IMPLEMENTATION OF ADVANCE ENCRYPTION STANDARD (AES) TO SECURELY STORE AND MAINTAIN DATA

DISSERTATION-II

Submitted in partial fulfillment of the

Requirement for the award of the

Degree of

MASTER OF TECHNOLOGY

IN

Electronic and Communication Engineering

by

L Harikrishnan

Under the Guidance of

Mrs. Komal Arora

Electronics and communication engineering

Lovely Professional University Punjab

MAY 2017

CERTIFICATE

This is to certify that the Dissertation-II titled "Implementation of Advance Encryption Standard (AES) to Securely Store and Maintain Data" that is being submitted by "L Harikrishnan" is in partial fulfillment of the requirements for the award of MASTER OF TECHNOLOGY DEGREE, is a record of bonafide work done under my guidance. The contents of this Dissertation-II, in full or in parts, have neither been taken from any other source nor have been submitted to any other Institute or University for award of any degree or diploma and the same is certified.

Mrs. Komal Arora
Assistant Professor
School of Electronics and Communication Engineering
Lovely Professional University
Phagwara, Punjab

Examiner I Examiner II

ACKNOWLEDGEMENT

With great pleasure and gratitude, I would like to thank my supervisor Mrs. Komal Arora under her guidance and supervision I was able to complete my work. She helped me through all my difficulties through her counseling and discussion and also showed great interest providing timely support and suitable suggestion. I express my gratitude towards all the people associated with Internet, IEEE and the plethora of technical websites, forums, & groups which have helped me with the study materials for my work. I would also like to express my heartfelt gratitude to my parents, brother, sister and friends who have always supported and encouraged me to pursue my dreams.

L Harikrishnan
Reg. No.11210777

DECLARATION

I, L Harikrishnan, student of B-Tech- M-Tech(Dual Degree) Electronics and communication under Department of Electronics and communication of Lovely Professional University, Punjab, hereby declare that all the information furnished in this Dissertation-II report is based on my own intensive research and is genuine.

This thesis does not, to the best of my knowledge, contain part of my work which has been submitted for the award of my degree either of this university or any other university without proper citation.

Date:

L Harikrishnan
11210777

ABSTRACT

In technology there is a fast development in Network security because to safeguard the private and confidential information that cannot be compromised. In order to do so many application are introduced into the world. Best way to do so system requires best Cryptography algorithms which will help the user to protect their information in the database. Hackers always been a threat to the society because according to them every algorithm have a bugs, threats and backdoor which will provide them the access to the system. Every cryptographer provides three basic properties Availability, confidentiality and data integrity. For an organization there confidential records are more vulnerable to outside competitors. In order to protect the confidential records I have implemented AES algorithm with SMS authentication. It's an application which provides any organization to safe guard their records in their database. Using this method I remove all fake accounts, full access to the authorized user, timestamp which provide date and time of upload and download file and which user have accessed the database. This application does not require more algorithms and also the size of the file is reduced which helps us to keep more number of records inside the database.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABREVATIONS

AES	Advance Encryption Standard
DES	Data Encryption Standard
SMS	Short Message Service
UMTS	Universal Mobile Telecommunication System
LTE	Long Term Evolution
RSA	Ron Rivest, Adi Shamir and Leonard Adleman
PC	Personal Computer
ZITMO	Zeus Within The Mobile
USB	Universal Serial Port
M2M	Machine to Machine
OTT	Over The Top
ICS	Industrial Control Systems
PSTN	Public Switched Telephone Network
APN	Access Point Names
P2P	Peer-To-Peer
IP	Internet Protocol
DOS	Denial of Service
IOT	Internet of Things
VOLTE	Voice Over LTE
AKA	Authentication and Key Agreement
EPS	Evolved Packet System
GSM	Global System Mobile
RRC	Radio Resource Control
NAS	Non Access Stratum
CSFB	Circuit Switched Fall Back
IMSI	International Mobile Subscriber Identity
TMSI	Temporary Mobile Subscriber Identity
AUC	Authentication Center
UE	User Instrumentality

PKI	Public Key Infrastructure
QOS	Quality of Service
OTP	One Time Password
S-BOX	Substitution Box

Chapter 1: Introduction

1.1 INTRODUCTION

Network security is the most concerned area of research today. From the word 'security' means protecting our private asset which we cannot compromise. In the field of security cryptography hackers has always been a threat to the society and cryptography algorithm .Many company and organization have invested to much money in there confidential database to deny access to the illegitimate user and also to protect their private network as well as public network database. Such database always had been an eye catching material to the Hackers. Every cryptography algorithm has weakness and threats which may exploit by the hackers and threats have become a major area of study because as the threats increases then the assets are more vulnerable. In order to overcome all those threats we need a strong security algorithm or encryption. Security algorithm such as DES, SNOW 3G, AES and etc. As far as tested and discovered the most powerful encryption is AES encryption right now. Here, in our research AES algorithm have been implemented in our program in additional SMS authentication also been used to remove fake users and also maximum access to the legitimate user and also encryption of Data before feeding into the Database server of the organization. Cryptography provides three basic fundamental ideas as follows:

- **Confidentiality:** Ensuring that the secrecy is maintained and the data or information may not be accessible to unauthorized users.

- **Availability:** Resources are limited and loss of information is not tolerable. The information should be available when information request is made by the authorized users.

- **Integrity:** Data integrity should not be disturbed or modified by unauthorized user. And also the authorized user must obtain the accurate information.

1.2 LIST OF NETWORK SECURITY ALGORITHMS

- **SNOW 3G**: SNOW 3G is an stream cipher algorithm which is being used and chosen in 2006 as the major key set of UMTS integrity algorithms and confidentiality. This algorithm was the first-set of

LTE cryptographic algorithm because SNOW 3G properly matches the requirements of 3GPP regarding time resources and memory space. SNOW 3G have two categories i.e. A cipher with an inner condition of 608-bits instated by 128 bit key and a 128 bit.

- **ZUC**: ZUC is a stream cipher which was discovered particularly for "4G" standard named LTE. The ZUC algorithm comprised of different algorithms such as a stream cipher called as ZUC, LTE encryption algorithm (128-EEA3) and LTE integrity algorithm which uses hash function in ZUC core.

- **DES**- DES (Data Encryption standard) is a symmetric key algorithm used for the encryption in earlier electronic data. Earlier, this algorithm was a powerful encryption but development in the power of computers needed strong algorithm which will stop or face the hackers.

- **RSA**-RSA complete full form is Ron Rivest, Adi Shamir and leonardAdleman. RSA algorithm is asymmetric cryptography algorithm. It was released in 1978.In other words it is also called public key cryptography which uses pair of key along with Two large value of prime number of prime numbers.

- **AES**- AES(Advanced Encryption standard) is a symmetric cryptographic algorithm. Today AES is also called as the Rijindael modified AES created by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. Uses only single key and this key is transported through a secured medium to the receiver.

1.2 COMPARISON BETWEEN AES AND DES

- **DES explaination**:

  DES is a symmetric cryptography algorithm which was adopted and executed by National Institute of Standard and Technology in 1977.DES depends on the guideline of Feistel structure where information (Plaintext) is isolated into two parts. In DES the plaintext is in 64 bit with 56 bit key together is to produce cipher text.

  From the flowchart below we can see that initially 64 bit plaintext plain text is rearranged to get 64 bit permuted input. This permuted information is partitioned into two parts which have two 32 bit block each.

Both the halves undergo sixteen rounds flowing the same function. After undergoing sixteen rounds ,a final permutation is done which results in 64-bit ciphertext.

Expansion Permutation is used on of the 32 bit block and it is expanded to 48 bit right portion. Xor is done between the 48 bit block with 48 bit subkey obtained from the 56 bit key to produce 48 bit output. S-box is also called as substitution box where 48 bit output from Xor operation is again Xor to reduce to 32 bit. In P-box step the 32 bit result is obtained form S-box step where S-box output is again permuted to produce 32-bit permuted output.

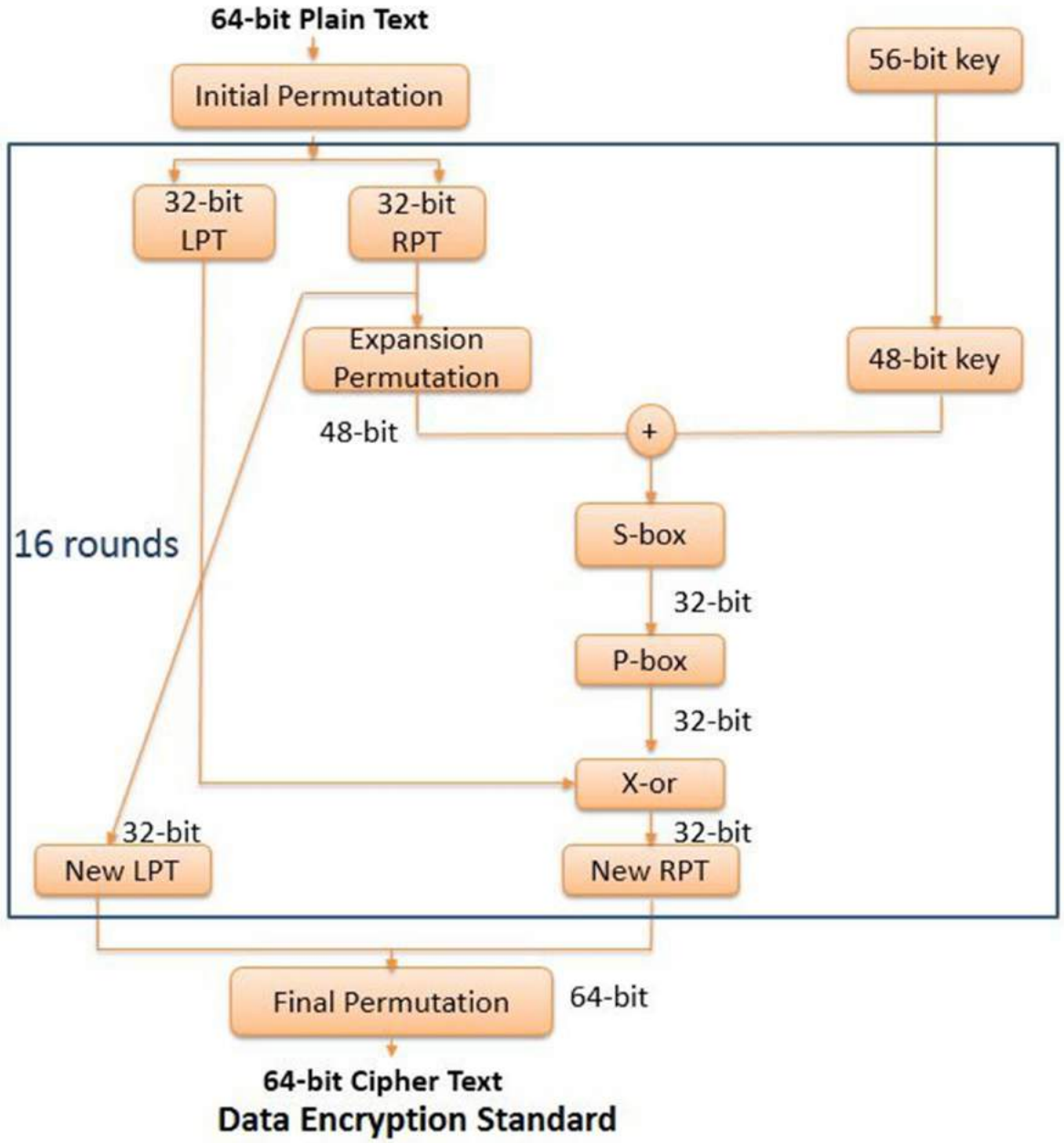

Figure1: Flowchart of Data Encryption Standard [23].

