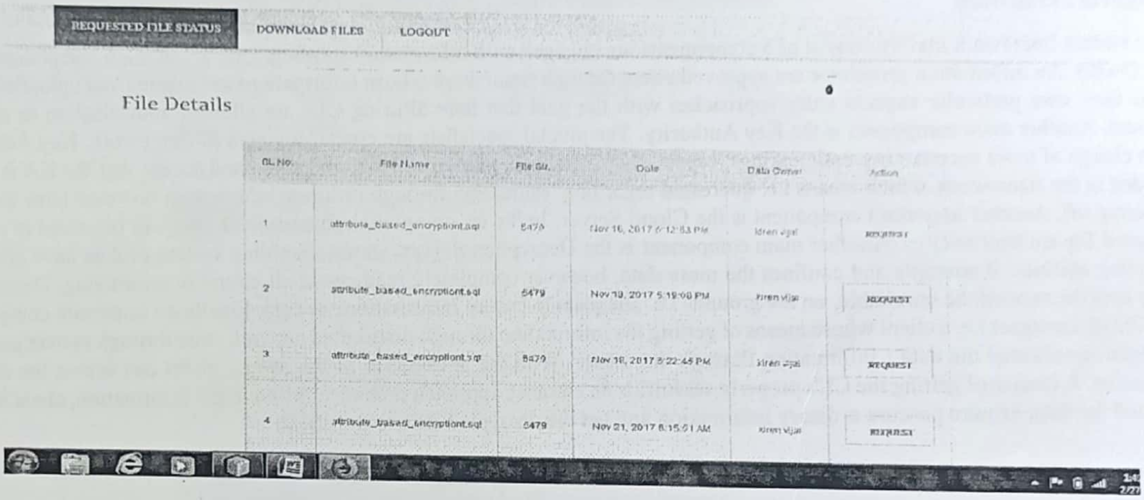

2. Stores Encrypted Data
1. Create/Upload
5. Gives msg
Key Authority
Cloud
Data Owner/sender
4. Client sends request to DO
3. Data is ready to go to the DS.
Decrypted data is given to the DS
Decryption Server
Client/receiver
6. Decrypted Data is given to client & download

Fig 1. Cipher Text Encryption Model



```
LS0gcGhwTXlBZG1pbiBTUUwgRHVtcAotLSB2ZXJzaW9uIDMuMi4wLjEKLS0gaHR0cDovL3d3dy5waHBteWFkbWluLm5ldAotLQotLSBIb3N0OiB5b2NhbGhvc3Ql
ZWAgdmFyY2hhcigyMCkgTk9UIE5VTEwsCiAgYGdlbmRlcmAgdmFyY2hhcigyMCkgTk9UIE5VTEwsCiAgYGRvYmAgdmFyY2hhcigyMCkgTk9UIE5VTEwsCiAgYGFl
MyCSIDMSIDEpOWoKLS0gLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0KCi0tCi0tIFRhYmxlIHN0cnVjdHV
dGlvbmAKLS0KCklOU0VSVCBJTlRPIGB0YmxfZGF0YW93bmVyX3JlZ2lzdHJhdGlvbmAgKGBpZGAsIGBmaXJzdG5hbWVgLCBgbGFzdG5hbWVgLCBgZ2VuZGVyYCw
dHJfNGAgdmFyY2hhcigxMDApIERFRkFVTFQgTlVMTCBDT01NRU5UICdGawxlIGNyZWF0aW9uIHRpbWUnLAogIGBtYXN0ZXJfa2V5YCB2YXJjaGFyKDIwMCkgREV
ZXVzYWJpbGl0eScsICc0NTEwJywgJ3NxbCcsICcxNTEwNTY4NTg3NTE2JywgJ21hc3Rlc18xNTEwNTY4NTg3NTE3LmtleScsICdzZWNyZXRfMTUxMDU2ODU4NzU
cGluZyBkYXRhIGZvciB0YWJsZSBgdGJsX2ZpbGVfcmVxdWVzdGAKLS0KCklOU0VSVCBJTlRPIGB0YmxfZmlsZV9yZXF1ZXN0YCAoYHJlcXVlc3RfaWRgLCBgcmV
ZG1pbicsICdhZG1pbicsICdhZG1pbicsIDEpLAooMywgJ3Z2dicsICd2aXNobnUnLCAnY2xpZW50JywgMSksCigiLCAnZGF0YScsICd2aXNobnUnLCAnZGF0YW9
```

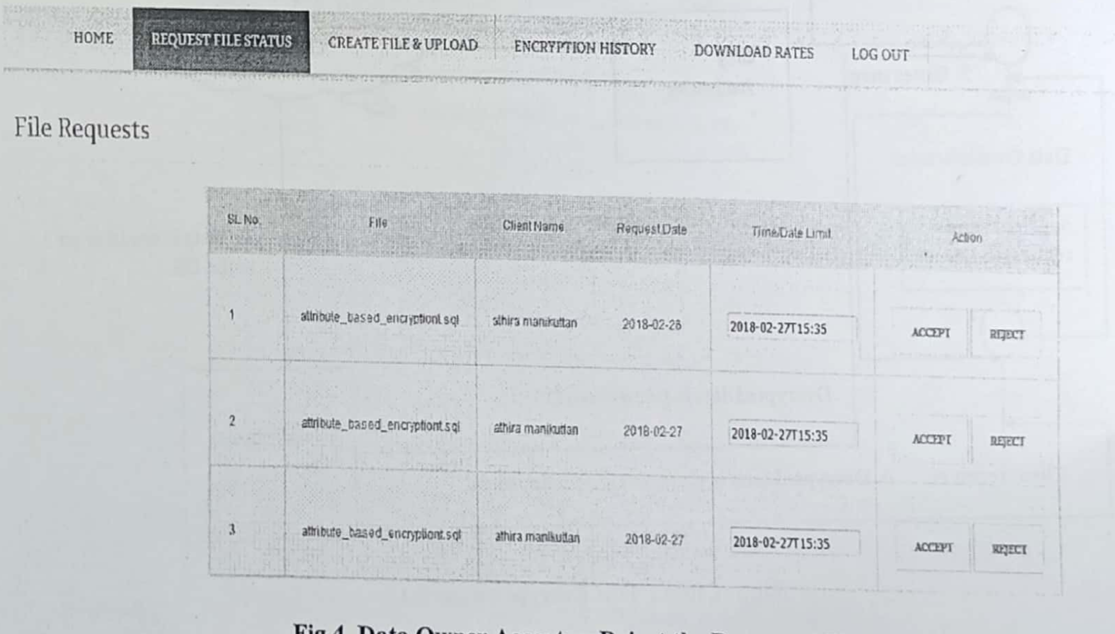
Fig 2. Encrypted File



File Details

SL No.	File Name	File Siz.	Date	Data Owner	Action
1	attribute_based_encryptiont.sql	5479	Nov 16, 2017 6:12:53 PM	kiren vijai	REQUEST
2	attribute_based_encryptiont.sql	5479	Nov 19, 2017 5:19:08 PM	kiren vijai	REQUEST
3	attribute_based_encryptiont.sql	5479	Nov 18, 2017 8:22:45 PM	kiren vijai	REQUEST
4	attribute_based_encryptiont.sql	5479	Nov 21, 2017 8:15:01 AM	kiren vijai	REQUEST

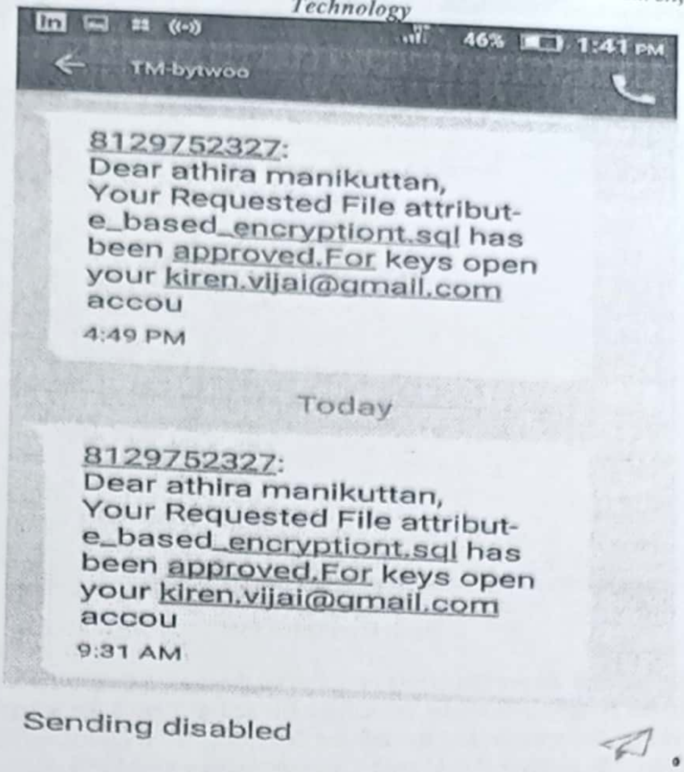
Fig 3. Client Sends a Request to Data Owner