- **AES explaination**:

AES (Advanced Encryption Standard) is a symmetric cryptographic algorithm. This algorithm was published in 2001 by the National standard and Technology. AES was invented in order to overcome the drawbacks of the DES algorithm because its key was small and the algorithm performs quite slower.

In the AES algorithm it takes the input of 128-bit of plaintext and as well as 128 bit secret key. And forms a 128 bit block which 4 X 4 square matrix. It follows 10 rounds among which 9 contains subbytes, Shift Rows, Mix columns and Add round keys. And the 10^{th} round involves Subbytes, Shift Rows and Add round keys and 16 bytes of ciphertext.

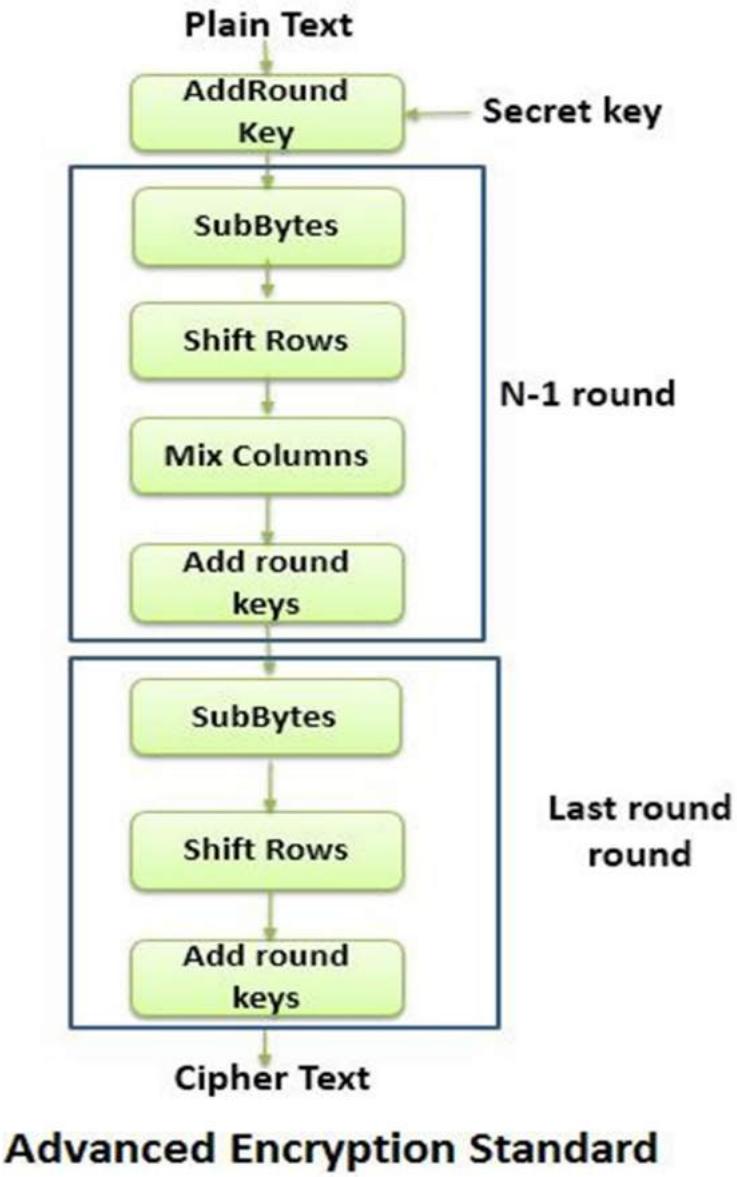

Figure 2: Flowchart of Advanced Encryption Standard [23]

1.3 Key difference between DES and AES

BASIC FOR COMPARISION	DATA ENCRYPTION STANDARD(DES)	ADVANCED ENCRYPTION STANDARD(AES)
Block	Data block is divided into two halves.	In AES the whole block is treated as single block.
Principle	DES works on the basic principle of Feistel Cipher structure.	AES works on the basis of substitution and permutation
Plaintext	Plaintext is taken as 64 bits.	Data is taken as 128,198 or 256.
Key size	DES key size is small.	AES key size is large as compared to DES.
Rounds implemented	16 rounds	10 rounds - 128 bit algorithm 12 rounds – 192 bit algorithm 14 rounds – 256 bit algorithm
Rounds Names	Permutation, Sbox, Pbox, Xor and Swap.	Sub bytes, Shiftrows, Mix columns, Add round keys.
Security	DES has a smaller key which results in less secure	AES has a large secret key which results in more secure.
Speed	DES is very slow	AES is faster as compared to DES.

Table 1: Difference between DES and AES [22]

1.4 MULTIPLE MARKET FORCES

- **Increasing malware**: Information proficient cell phones and tablets combined with giant, remote learning funnels as of now pull in imperative consideration from cybercriminal systems, today's "or" From an insignificant standard, malware-based dangers to cell phones were up 4000 p.c in 2012 and enlarged an extra thirty. Within theinitial3 months of 2013, with regards to McAfee® Labs™. Malevolent code engineers currently promptly take systems produced for private PCs and adjust them to the confined impression and advances of cell phones. For instance, ZITMO remains for "Zeus inside the Mobile," a reuse of the wide embraced Zeus toolbox that makes malware programming clear for non-specialized offenders. ZITMO executes cash misrepresentation by commandeering programs and SMS verification procedures. On the far side versatile malware, "out-dated" assaults on a ton of typical operative frameworks stay terribly successful, subsequently of several such gadgets (desktop, portable PCs) square measure associating through remote broadband through a strategy for "tying." Tethering through USB 4G "sticks," or possibly through telephones, puts these considerable measure of typical

gadgets inside the broadband web. In spots wherever fastened line broadband isn't out there, remote broadband can fill that market hole and present this assault possibility [4].

- **Social Engineering:**.Perhaps a ton of risky even than the spike in portable malware is that the spike in "SMiShing" and "phishing" assaults focusing on the social connections and interest of versatile clients. These assaults include malignant messages sent as messages or instant messages to be expended on the little screens and confined review territories of the numerous portable, great devices. The message tricks a client into clicking a connection, putting in associate application, or advancing toan web website. The result 'soft that personality and accreditations zone unit handed over by the client to the aggressors volitionally however unwittingly; and overwhelming extortion is that the result.

- **Unprotected devices**: Today, but five% of "smart" cell phones run security computer code code, and great gadgets speak to solelyatiny low part of cell phones as a full. This is often partlyas a consequence of essential handsets (or "highlight telephones") with confined abilities still structure eighty two% of handsets on versatile systems around the world. Be that as it may, this profile is ever-changing quick as cell phones costs drop cleave slash. A few places in Asia square measure transitioning from highlight telephones to good phones at rates moving toward twenty five% for every year3—which means keen gadgets arethe sole form of cell phones inside four years. Another reason for the deficiency of appropriation of security PC code is client esteem affectability. Paid clients represent over eighty five% of cell phones around the world. The apparent worth of a month to month premium for security PC code is restricted once the client's run of the mill month to month inconclusive quantity is just $10. great gadget clients square measure those driving bearers to conjecture in LTE. Benefit providers with immersed markets wish to offer versatile applications and learning administrations to cell phones and pill clients. "In 2012, a fourth-era (4G) affiliation produced nineteen times extra activity on the normal than a non-4G affiliation. in spite of the fact that 4G associations speak to solelyzero.9 % of versatile associations these days, they as of now record for fourteen% of portable information movement [4].

- **Machine-to-machine (M2M) communications and over-the-top (OTT) content:** New applications and administrations are likewise associating new classifications of implanted remote gadgets to make a quickly developing "Internet of Things," giving development and income chances to transporters even with declining edges in built up lines of business. These machine-to-machine frameworks append to systems (counting the Internet) from multiple points of view, yet remote systems regularly display an

ideal type of availability, empowering: remote industrial control system (ICS); area and following of transportation and coordination's; broadband conveyance of outsider video and gaming content; remote indoor regulators; health applications and services; creative home mechanization; and a great deal more. Regularly worked with constrained power, preparing, and memory assets, these gadgets require particular security. Aggressors will target such under ensured M2M frameworks to disturb basic foundation or commit fraud.

- Voice goes digital: As of now, 3G and 3.5G remote systems have jumped PSTN/wound consolidate systems to benefit provincial groups, particularly within the Asia Pacific, Latin American, and African areas. Get to focuses within the house give the local system interface, and LTE arranges square measure being conveyed to backhaul the information activity.

The growing data transmission of 4G gives a bigger assault surface to cybercriminals. The spill of information through a 24 kb– 256 kb 2G and 3G remote system turns into a flood of information with 3-150 Mbit 4G systems. Without forceful countermeasures, criminal exercises will expend such an extensive amount this new transfer speed that clients who have paid to move up to 4G administrations will get 2G speeds. Fig.1: outlines the attackers' computerized testing and examining programming and the activity from "enslaved" gadgets that can rapidly consume center data transmission. These activities can flood the remote architecturally private network (APN) that associates the cell phones of the 4G system to the Internet.

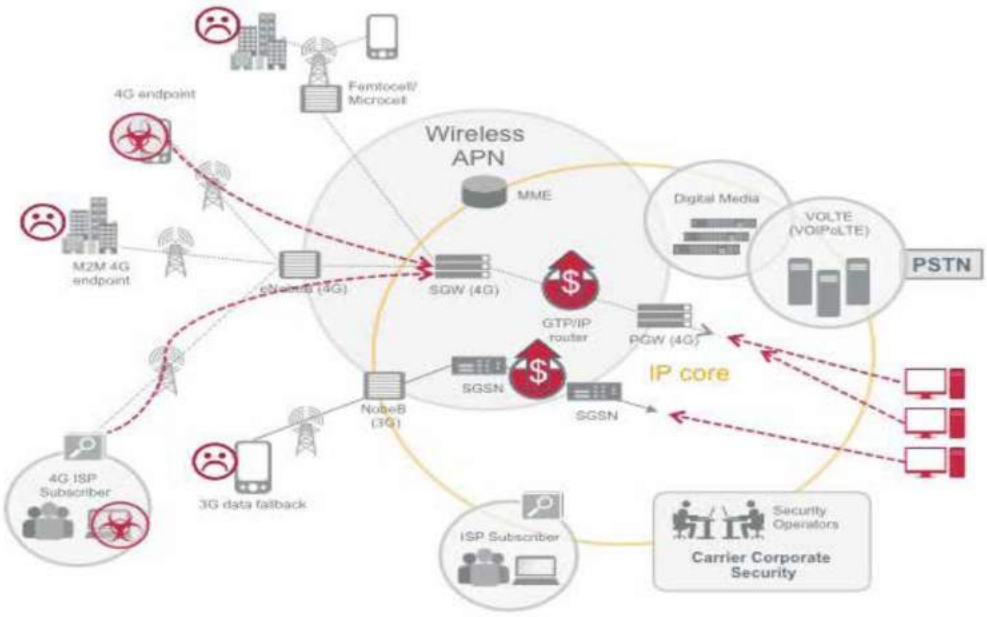

Figure 3: Attacks into a mobile network [4].

1.5 MOBILE TO MOBILE ATTACKS

Dissimilar to 3G movement that passages straightforwardly into the center IP organize from the cell phone, 4G activity is all IP-based and can travel specifically from cell phone to cell phone inside the remote APN. This "peer to peer" (P2P) correspondence decreases backhaul activity. Be that as it may, it additionally allows mobile to-mobile (Mob2Mob) assaults. A compromised cell phone can target and sweep huge quantities of other, locally neighboring, cell phones on the double, expending immense measures of range. This movement much of the time goes concealed by the transporter on the grounds that the remote APN to which the device interfaces has constrained instrumentation and couple of inside security capacities. Notwithstanding redirecting range, a portable to versatile assault depletes the battery on the casualty's gadget by keeping up a system association. The assault can likewise bring about a refusal of-administration (DoS)[9] circumstance because of flagging blockage. In an assault, the activity may enter the system from one cell phone, play out a mechanized output to search for devices with comparable IP numbers (demonstrating that the gadgets are on the same subnet), and afterward reach pull out over the 4G system to contact those gadgets. Once an aggressor has depleted one scope of IP addresses, the assault moves to the following extent and starts to assault and infect the new devices.

Unfortunately, the simple act of scanning for responding IP addresses of other mobile devices can cause severe DoS due to the previously mentioned signaling congestion. To avoid users being denied a connection, the operator would need to invest in better security or: more spectrum, more LTE base stations (eNodes), and more backhaul network—which lead to more capital expense, more operating expense, and more management complexity. The user may experience degraded service and also bear the burden of these incremental costs over time. Definitely, despondent users lead to account agitates.

1.6 Machine to machine fragility

The Internet of Things (IOT) incorporates not just devices overseen by individuals, for example, desktops and advanced cells, yet semi-computerized and completely robotized devices that control physical results, for example, movement lights, pipeline weight sensors, electrical matrices, and water utilities. These devices are in some cases alluded to as participating in "machine-to-machine" (M2M) organizing. Generally, these settled capacity devices were worked without much worry for security, since they utilized restricted, committed systems that were not associated with an open system. Straightforward testing of the

system can have unfavorable impacts by destabilizing controllers. Impeding potential alleviations, field-based sensors are asset obliged, with negligible memory and CPU to save: there is no "room" to introduce firewalls or even essential security capacities. At times, these devices run heritage, unpatched, and unpatchable working frameworks. As a rule, even current M2M frameworks and gadgets are not expected to work inside the antagonistic and unhygienic condition of the Internet—yet that is the thing that 4G will progress toward becoming without satisfactory security.

Whenever assaulted, gadgets may simply close down—all of a sudden, and now and then without a simple or quick recuperation. Interruption of ICS gadgets can prompt exorbitant common crises or death toll. This dreaded situation is driving basic Infrastructure administrators and the legislatures that direct them to put intensely in comprehension and actualizing more thorough security controls. For specialist organizations hoping to give the systems to these expanding new M2M applications, a level of security and mindfulness identified with portable on-versatile assaults will be a business empowering influence.

1.7 LAWFUL INTERCEPT COMPLIANCE

National regulations and licensing rules typically obligate carriers to intercept many different types of traffic when they receive a judicial order. In 4G networks, full interception for a given endpoint requires data collection at up to three different places in the IP network.

3.5.1: Edge cache traffic—Create a system for managing copies of frequently requested content that is stored at the edge of the network, so one copy can serve many endpoints without multiple downloads through the backhaul network.

3.5.2: Voice calls—Track and intercept voice over IP and voice over LTE traffic.

3.5.3: Internet traffic—Intercept “long haul” email and web interactions headed to and from the Internet directly (versus the edge cache).

Government regulators expect carriers to solve this problem before LTE services go live. Actually, regulators don’t necessarily possess any awareness of LTE or 4G network improvements. They simply require that judicial orders are fulfilled. The problem of “how” is largely left to the service provider to

figure out. Furthermore, lawful access requests normally accompany valuable little remuneration for specialist co-ops, so the more productive and rich the arrangements, the better! Planning this interference, checking, and accumulation ability into the important purposes of the system will enable you to protect your system consistence with legal get to demands and legal requests.

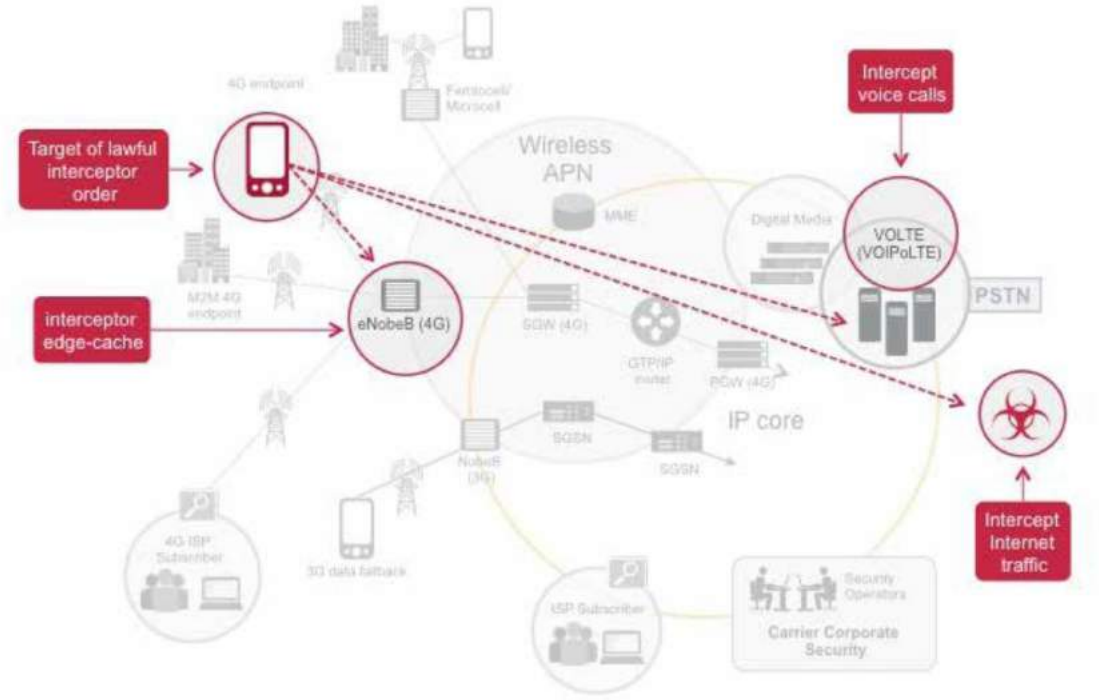

Figure 4: Lawful intercept compliance [4]

1.8 CONTENT AND MEDIA DELIVERY

Paid-for substance and media, for example, films or music-on-request, are another component of the 4G broadband biological community. They show the possibility of critical extra incomes to specialist organizations, particularly since up to 50 percent or a greater amount of the information going over the Internet is as of now video, as per Cisco. Making video and music accessible from limited entrances associated specifically to the remote APN can offer execution and assortment that can't be had from "over the top" administrations got to by means of the Internet. Just like the case with VOLTE, unapproved get to and disavowal of-administration assaults can imperil expected income from broadband media administrations, corrupt administrations, and dissolve membership and selection rates. Bearers ought to anticipate that assailants will endeavor to upset substance conveyance frameworks amid pinnacle times. Web hoodlums, hack activists and different malignant gatherings are capable at unleashing their assaults amid real occasions—World Cup matches, races, or illustrious weddings, for instance.

Also, discount disturbance of a communicate administration will be a great deal more unmistakable than a substantial number of generally irrelevant dropped calls. Endorsers who have paid a premium to watch a noteworthy wearing occasion will rapidly share their outrage through online networking. This harms your association's notoriety and can hose memberships and long haul reception of new administrations.

1.9 AIMS AND OBJECTIVES:

The objective of this thesis are as follows:

- To deny access to the unauthorized user by using authentication code such as OTP number.
- To eliminate all fake accounts and also provide easy interface to the user.
- To providing confidentiality by encrypting the file using AES algorithm.
- To provide timestamp so that we can see which user logged on to the database.
- Encrypting the file helps in reducing the size of the file.
- To make user friendly interface to the authorized for download and upload option.
- To reduce the size of the file by using the AES algorithm so that the server database can keep many records.
- To make the file unreadable we implement encryption so that the file in the database be unreadable to the hackers.
- To analyze the performance of each round in the AES algorithm.

Chapter 2: Literature review

NouraAleisa [3] described the near review between the DES and AES. Here AES utilizes 3 basic key lengths, 128, 192, and 256 bits, though for DES the encoding key lengths 56, 112, and 168 bits. DES contains a shorter length and weaker encoding keys when put alongside AES. AES is safe towards to differential, truncated differential, direct, introduction and sq. assaults, in refinement to DES that is at danger of dangers like differential and direct science since it has feeble substitution tables. Encoding technique time is a great deal of in DES since it is contrasted with AES encoding. Moreover, AES is taken into account to be unbreakable as compared to DES as a result of DES encoding is prone towards several threats. AES is being a lot of helpful in each hardware and software package. Conjointly it works quickly and with efficiency in little devices like good phones. AES have larger blocks as compared to the DES blocks.