File Requests

SL No.	File	Client Name	Request Date	Time/Date Limit	Action
1	attribute_based_encryptiont.sql	athira manikuttan	2018-02-28	2018-02-27T15:35	ACCEPT REJECT
2	attribute_based_encryptiont.sql	athira manikuttan	2018-02-27	2018-02-27T15:35	ACCEPT REJECT
3	attribute_based_encryptiont.sql	athira manikuttan	2018-02-27	2018-02-27T15:35	ACCEPT REJECT

Fig 4. Data Owner Accept or Reject the Requested File

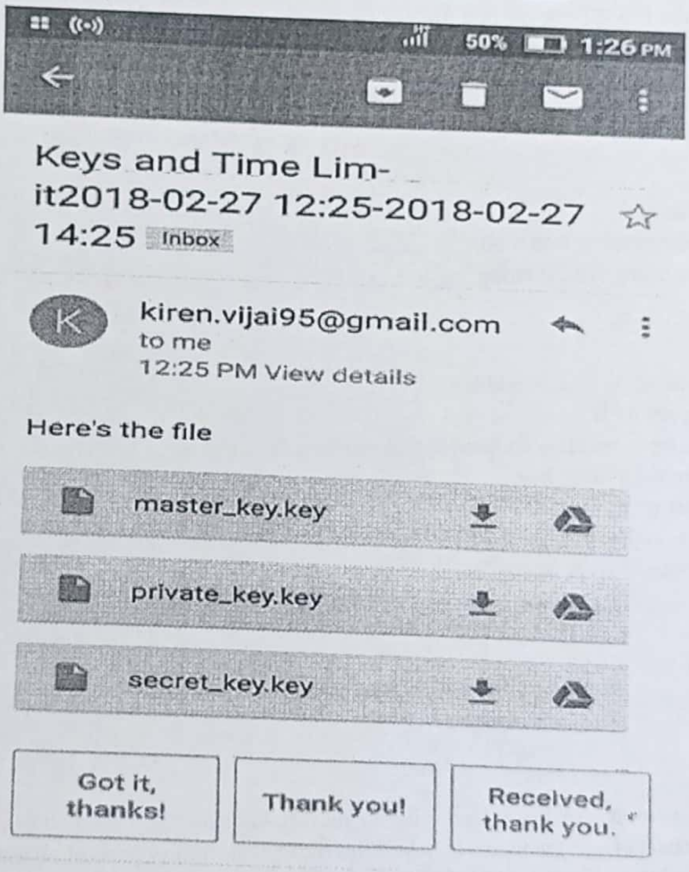


8129752327:
Dear athira manikuttan,
Your Requested File attribute_based_encryptiont.sql has been approved.For keys open your kiren.vijai@gmail.com accou
4:49 PM

Today

8129752327:
Dear athira manikuttan,
Your Requested File attribute_based_encryptiont.sql has been approved.For keys open your kiren.vijai@gmail.com accou
9:31 AM