Tyson Macaulay[4] discussed about the 7 Deadly Threats to 4G. This paper provides a detailed description about the threats such as:

- Wireless APN flooding.
- Mobile to mobile attacks.
- eNodeB/Femtocell/microcell compromise
- Machine to machine fragility.
- Lawful intercept compliance.
- VOLTE service assurance.
- Content and media delivery

AlyaaGhanimSulaiman et al. [8] has done a comparative study on 4G/LTE cryptanalytic algorithms. In half of the paper the author evaluated the core algorithms supported completely different views like assessing the execution of LTE's center calculations in equipment stage, Evaluating LTE's center calculations from security viewpoint and quality assaults on LTE's algorithms. Conjointly mentioned on attacks supported formula quality like time, memory and knowledge. And conjointly showed the attacks that square measure prone to LTE algorithms like ZUC, SNOW 3G and AES.

Mahdi Aiash et al.[6] discussed about the difficulties which are in 4G systems. a decent thanks to deliver the goods this is frequently by investigation the possibility of stretching out current security systems to 4G systems. Consequently, this paper utilizes the X.805 normal to analyze the possibility of executing the 3G's Authentication and Key Agreement (AKA) convention in an exceedingly 4G correspondence structure like YComm. Amid this paper, they analyzed whether or notit'sdo able to utilize 3G security instruments like AKA for 4G frameworks like Y-Comm. The X.805 structure are wont to approve the AKA instruments on Y-Comm, thereupon uncovering what advance safety efforts square measure required to secure 4G frameworks. the rest of the paper is organized as takes after: Describing the plan of the X.805 ordinary, Explaining in regards to the AKA convention of 3G systems, Introducing the Y-Comm structure as partner case of 4G systems though conveying the AKA convention with Y-Comm; this proposition is analyzed exploitation the X.805 typical.

VikasKaul et al [7] has done a detailed explanation about the new security enhancements in knowledge transmission for next generation crypto graph lightness the doable weaknesses at intervals this AES cryptography algorithmic program. Associate in Nursing increased cryptography methodology with AES algorithmic program is employed here at intervals TLS. Sweetening is completed in AES by initial exploitation chaos so modifying the S-box .The use of chaos sequence makes the key area infinite and therefore the static S-box is created dynamic exploitation cipher key. to extend the quality of the system, AES is integrated in spherical structure. The analysis focuses on: Encryption- decipherment time, Throughput-speed and Avalanche result. Results show that speed of around 2Mbps is achieved that is compatible with LTE networks. Additionally performance analysis of ancient AES and increased AES don't show abundant deviation and then increased version will bea decent various. additional attack resistance and quality is achieved by group action AES in a very spherical structure which provides non one-dimensionality to the system .The number of rounds within the increased system will be created variable so it can do the specified turn out and speed creating the system additional compatible to the next generation networks.

Ghizlane Orhanou et al. [11] introduced a brand new arrangement of cryptanalytic calculations is being anticipated for incorporation inside the “4G” portable ordinary known as LTE (Long Term Evolution), and in this manner the calculations square measure opens for open examination. The new arrangement of secrecy and trustworthiness calculations EEA3/EIA3 depends on the new stream figure ZUC. Inside the gift paper, we tend to have an enthusiasm for making the confirmation and subsequently the execution yet

as movement the scientific examination of the 2 calculations, as we have done, in past works, with the primary2 sets of the LTE cryptanalytic calculations EEA1/EIA1 and EEA2/EIA2. The check of the classification algorithmic lead comes about on an adjustment of the anticipated 3GPP algorithmic manages code to satisfy the particulars necessities. Security is a fundamental element of the third and fourth era of the 3GPP family and its development is an essential issue. EPS (Evolved Packet System) (or LTE-SAE, future Evolution - Service design Evolution) gives security features in an exceedingly comparable way as its antecedents UMTS (Universal Mobile Telecommunication System) and GSM (Global System Mobile). furthermore to the shared confirmation usefulness of the system and in this way the client, 2 alternative security capacities range unit given to confirm information security amid its transmission over the air interface and through the LTE-SAE framework: figuring of every client and flagging data (in the RRC (Radio Resource Control) layer) so asto affirm their secrecy, and flagging data honesty assurance.

PreranaChoudhari et al. [12] has presented the planning and analysis of security improvement for information transmission in 4G networks. a complicated encoding technique with AES algorithmic program is employed here. Improvement is finished in AES by modifying the S-box. The static S-box is formed dynamic mistreatment cipher key. To extend the quality of the system, AES is employed in spherical structure.

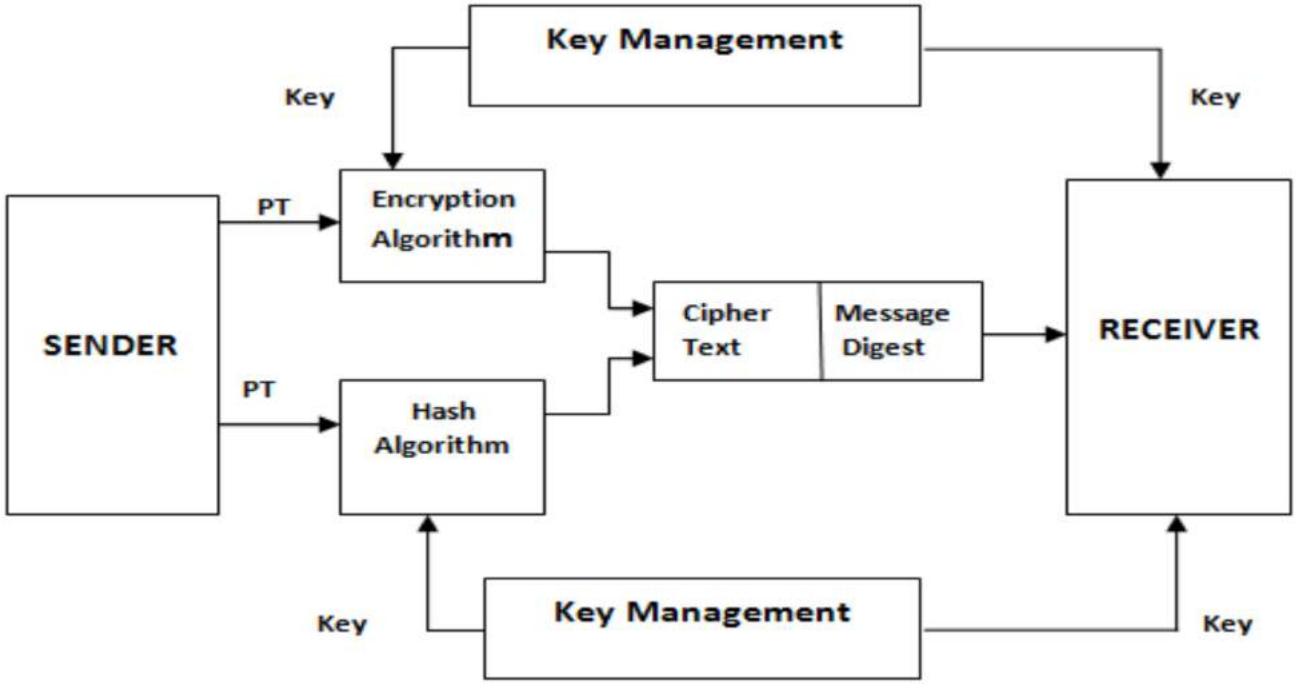

Figure 5: Block Diagram AES System [12]

There are major drawbacks in different 3G/4G cipher algorithmic programs thence AES cipher algorithm is employed within the planned system. as a result of AES is that the most secure algorithmic program. There are sure attacks on the AES algorithmic program like linear, algebraical attacks the nceto extend the complexness AES is employed in spherical structure. The S-box of AES algorithmic program is improved by creating it dynamic. This work is targeted on improvement of coding algorithmic program. the entire science system has been developed during this project. This includes coding of information, key exchange and message authentication. RSA is employed for key exchange and SHA-256 for message authentication. additional performance analysis of hand-picked is oscelescoding algorithms should be done.

Anastasios N. Bikos et al. [13] has done a elaborative study on the potential security problems which will occur within the preparation of the long-run Evolution/System design Evolution protocol in rising 4G wireless technologies offers a photograph of this state of the art. Most of the analysis comes we have a tendency to mentioned during this article may simply integrate with the approaching SAE/LTE protocol readying within the 4G wireless network surroundings (that is, the service layers usage) in an efficient, layered, and intelligent manner to confront the rising challenges of recent un even security threats. This work, though, still leaves United States with the necessity to check the simplest compromise for together with a quality protocol and key management answer that most closely fits the SAE/LTE design, whereas at a similar time maintaining a multilayered and dimensional security approach. These 2 aspects—the choice of an easy ciphering key hierarchy distribution mechanism (Hokey project) and providing a superimposed network security design (Y-Comm and X.805 recommendations)—emerge as in all probability the foremost promising and novel solutions for effort LTE/SAE security problems on 4G wireless networks

Guan-HuaTu et al. [14], has provided a support voice calls important to mobile users and carriers, 4G LTE cellular networks adopt 2 solutions: VoLTE(Voice Over LTE) and CSFB (Circuit-Switched Fall Back).during this paper, they disclose that each schemes are harmful to mobile users from a security perspective. The adoption of the newest VoLTE permits associate assailant to governs the radio resource states of the victim's device in a very silent decision attack, thereby debilitating the victim's battery 5-8 times quicker. CSFB exhibits 2 vulnerabilities of exposing 4G↔3G network switch to adversaries. might} be additional exploited to launch Ping-Pong attacks wherever mobile users may suffer from up to ninety one.5% performance downgrade, or 4G denial-of-service (DoS) attacks wherever mobile users arempty 4G LTE property while not their consent. we have a tendency to devise 2 proof-of-concept attacks as

showcases, and demonstrate their viability over operational LTE networks. we tend to analyze their root causes and uncover that the issues exist on the face of it sound design selections for purposeful correctness however such selections bear surprising and intriguing implications for security style. we finally propose remedies to mitigate the attack injury.

VidyaKrishnamoorthy et al. [15] discussed on fourth generation (4G) network is new wireless technology that gives a lot of advancement to the wireless market. In 4G, the forward key separation plays a significant role in relinquishing method and it are often vulnerable attributable to the presence of scalawag base stations. Sporadically change the foundation key hold on in base stations reduces the consequence of the attacks. But, the choice of the simplest potential key update interval may be a obscure issue because it is tough to realize stability between the degree of the exposed messages and therefore the signalling load. To attack the service of internet sites, competitors register into the web site multiple times and degrade the performance of the online server. Hence, this paper proposes a technique that maintains history/status tables to stay a record of the media access management address in associate computer network atmosphere. The distinctive addresses, the media access management and web protocol addresses area unit maintained within the standing tables and wont to establish every node clearly. The projected system guarantees genuineness of the host connected within the atmosphere. Finally, the performance analysis shows that our projected system provides higher security and vital reduction in latency.

Ghizlane Orhanou et al. [16] has done an elaborative review on SNOW 3G which may be a stream figure algorithmic program that had been shaped and picked in 2006 on the grounds that the heart of the second arrangement of UMTS secrecy and trustworthiness calculations. It's been unbroken because the motor of the arrangement of LTE crypto logical calculations also. The justification is that SNOW 3G regards appropriately the 3GPP necessities relating to the time and memory assets. This stream figure might be a2parts stream figure with an inside condition of 608 bits instated by a 128-piece key and a 128-piece organize vector IV. inside the gift paper, we'll keen on SNOW 3G algorithmic program structure, its part sand so its 2 distinctive operation modes. From that point forward, on its proficiency by taking in its time and area complexness. Here elaborate investigation of the stream figure SNOW 3G structure has been administered. Studied the 2 intuitive modules that represent the SNOW 3G algorithmic program and their various parts. the objective is to handle enough SNOW 3G operation and to check its time and area complexness. SNOW 3G incorporates a straight time multifaceted nature, that certification proficiency and quickness throughout the encryption/unscrambling strategy. In addition, SNOW 3G incorporates a

consistent area complexness. SNOW 3G expend a proceeding and as of now notable quantity of brief memory that is incredibly helpful for frameworks with tiny remembering like portable gear. From the investigation of the time and area complexness of SNOW 3G, we will reason that this stream figure was well been the focal point of the classification and uprightness calculations of the third era of portable Telecommunications since 2006, and conjointly for the arrangement of security calculations for LTE.

Okoye Emmanuel Ekene et al. [17] discussed about the Evolved Packet System Authentication and Key Agreement (EPS-AKA) gives security and protection improvements in third Generation Partnership Project (3GPP), the International Mobile Subscriber Identity (IMSI) is dispatched in clear content so as to get benefit. Various endeavors to supply security systems to protect this distinctive non-open personality haven't brought about ways enforced to defend the disclosure of the IMSI. The presentation of the IMSI conveys hazard to client security, and information of it will result in many uninvolved and dynamic assaults focused at particular IMSI's and their individual clients. Assist, the Temporary Mobile Subscribers Identity (TMSI) produced by the Authentication Center (AuC) are observed to be vulnerable to rainbow and savage constrain assaults, therefore An offender UN organization gets hold of the TMSI will be ready to perform social designing in following the TMSI to the comparing IMSI of a User instrumentality (UE). This paper proposes amendment to the EPS-AKA verification strategy in 4G future Evolution (LTE) Network by together with the work of Public Key Infrastructure (PKI). The correction would end in the IMSI never being discharged inside the reasonable in an untrusted organizes.

RajaniMuraleedharan et al. [18] Suggested that Mobile systems turned into an important a piece of our everyday lives. the information imparted needs secure interchanges to high risk and nature of-administration (QoS). Subsequently, arranging a 4G system to supply secure IP-based administration by trade off requirements like battery life, data measure and size to portable clients might be a troublesome errand. amid this paper, an intellectual system utilizing partner degree evolutionary run, Swarm Intelligence, is anticipated. This structure utilizes a totally interesting methodology that uses an esteem play out that picks the best parameters to supply relate degree versatile nature of administration (QoS) upheld the client's yearnings. This approach guarantees capacity and quantify ability between totally unique regulation procedures inside the physical layer and upgrades security against Denial of Service assaults like sticking assaults and flag assault. the most commitment amid this paper is applying partner degree versatile psychological manage to the 4G system to help QoS and security of the system while not utilizing any convoluted procedures. Since 4G is focused on giving heterogeneous administration a

subjective insight is most appropriate as they'll develop and perform as indicated by the client's necessities rather than old settled methodologies. There range unit a few modern routes that to disentangle DoS assaults that generally increment the response time and energy of the framework, utilizing our approach DoS is all around caught with ninety six location rate while accomplishing partner degree versatile adjustment, mistake amendment, control administration, handover, QoS, client communications and movement prioritization. the information gathered by the tablet rundown are frequently expansion an investigated for abnormalities utilizing hypothesis organize, which might be nourished back to the operators to anticipate the DoS assault. Modulations like OFDM, W-CDMA are fused in our future work to assess period 4G arrange.

Eddy PrasetyoNugroho et al. [19] created a system which will eliminate and prevent from fake accounts. In order to do so the author used SMS authentication code. This is created using AES algorithm and send to the authorized users Gmail account or mobile number. And this code is also providing with timestamp and also be used as one time password. Modification is made in the rounds of the AES algorithm such as confusion and diffusion. Changes are done in the S-box and shift Rows. And this modification is tested in Avalanche Effect and Randomness Test.

Ali Akbar Pammu et al. [20] made an arithmetic operation which will hide the and shield the calculation from Side Channel Attack. Likewise this operation runs parallel with S-confine operation request to conceal the spillage control dispersal. There are 2 enter choices in our arranged covering strategy. In the first place, the work of the math hiding is autonomous with S-Box operation and its energy dispersal is prevailing over the S-Box. Thusly, the dependency of the entire power scattering with prepared information inside the AES algorithmic control is similarly low.

Mohamad Ali Sadikin et al. [21] used both symmetric and asymmetric algorithm. In order to provide both encryption and digital technique to medical data to avoid problems of stealing or forgery of medical data. Authors used java programming to implement AES 265 bit , RSA 2048-bit algorithms and SHA 256 .This algorithms provides confidentiality ,integrity non repudiation and authentication. This research also does test such as block testing and white box testing in order to test the software input, output, and code without testing design and process happens in the system.

Chapter 3: Rationale And Scope Of The Study

3.1: BENEFITS OF THE EARLIER WORK PUBLISHED

- In earlier research paper, the author's main focus was on to create new account using SMS authentication code.
- The SMS authentication code was created using AES algorithm.
- The Author changed the AES algorithm on the basis of confusion and diffusion.
- Implemented a new concept such as OTP number. OTP number is created using AES algorithm which is best thing of the Base paper.

3.2: PROBLEMS AND SOLUTION

- In earlier research paper the author discussed about how to create the new account but didn't account what if other authorized user wants to access the data.
- The earlier research had not considered the size of the file so , in this research size of the data is also taken into account by encrypting the file before uploading into the database.
- When the size of file is reduced, more number of file can be kept inside the database.
- Timestamp is also been provided i.e when user logged on to the server, time, date and which file did user accessed. So no malpractice can be found.
- This research also removes all fake accounts but also provide access to all authorized user.
- Even hackers attack the database it would be a useless effort because whole file is encrypted in the database.

Chapter 4: Research Methodology

4.1. AES INTRODUCTION

The Advanced Encryption Standard, a calculation otherwise called Rijndael altered AES after its creators Vincent Rijmen and Joan Daemen. This calculation follows up on 128-piece squares and can utilize a key of 128, 192 or 256 bits long. For encryption, each round comprises of the accompanying four stages:

1) Substitute bytes,
2) Shift rows,
3) Mix columns, and
4) Add round key.

5.2: AES S-BOX

The Rijndael S-box is a grid i.e. square cluster of numbers utilized as a part of the propelled Encryption Standard (AES) cryptographic calculation. The S-box is the substitution box which fills in as a query table. The S-box is created by deciding the multiplicative converse for a given number in GF (2^8)[1].

4.2 FLOW OF MODEL DEVELOPMENT

- 128 bits key length is utilized for the improved AES calculation.
- The framework encryption and unscrambling is the same as conventional AES calculation.
- The round capacity of encryption process is likewise comparable as the conventional AES calculation.
- There is extra period of making S-box dynamic.
- Before sub byte arrange, the static S-box is changed over into dynamic utilizing figure key.
- The round structure of AES is utilized.
- Dynamic S-box is connected in the round structure of AES as we take 256 bit information as Input to the framework.
- Here the Input Data is part into two squares of 128 bits each.
- One Block is given as Input to the AES area of the System.
- The other Block is given as Input to the AES area of the System in the following round according to the round structure.

- This is accomplished for 1, 2, 5 and 10 adjusts individually.
- These yields are then joined together to shape 256 bit block of encoded information.

4.3 DYNAMIC S-BOX GENERATION

Here S-box is made dynamic as appeared in Fig 6. The hexadecimal digits of the key are XORed with each other and acquired number is utilized as the move value [1]. S-box is turned by that move esteem. The backwards S-box is likewise adjusted after S-box to acquire rectifies reverse qualities.

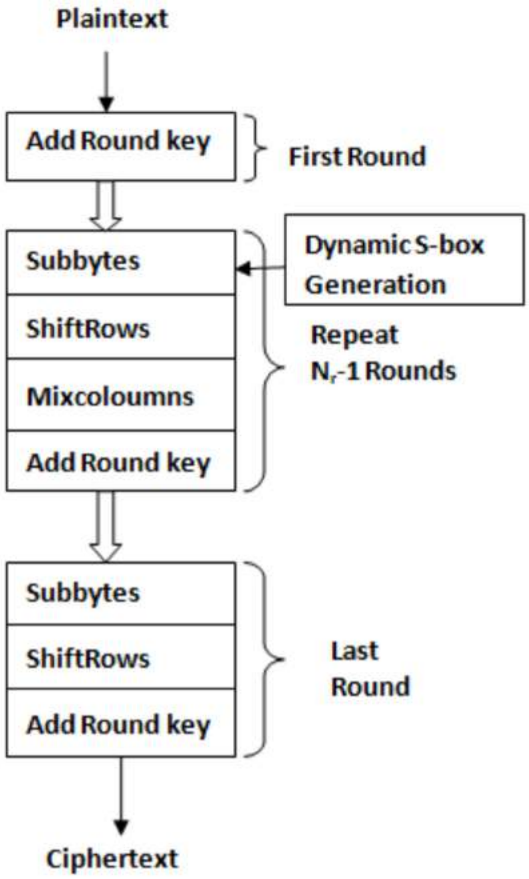

Figure 6: AES dynamic S-box [7]

4.4 ROUND STRUCTURE WITH DYNAMIC S-BOX

The Round structure of AES is utilized as appeared in Fig. 7. Here the Input Data is part into two blocks of 128 bits each. One Block is given as Input to the AES area of the System. The other Block is given as Input to the AES segment of the System in the following round according to the Round structure. This is accomplished for every one of the ten adjusts separately. These yields are then joined together to frame 256 bit block of scrambled information. The dynamic S – box is connected to the Round structure of AES as

appeared in Fig. 7. In the round structure, AES is connected n times to the piece of information, henceforth add up to n different S-boxes are made consequently it is called dynamic S-box.