Fig 5. Approved Message is Send to Client



Keys and Time Limit2018-02-27 12:25-2018-02-27 14:25 Inbox

kiren.vijai95@gmail.com
to me
12:25 PM View details

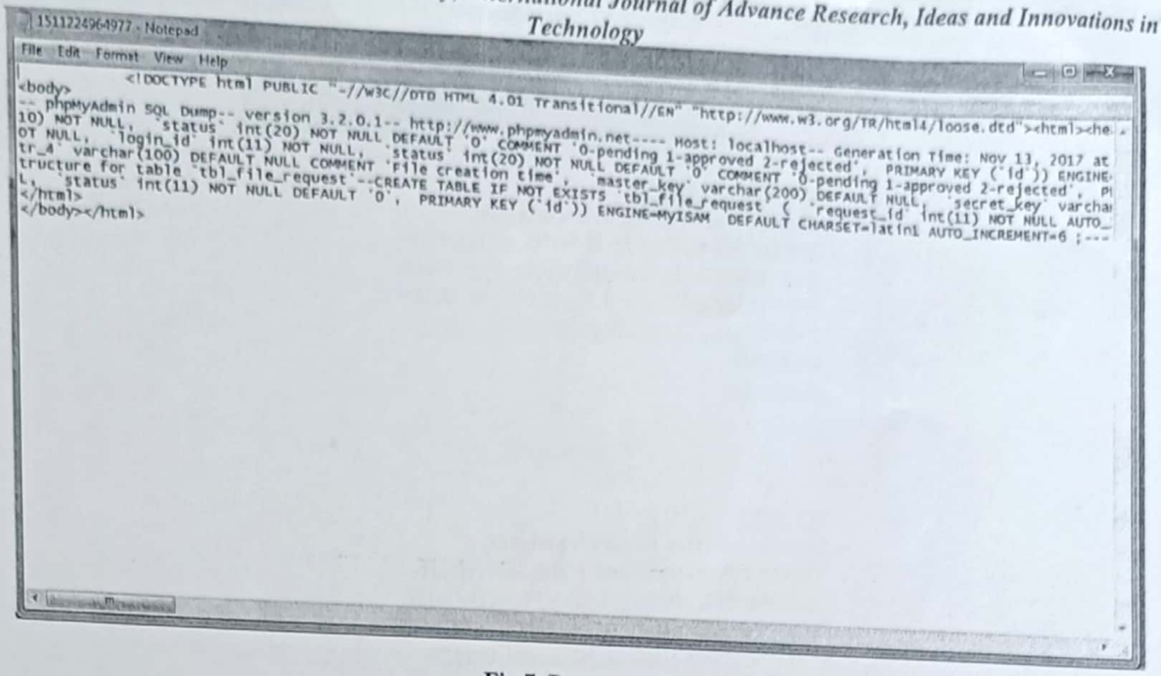
Here's the file

master_key.key

private_key.key

secret_key.key

Fig 6. Also send the keys and time limit to client's mail id by the data owner and an alert is also send to the client's Smartphone



```
              <!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"><html><he
<body>
-- phpMyAdmin SQL Dump-- version 3.2.0.1-- http://www.phpmyadmin.net---- Host: localhost-- Generation Time: Nov 13, 2017 at
10) NOT NULL,  `status` int(20) NOT NULL DEFAULT '0' COMMENT '0-pending 1-approved 2-rejected',  PRIMARY KEY (`id`)) ENGINE
OT NULL,  `login_id` int(11) NOT NULL,  `status` int(20) NOT NULL DEFAULT '0' COMMENT '0-pending 1-approved 2-rejected',  PI
tr_4` varchar(100) DEFAULT NULL COMMENT 'File creation time',  `master_key` varchar(200) DEFAULT NULL,  `secret_key` varchar
tructure for table `tbl_file_request`--CREATE TABLE IF NOT EXISTS `tbl_file_request` (  `request_id` int(11) NOT NULL AUTO_
L,  `status` int(11) NOT NULL DEFAULT '0',  PRIMARY KEY (`id`)) ENGINE=MyISAM  DEFAULT CHARSET=latin1 AUTO_INCREMENT=6 ;---
</html>
</body></html>
```

Fig 7. Decrypted File

In the model shows, fig 1, firstly the data owner can create or uploaded the data, information or file. Through the Key authority, provides the key to the owner of the system. The sender uploaded a file and encrypted file is kept over cloud fig 2. Whenever the sender wants data, at that time, owner decrypts the data through the decrypted server. Decrypted data can access by the data owner. If receiver acquires the information. The receiver should send a request to data owner Fig 3 and the data owner can accept or reject the request Fig 4. The approved message is sent to the client's smartphone Fig 5.Sender approves the request fig 5, the sender sends a message to the client and also given a time limit to access the file. The time limit is also sent to the client mail id fig 6. Within the time limit, client should access the file. The decrypted file can be accessed by the client Fig 7. After the time limit client can't access the file. Also, the client sends a re-request to the data owner to again access the file.

4.2 Implementation

4.2.1 Base64 Algorithm

- Convert the txt into 8 bit.
- Combine them and Convert them into 6 bit.
- Finally, get the corresponding ASCII string.