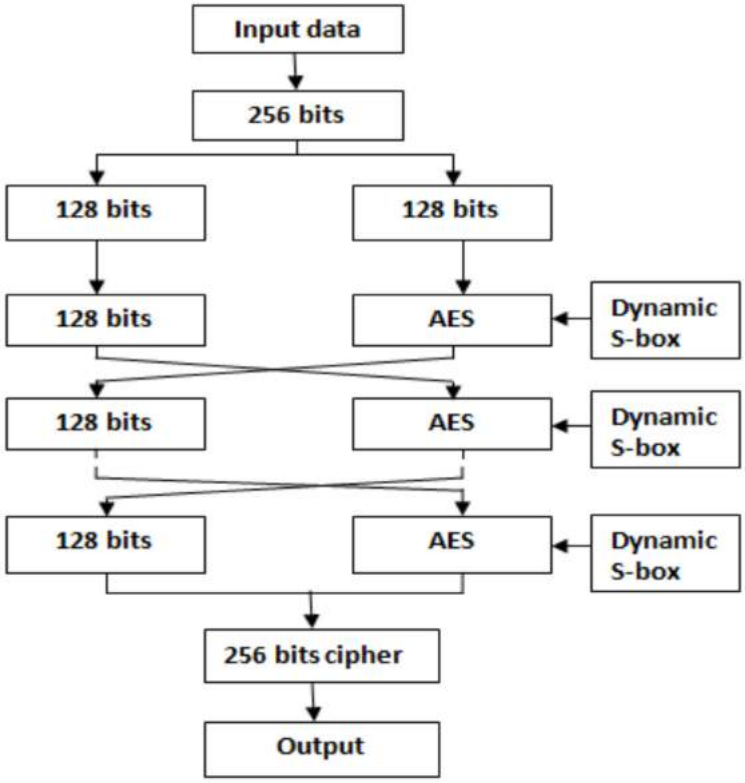

Figure 7: Round AES [7]

4.5 GENERATION OF CONTROL KEY AND ENCRYPTION KEY

There is an additional step of generating two keys shown in Fig 8. The control key is used to control controls the times of row-shift Encryption key is used as add round key.

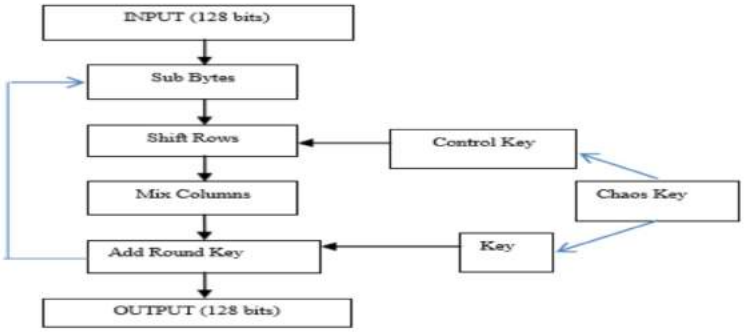

Figure 8: Round AES -2 [7]

4.6 Round structure with Control Key and Encryption key

The Round structure of AES is utilized as appeared in Fig 7. Here the Input Data is part into two squares of 128 bits each. One Block is given as Input to the AES area of the System. The other Block is given as Input to the AES segment of framework in the following round according to the Round structure.This is accomplished for every one of the ten adjusts individually. Yields are joined together to frame 256 piece square of scrambled information. Control Key and Encryption key is connected to the Round structure of AES as appeared in Fig. 9 [7].

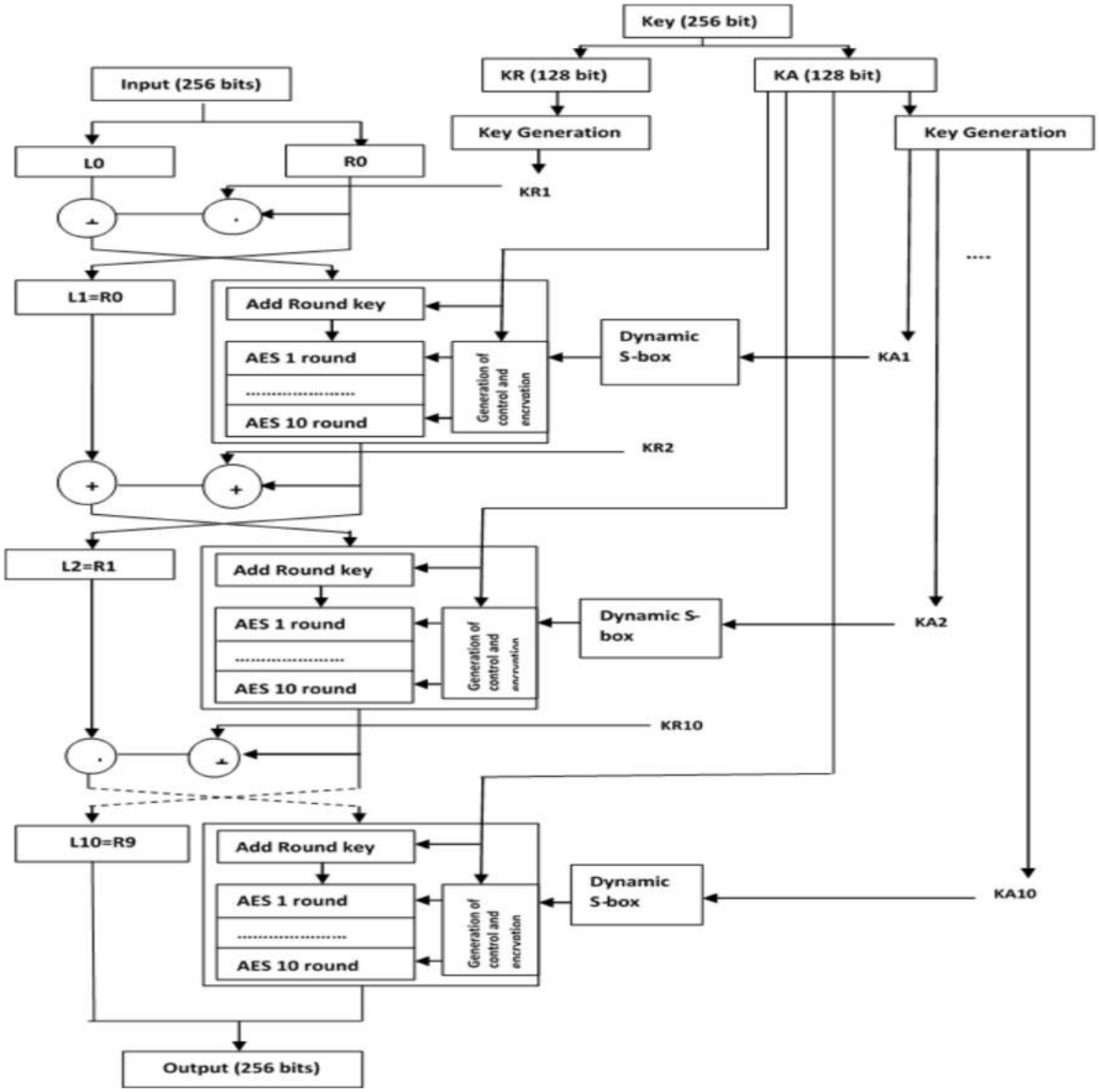

Figure 9: Round structure with Control Key and Encryption key [7]

4.7 PROPOSED SYSTEM

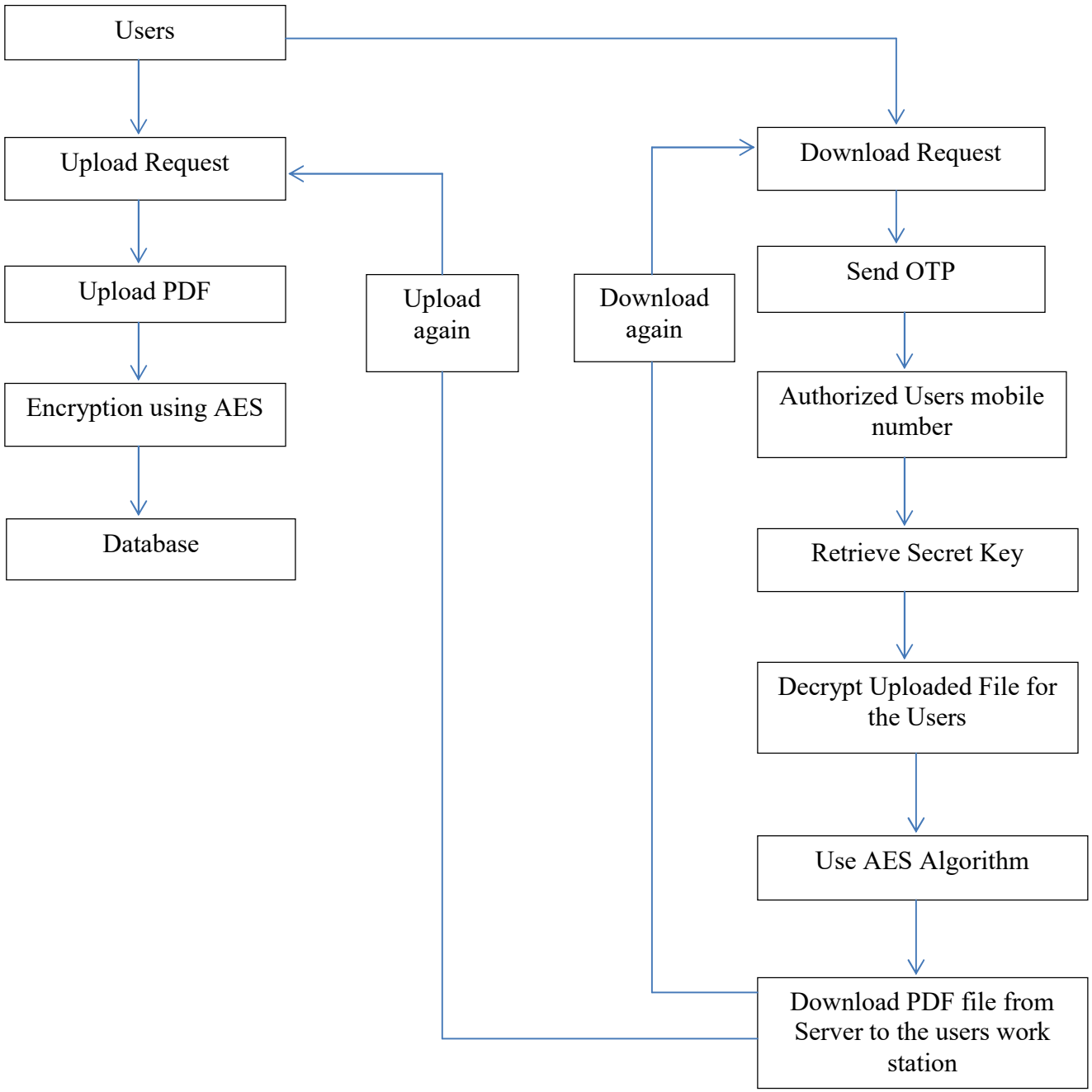

Figure 10: Proposed System Block Diagram

Steps involved In Uploading the File:

- When Users makes request to the server for uploading the file first makes the request to the database.
- File such as PDF is uploaded to the server database.

- Before uploading to the server the file is encrypted using AES algorithm and the secret key is dynamically generated.
- And the encrypted file is stored in the database which size is very less which is the biggest advantage in this research.