4.2.2 RSA Algorithm

- Take two numbers of prime let it be A and B
- Let n be the public key, n= A*B.
- Given a small exponent be e, must be an integer also not be a factor of n.
- 1 < e < φ (n), n and e are the public key
- Calculate φ (n), such that φ (n) = (A-1) (B-1)
- Calculate greatest common divisor (e, (A-1))
- Calculate greatest common divisor (e, (B-1))
- Calculate greatest common divisor (e, φ (n))
- Calculate ed mod φ (n) =1
- Calculate c = m ^ e mod n, for encryption.
- Calculate m = c ^ d mod n, for decryption.

5. CONCLUSION

Ciphertext arrangement quality systems use the information is mainly kept on the cloud. It is one of the efficient and security provided to the system to avoid attacks from the attackers. An innovative community pivotal administration convention for upgrade the authentication and effectiveness of pivotal administration in figure content approach property based encryption for cloud information sharing framework. Dispersed key age, problems off, capacity over personal pivotal to lack of acknowledgment including the additional visible framework. The acquaint characteristic gatherings with construct the personal pivotal to compute the gathering information and data repudiation to the system to provide more authentication and security to the framework. The proposed collective instrument superbly addresses key escrow issue as well as a more terrible issue called key presentation that past research scarcely took note. In the interim it advances customers client encounter since just a little measure of obligation to makes unscrambling. Hence, information is stored in the cloud framework helping enormous execution limited front-end gadgets concerning over more authentication and also protects the owner's privacy and provide more security. The keys are always updating each time. Thus provide more security to the data owner and also provide authentication. Now expand the preparatory discoveries to build up information plot by diminishing the complex information measure, encode rate, decoding rate, thus as yet unenclosed issues i.e. impede down to earth utilization of trait information sharing. Thinking of some as particular mechanical situations, for example, individual wellbeing record gets to control, plus, the expressiveness of access strategy needs improvement too.

6. REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. Euro Crypt, 2005, pp. 457_473.

[2] J. Bethencourt, A. Sahai, and B.Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Secur. Privacy, May 2007, pp. 321_334.

[3] N. Attrapadung and H. Imai, "Conjunctive broadcast and attribute- based encryption," in Proc. Int. Conf. Pairing-Based Cryptogr., 2009, pp. 248_265.

[4] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Public Key Cryptogr., 2011, pp. 53_70.

[5] M. Green, S. Hohenberger, and B.Waters, "Outsourcing the decryption of ABE ciphertexts," in Proc. USENIX Secur. Symp., 2011, p. 34.

[6] J. Lai, R. H. Deng, C. Guan, and J.Weng, "Attribute-based encryption with veriable outsourced decryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1343_1354, Aug. 2013.

[7] S. Lin, R. Zhang, H. Ma, and M.Wang, "Revisiting attribute-based encryption with veriable outsourced decryption," IEEE Trans. Inf. Forensics Security, vol. 10, no. 10, pp. 2119_2130, Oct. 2015.

[8] M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proc. ACM CCS, 2009, pp. 121_130.

[9] G. Zhang, L. Liu, and Y. Liu, "An attribute-based encryption scheme secure against malicious KGC," in Proc. TRUSTCOM, Jun. 2012, pp. 1376_1380.

[10] J. Hur, "Improving security and efficiency in attribute-based data sharing,"IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2271_2282, Oct. 2013.

[11] P. P. Chandar, D. Mutkuraman, and M. Rathinrai, "Hierarchical attribute based proxy re-encryption access control in cloud computing," in Proc. ICCPCT, Mar. 2014, pp. 1565_1570.

[12] X. A. Wang, J. Ma, and F. Xhafa, "Outsourcing decryption of attribute based encryption with energy efficiency," in Proc. 3PGCIC, Nov. 2015, pp. 444_448.

[13] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. ACM CCS, 2007, pp. 456_465.

[14] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, pp. 1214_1221, Jul. 2011.

[15] M. Pirretti, P. Traynor, P. McDaniel, and B.Waters, "Secure attribute-based systems," in Proc. ACM CCS, 2006, pp. 99_112.

[16] A. Boldyreva, V. Goyal, and V. Kumar, ``Identity-based encryption with efficient revocation," in Proc. ACM CCS, 2008, pp. 417_426.

[17] A.-P. Xiong, C.-X. Xu, and Q.-X. Gan, "A CP-ABE scheme with system attributes revocation in cloud storage," in Proc. ICCWAMIP, Dec. 2014, pp. 331_335.

[18] W. Qiuxin, "A generic construction of ciphertext-policy attribute-based encryption supporting attribute revocation," China Commun., vol. 11, no. 13, pp. 93_100, 2014.