Steps involved in downloading the file:

- When users makes request to the server for downloading the file first makes the request to the database.
- In order to check whether the user is authorized user so it sends a OTP number to the users mobile number.
- Once the user prompt the OTP number from background process the secret key is retrieved.
- By doing so the fake account is eliminated and it is very effective
- Once secret key is retrieved the uploaded file which is in encrypted format is decrypted to the original file.
- After Decryption, the user is able to download the original file.

Chapter 5: Simulating Cryptography Algorithms

5.1 SIMULATING THE PERFORMANCE OF CORE ALGORITHMS IN HARDWARE PLATFORM

Actualizing the crypto logic calculations in FPGA (Field Programmable Gate Array) equipment stage that is a ton of appropriate for 4G period to affirm security of remote correspondence, in line with Lingchen Zhang[8], the aftereffects of executing SNOW 3G and ZUC in Xilinx's Virtex-5 FPGA as investigation gadgets demonstrated that the SNOW 3G performs higher yield than ZUC and expended less assets than ZUC as appeared in table one to boot, each SNOW3G and ZUC are versatile in leveling completely different output with the devoured space.

Algorithm	Technology	Freq(MHz)	Area(Slices)	Throughput(Mbps)	Throughput/Area
ZUC	Virtex-5	108	356	3456	9.7
SNOW 3G	Virtex-5	366	164	11712	71.4
AES	Virtex-5	350	349	41000	11.67

Table 2**:** Comparison on the performance of cryptographic Algorithms on FPGA hardware platform [8]

5.2 SIMULATINGALGORITHMS FROM SECURITY PROSPECTIVE

The primary targets of security are to ensure privacy and uprightness of the calculations. Furthermore, it's important to comprehend the time, space and data quality of an algorithmic manage to comprehend its potency throughout the execution. Be that as it may, steady alludes to the least complex instance of running the algorithmic rule whereas exponential alludes to the most pessimistic scenario of running the algorithmic run the show. The time, space and knowledge quality are variables to live the amount of security that is offered by the algorithmic run the show. Thusly, amid this area introductory we will demonstrate the quality estimations of the thought calculations and so we are going to justify the quality of each set severally that are given in Table a couple of and Table three severally.

LTE algorithms	Type	Key size (bits)	Memory(Space complexity)	Time Complexity
SNOW 3G	Stream Cipher	128-bit	O(1) Constant	O(n) Linear
AES	Block Cipher	128, 192 or 256	O(1) Constant	O(1) Constant
ZUC	Stream Cipher	128–bit	O(1) Constant	O(n) Linear

Table 3: The space and time complexity of the core algorithms [8]

LTE Algorithms	Based on	Type	Security Goal	Key Size	Key Stream	Time Complexity	Space Complexity
UEA2/EEA1	SNOW3G	Stream Cipher	Confidentiality	128-bit	32-bit words	O(n) Linear	O(n) Linear
UIA2/EIA1	SNOW3G	Stream Cipher	Integrity	128-bit	32-bit words (MAC-I)	O(n) Linear	O(1) Constant
EEA2	AES	Block Cipher	Confidentiality	128-bit	128-bit	O(n) Linear	O(1) Constant
EIA2	AES	Block Cipher	Integrity	128-bit	128-bit(MAC-I)	O(n) Linear	O(n) Linear
EEA3	ZUC	Stream Cipher	Confidentiality	128-bit	32-bit words	O(n) Linear	O(n) Linear
EIA3	ZUC	Stream Cipher	Integrity	128-bit	32-bit words	O(n) Linear	O(n) Linear

Table 4: Space and Time complexity of the three sets of security algorithms [8]

It will bedetected from the Table 4, AES offers constant values for each time and housecomplexnessthatis that the best case supported the quality security criteria, which means that AES is extremely economical throughout the execution in terms of your time and house. Moreover, there's a similarity between ZUC and SNOW 3G wherever each of them supply constant house complexness and linear time complexness. It will be seen that the comparison of the confidentiality and integrity algorithms of LTE network showed an honest end in term of house complexness that provides either constant or linear worth. which means that it provides high speed and potency throughout implementing the cryptography and cryptography operations and additionally this results of house complexness is suited to mobile equipment's wherever the most message length that standardized by 3GPP is 20, 000 bits.

5.3 COMPLEXITY ATTACKS ON CORE ALGORITHMS

In this section, Common attacks on every LTE‘s core algorithmic program to indicate the resistance of every algorithmic program against specific attack like guess and determine attack, differential attack , meet within the middle attack et al. learning the time and space complexness of every attack on each LTE algorithmic program will offer use stronger image of the resistance of every algorithmic program against potential attack, the main points of the complexness attacks with the reference will be found in Table 4. The results in the Table 4 shows that ZUC includes a higher resistance than SNOW 3G against totally different attacks like Guess and verify attack with 2403 time complexness and Differential chosen IV Attack with 299.4 time complexity[2]. per Tang Ming (2012)[8], the ZUC algorithmic program will resist totally different cryptanalytic attacks like weak key attacks, guess-and-determine attacks, algebraic attacks, temporal order attacks.

In addition, Tang explicit that once Chunfang Zhou extended the differential properties of the data format stage of ZUC from twenty rounds to twenty four rounds, they found that ZUC will still resist against chosen-IV attacks. by experimentation, supported Tang Ming study the ZUC algorithmic program shows some weaknesses against DPA attack . Eventually, from learning the attack complexness on AES algorithmic program, the values of the attack complexness that are bestowed in Table (4) will not exceed the 7-rounds of 128-bit that the studies thus far approved that AES has high effectiveness in resisting potential attacks as a result of there’s no attack thus far can break AES algorithmic program of the full-rounds .

Going more, perSha'banSahmoud (2013)[5], AES shows terribly high resistance against multiple attacks like brute-force attack, linear attack and differential attack. The high immunity of AES is attributable to its ability

to totally different lengths of keys to guard from different attacks. We will infer that ZUC and AES supply terribly high invulnerability against various assaults though SNOW 3G offers less resistance against very surprising assault than ZUC and AES.

LTE algorithm	Attack	Complexity		
		Time	Mem	Data
ZUC	Guess and Determine	2^{403}	–	9×2^{32}
	Differential chosen IV Attack	$2^{99.4}$ and 2^{67}	–	$2^{13.3}$ and 2^{54}
SNOW 3G	Guess and Determine	2^{320}	–	9×2^{32}
	Differential Resynchronization Attacks	$2^{57.1}$	2^{25}	2^{33}
	Differential chosen IV attack	$2^{57.1}$	2^{25}	2^{33}
	Chosen IV resynchronization attacks.	2^{53}	–	2^{57}
AES	A collision attack	2^{72}	–	2^{32}
	SEQUARE	2^{120}	–	2^{119}
		$2^{36.5}$	–	2^{8}
	Meet-in-the-middle	2^{128}	–	2^{32}
		2^{40}	2^{40}	–
	Impossible differential attack	2^{120}	2^{45}	$2^{115.5}$
	Differential Fault Analysis	2^{40}	2^{32}	–
	Differential Attack	2^{47}	–	2^{24}

Table 5: Survey on complexity attacks on different algorithms [8]

Chapter 6: Results and Discussion

6.1 AES RESULTS

Input string: 123113121321313564648

Secret Key: const

Encrypted value: a5zwdmQbMQBe1h2EEz8Y7h0uLOyiGt6g40ztCXbA3FM=

Decrypted value: 123113121321313564648

Here a random input string is given as shown above. With a secret key as 'const'. The encrypted value is 16 byte each symbol is 8 bit here. The first information was appropriately recovered by means of unscrambling of the ciphertext. The execution of AES is turned out to be precisely scrambling and ecrypting the information messages with significantly higher security and insusceptibility against the unapproved clients. In Result both encryption and decryption is done.

6.2. TIME STAMPS

- Upload data is monitored from the moment we get the upload request from user and tracked parameters as follows:

Field	Type	Null	Key	Default	Extra
id	bigint(20)	NO	PRI	NULL	auto_increment
file_name	varchar(255)	YES		NULL	
time	datetime	YES		NULL	
users_id	bigint(20)	YES	MUL	NULL	
pass_key	varchar(255)	YES		NULL	

Table 6: Time Stamps for Uploading Request

- The timestamp here lets us exactly know when the user successfully uploaded a file, also which user and which file as shown below.

10	2016-08-04-09-27-55-840_1470283075840_XXXPG5165X_ITRV.pdf	2017-04-25 06:34:38	1	34221
11	pan card_1.pdf	2017-04-25 07:30:12	1	34251
12	ResumeAravpdf2.pdf	2017-04-25 10:02:02	1	45451
13	main module.docx	2017-04-25 10:11:41	1	80091
14	pic.jpg	2017-04-25 10:13:30	1	01191
15	pic.jpg	2017-04-25 10:33:28	1	91191

Table 7: Timestamp showing date and time

- The same stands true for download request having following data.

id	pass_key	status	time	message_template_id	users_id
1	0	success	2017-04-19 08:38:12	1	1
2	0	success	2017-04-19 08:51:19	1	1
3	0	success	2017-04-19 08:55:46	1	1
4	0	success	2017-04-19 09:14:56	1	1
5	0	success	2017-04-19 09:31:47	1	1
6	77188	success	2017-04-19 09:38:37	1	1
7	82660	success	2017-04-19 09:52:52	1	1
8	29664	success	2017-04-19 09:59:16	1	1
9	58852	success	2017-04-19 10:15:08	1	1
10	96494	success	2017-04-25 06:36:02	1	1
11	73743	success	2017-04-25 06:41:47	1	1
12	47017	success	2017-04-25 06:44:23	1	1
13	15158	success	2017-04-25 07:12:55	1	1
14	88108	success	2017-04-25 07:16:15	1	1
15	71906	success	2017-04-25 07:21:06	1	1
16	15043	success	2017-04-25 07:21:53	1	1
17	34399	success	2017-04-25 07:23:34	1	1
18	83366	success	2017-04-25 07:23:34	1	1
19	18148	success	2017-04-25 07:30:15	1	1
20	47191	success	2017-04-25 08:10:18	1	1
21	48248	success	2017-04-25 08:14:08	1	1
22	33539	success	2017-04-25 08:23:57	1	1
23	35251	success	2017-04-25 08:31:35	1	1
24	56573	success	2017-04-25 09:45:37	1	1
25	28045	success	2017-04-25 09:47:29	1	1
26	6038	success	2017-04-25 10:02:15	1	1
27	4354	success	2017-04-25 10:34:11	1	1

Table 8: Time Stamp for Downloading Request

6.3 UPLOAD FILE WEBSITE PROCESS:

- Login with permitted credentials:

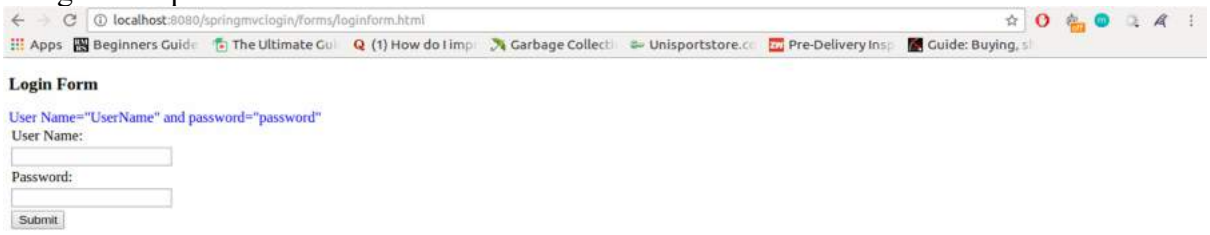

Figure 11: Upload File Website

- Once logged in go to upload doc link and upload any type of file.