[19] S. S. M. Chow, "Removing escrow from identity-based encryption," in Proc. Int. Conf. Pract. Theory Public Key Cryptogr., 2009, pp. 256_276.

[20] M. S. Ahmad, N. E. Musa, R. Nadarajah, R. Hassan, and N. E. Othman, "Comparison between Android and iOS operating system in terms of security," in Proc. CITA, Jul. 2013, pp. 1_4.

[21] V. Goyal, O. Pandey, A. Sahai, and B.Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM CCS, 2006, pp. 89_98.

[22] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," ACM Comput. Surv., vol. 35, no. 3, pp. 309_329, Sep. 2003.

[23] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1_11, 2011.

[24] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," Wireless Commun. Mobile Comput., vol. 13, no. 18, pp. 1587_1611, Dec. 2013.

[25] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, ``Security and privacy challenges in cloud computing environments," IEEE Security Privacy, vol. 8, no. 6, pp. 24_31, Nov./Dec. 2010.

[26] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362_375, Feb. 2013.

[27] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute- based encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131_143, Jan. 2013.

[28] Q. Liu, G. Wang, and J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," Inf. Sci., vol. 258, pp. 355_370, Feb. 2014.

[29] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the Internet of Things," Future Generat. Comput. Syst., vol. 49, pp. 104_112, Aug. 2015.

[30] H. Hong and Z. Sun, "High efficient key-insulated attribute based encryption scheme without bilinear pairing operations," SpringerPlus, vol. 5, no. 1, p. 131, Feb. 2016.

[31] M. R. Rahimi, J. Ren, C. H. Liu, A. V. Vasilakos, and N. Venkatasubramanian, "Mobile cloud computing: A survey, state of art and future directions," Mobile Netw. Appl., vol. 19, no. 2, pp. 133_143, Apr. 2014.

[32] D. Pletea, S. Sedghi, M. Veeningen, and M. Petkovic, "Secure distributed key generation in attribute based encryption systems," in Proc. ICITST, Dec. 2015, pp. 103_107.

[33] X. Xu, J. Zhou, X. Wang, and Y. Zhang, "Multi-authority proxy re encryption based on CPABE for cloud storage systems," J. Syst. Eng. Electron., vol. 27, no. 1, pp. 211_223, Feb. 2016.

[34] S. Easwarmoorthy, S. F, and A. Karrothu, "An efficient key management infrastructure for personal health records in cloud," in Proc. WiSPNET, Mar. 2016, pp. 1651_1657.

[35] N. Oualha and K. T. Nguyen, "Lightweight attribute-based encryption for the Internet of Things," in Proc. ICCCN, Aug. 2016, pp. 1_6.

[36] Guofeng Lin,Hanshu Hong and Zhixin Sun, "A Collaborative key management protocol in Ciphertext policy attribute-based encryption for cloud data sharing", May 2017.

IJCSE International Journal of Computer Sciences and Engineering
Open Access

Research Paper Vol.-5, Issue-9 , Sep 2017 E-ISSN: 2347-2693

IMPROVAL AQUAPRO

Preethi Sebastian[1], Susan V Nainan[2], Jeneesh Scaria[3]

[1,2,3]Department of Electrical Electronics Engineering, Mangalam College of Engineering Ettumanoor, Kottayam

Available online at: www.ijcseonline.org

Received ..../2017, Revised: ....2017, Accepted: ....2017, Published: 30/Sep/2017

Abstract— The current method of raising tilapia in the Philippines is through fish ponds exposed to the weather. Methods for measuring pH, temperature, dissolved oxygen, and ammonia are limited to manually using a chemical test kit. The current system relies on manually regulating the water quality sothe fish are at risk of harmful situations resulting from unsafe levels of temperature, pH, dissolved oxygen, or ammonia. This study aims to solve that problem by creating a system that automatically measures and regulates the pH, temperature, dissolved oxygen, and ammonia. This study takes advantage of electronic sensors for pH, temperature, and dissolved oxygen, while computing the ammonia factor, to allow the user to measure the levels of the said parameters at any given time, process, send the data to a LabVIEW database, and use the data to automatically take corrective action against harmful levels of pH, temperature, dissolved oxygen, and ammonia while notifying the user through SMS. The proponents of this study built the prototype and tested it on two different trials of 50 fingerlings each in a 1 cubic-meter glass aquarium.

Keywords— Tilapia farming, pH, Temperature, Control Actuators , Ammonia

I. INTRODUCTION

Tilapia farming is a very large industry in the Philippines. The Philippines produced 260,525.67 metric tons of tilapia in 2012 [1]. Fish farms are all over the country usually raise the fish in containers fresh-water lakes or large man-made ponds; the majority with a common depth of 70-80 cm [2]. The current system leaves the fish outdoors and exposed to elements. The fish are vulnerable to situations where the pH, temperature, DO, or ammonia levels become harmful. It only takes one of those parameters to be at a lethal level for entire batches of fish to die off and cause major losses for the whole growing cycle. This requires constant vigilance which can be cumbersome for the staff.This study intended to provide a solution for such events. The system proposed is meant to provide a means to provide real-time measurements and regulation for pH, temperature, DO, and ammonia. The system was designed to measure and automatically take corrective action as soon as harmful levels of any of the said parameters are detected to reduce the possibility of fish kill. The system takes advantage of electronic sensors to provide real-time parameter measurements, a controller to process, store the data, and automatically take corrective action when needed, perform thesaid corrective action while notifying the user through SMS. Elements found in previous studies and recommendations wereintegrated to design this system.

II. LITERATURE REVIEW

The National Aquaculture Sector of the Philippines observed the typical method of raising tilapia in the Philippines involves placing the tilapia in large outdoor ponds,pens, and cages. These containers are usually placed in freshwater lakes or man-made ponds. The tilapia are fed and sampled or transferred when necessary. It is usually an affordable and basic set up [3].The Metropolitan Fishing Group based in Singapore uses Dissolved Oxygen (DO) sensors to monitor the DO levels of their fish tanks. When the sensors detect critically-low levels of DO, their system immediately notifies the staff to manually replenish the DO through operating a special pump. Their tanks also use electronic filters to ensure optimal water quality for their fish. [4]. It is recommended that future studies utilize a database to record data trends, and a GSM module to notify the user remotely [5].In the area of real-time pH measurement, a research group explored the use of Ion Selective Electrodes (ISE)in measuring ammonia and the pH levels of a solution. They fabricated their own ISE's by

IJCSE International Journal of Computer Sciences and Engineering
Open Access

Research Paper Vol.-5, Issue-12, Dec 2017 E-ISSN: 2347-2693

Privacy Protection on Cloud Computing with Auditing Scheme

Nimmymol Manuel[1*]· Simy Mary Kurian[2], Neena Joseph[3], Neema George[4]

[1,2,3,4] Department of Computer Science & Engineering,Mangalam College of Engineering, Kerala, India

e-mail: nimmymol.manuel@mangalam.in,simy.kurian@mangalam.in ,neen.jseph@mangalam.in,neema.george@mangalam.in

*Corresponding Author: nimmymol.manuel@mangalam.in, Tel.: +91 9496380516

Available online at: www.ijcseonline.org

Received: ………/2017, Revised: ………..2017, Accepted: ………2017, Published: 30/Dec/2017

Abstract— Distributed computing gives an assortment of administrations to our current specialized regions. It is helpful for the two customers and organizations to utilize applications without access their own records. Security is an unavoidable component of our cloud administration. So we ought to make sure that our specialist organization can give the security to our information. Yet, various prominent hacking cases will prompt various sorts of safety issues on cloud. It for the most part happens in multi clients distributed computing regions Cloud security is significant in each field of clients. Everybody needs to give their data completely safe. For this reason, here we can utilize property-based encryption that is a kind of open key encryption. Characteristic based encryption permits information proprietors and clients to encode and decode in light of the individual ascribes. So we propose a audit scheme which gives a sort of security insurance on clients and ke*p from unapproved access from programmers.,

Keywords— Encryption, CP-ABE, Collusion Attack

I.

II. INTRODUCTION

Distributed computing is a technique for conveying different administrations where assets are recovered from the Internet through online applications. Instead of keeping records on a hard drive or neighborhood stockpiling gadget, cloud-based capacity makes it conceivable to save them to a distant data set. Distributed computing is usually utilized in the present IT world in light of its high openness and accessibility.

Significant dangers to cloud security incorporate information break, information misfortune, account hacking, unreliable application programming Interfaces (APIs),poor decision of distributed storage gives and shared innovation that can think twice about security. There are a few kinds of encryption strategies are utilized on distributed computing for giving security on clients information and qualities. Out of these the most presumably utilized strategy is property based encryption.

Clinical proposition is a fundamental part in current medical care the executives. Wellbeing data at different levels could be produced from Medical theory. Exact and solid data is required for arranging medical care exercises and wellbeing planning and this could be acquired uniquely from these records. It works on the capacity, recovery, and sharing of the clinical data more productive. We center around numerous information proprietor situation.

The significance of information honesty has been featured by the accompanying examination works under various framework and security models. The major issue related to security problem is collude attack.

So here present an auditing scheme for security assurance on the information's put away on the cloud server. It really takes a look at the trustworthiness of put away information without help from anyone else. Through point by point security investigation, the proprietor's archive is demonstrated to be safer.

The rest of this paper is coordinated as follows. In section2, the related works are talked abou*. Section3, the proposed strategies are introduced. In section4, Experiment result followed by Conclusion.

III. RELATED WORK

There exists an issue over scrambled cloud information when customized multi-watchword positioned search is utilized to check regardless of whether questioned catchphrases where present.

The framework is a combination of both proxy signature, enhanced TGDH and proxy re-encryption both together into

IJCSE International Journal of Computer Sciences and Engineering
Open Access

Research Paper   Vol.-6, Issue-1, Jan 2018   E-ISSN: 2347-2693

Improving Image Encryption Using WU's Algorithm

Simy Mary Kurian [1*], Nimmymol Manuel [2], Neena Joseph [3], Neema George [4]

[1] Department of Computer Science & Engineering,Mangalam College of Engineering, Kerala, India
[2] Department of Computer Science & Engineering,Mangalam College of Engineering, Kerala, India
[3] Department of Computer Science & Engineering,Mangalam College of Engineering, Kerala, India
[4] Department of Computer Science & Engineering,Mangalam College of Engineering, Kerala, India

e-mail: simy.kurian@mangalam.in ,nimmymol.manuel@mangalam.in,neena.joseph@mangalam.in,neema.george@mangalam.in

*Corresponding Author: simy.kurian@mangalam.in, Tel.: +91 9656294800

Available online at: www.ijcseonline.org

Received: ..../2018, Revised: ....2018, Accepted: ....2018, Published: 30/Jan/2018

Abstract— In this advanced world, pictures are generally utilized in various cycles. Along these lines, the security of picture and information from unapproved utilizes is significant. Presently, data security is turning out to be progressively significant in information capacity and broadcasting. It is fundamental for getting picture, either on the way or store on gadgets. Nonetheless, some picture encryption calculations actually have numerous security issues and can be effortlessly gone after by assailants. This proposed framework plays out the cryptanalysis of a recently proposed variety picture encryption scheme utilizing Wu's algorithms . For encryption plot, typically utilizes a pseudo-irregular encryption key created by a calculation and which makes the picture safer. An approved recipient can without much of a stretch unscramble the message with the mystery key given by the originator to recipient however not to unapproved clients

.

Keywords— Encryption, Wu's algorithms

I.

II. INTRODUCTION

Encryption is the most common way of encoding information utilizing a mystery key so it can stay covered up or difficult to reach to unapproved clients. This safeguards individual data and touchy information and builds the security of correspondence between client applications and servers. Today all utilization social, the unapproved clients are hack our own information. We are not fretted over that kind of wrongdoing. However, today the digital violations are increment. After increment the digital wrongdoing we are consider it.

That time is give more significance digital protection. In friendly Medias give heaps of safety highlights. In early day's kin are utilizing social Medias and which are utilized for associating various people groups. Yet, today its utilized for business. So this time the digital wrongdoings are increment. The encryption method is utilized to forestall the digital wrongdoings.. In this strategy is profoundly validated and give greater security of our own information. The singular mystery keys are utilized the information move and it is exceptionally private.

III. RELATED WORK

The accessible symmetric key calculations like DES, AES and public key calculation RSA as found in [1] for the most part include more number of calculation or activity. Tumult hypothesis is a piece of science and utilized in a few propelling regions like nervous system science for EEG investigation, cardiology for early stage chick heart cells [2], climate prediction[3], correspondence, control and hypothesis of circuits[4], Direct succession Code Division Multiple Access framework [4,9]. Numerous scientists have shown mayhem groupings can be utilized for encryption of pictures [4,10].

Calculated work is one disarray work which has a property of high aversion to introductory condition, created arrangement is pseudo arbitrary non intermittent and flighty for appropriate decision of bifurcation boundary 'r'. Benefits of utilizing Chaos hypothesis explicitly for scrambling the