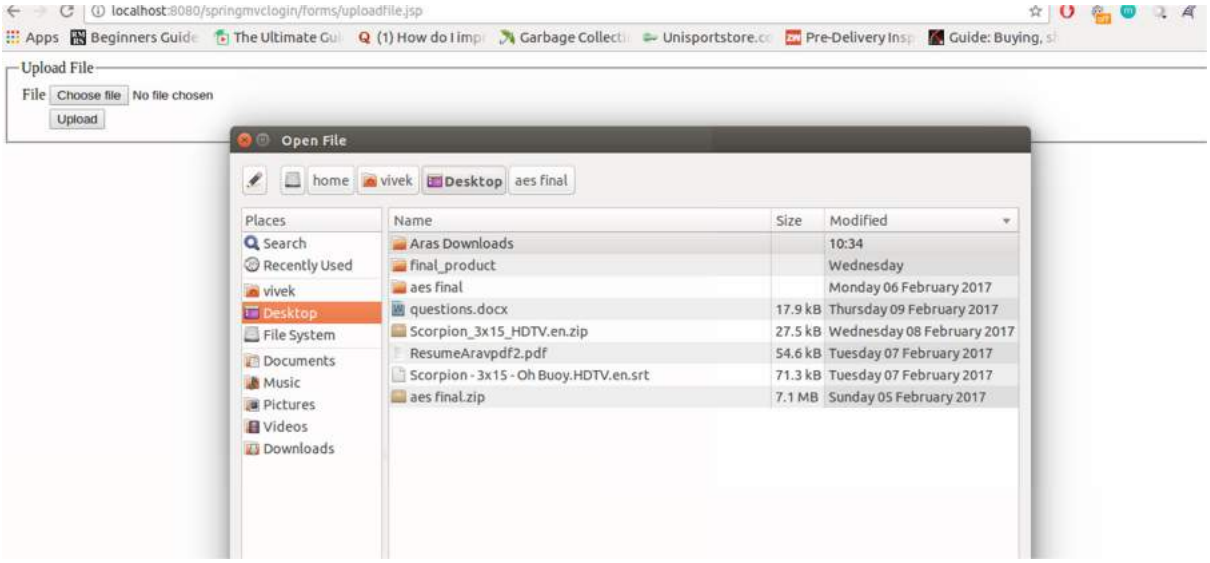

Figure 12: Path to upload file

- Once uploaded the file will be listed in the dash board page as shown below;

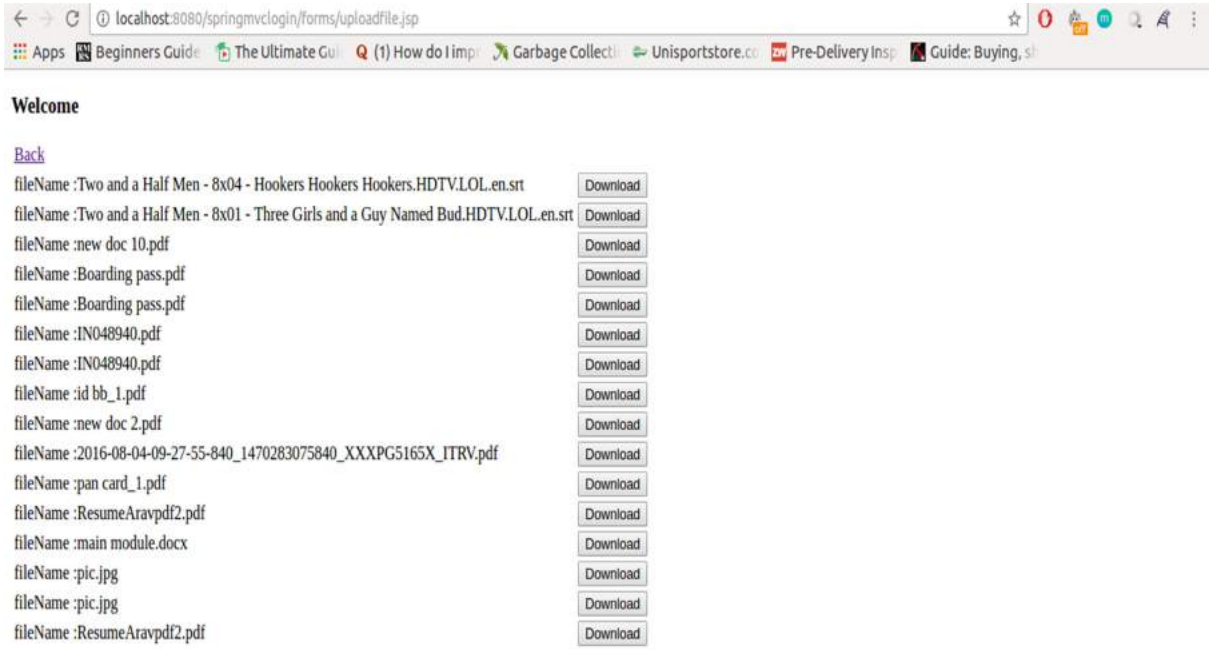

Figure 13: List of uploaded file

- As part of upload we only store encrypted hexadecimal version of the file in our servers as attached in the part of the mail, below is part of content the file contains.

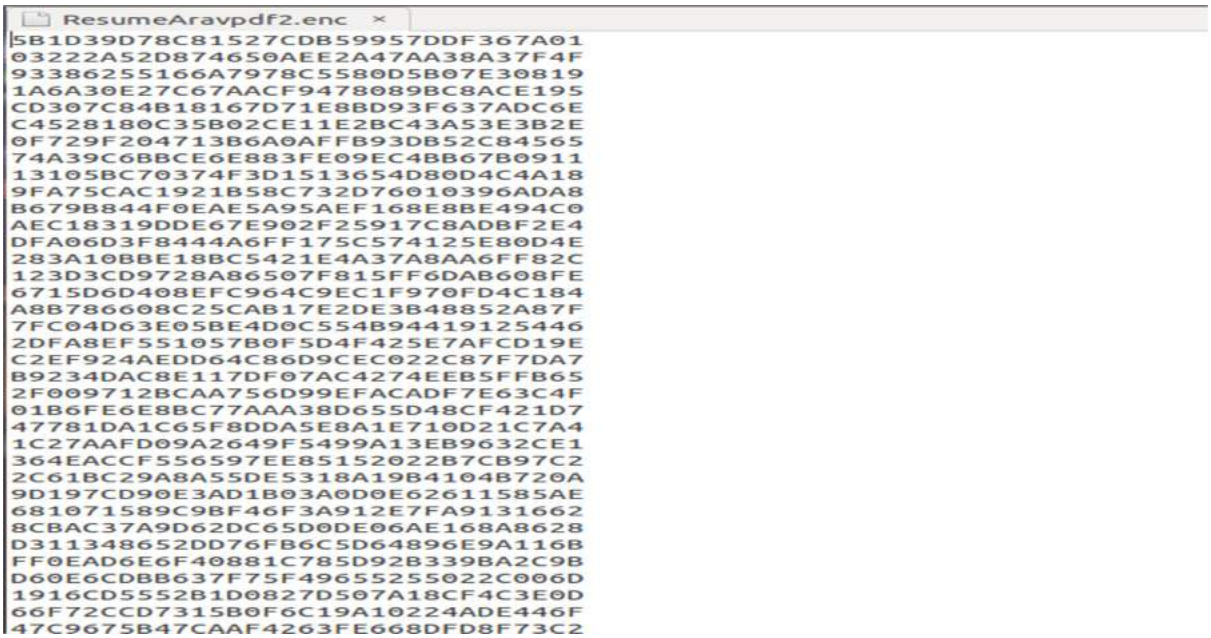

Figure 14: Encrypted file in Hexadecimal format

6.4 DOWNLOADING A FILE:

- First Step is to login on the site and go to the dashboard page where all the files for that particular file will be listed.
- Click on Download button, which in turn will show a text where a 5 digit OTP is asked for (which would have been already sent to the user on his/her registered mobile. Once the user prompt that field with correct value and clicks on download again the required file will downloaded on his/her browser, the mentioned steps is shown in below snapshots.

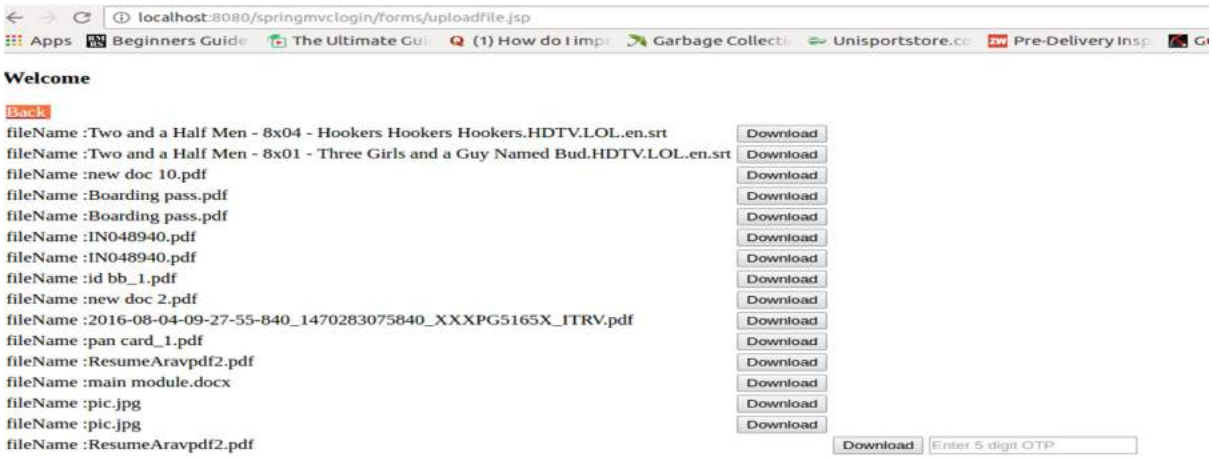

Figure 15: Website showing - 5 digit OTP number

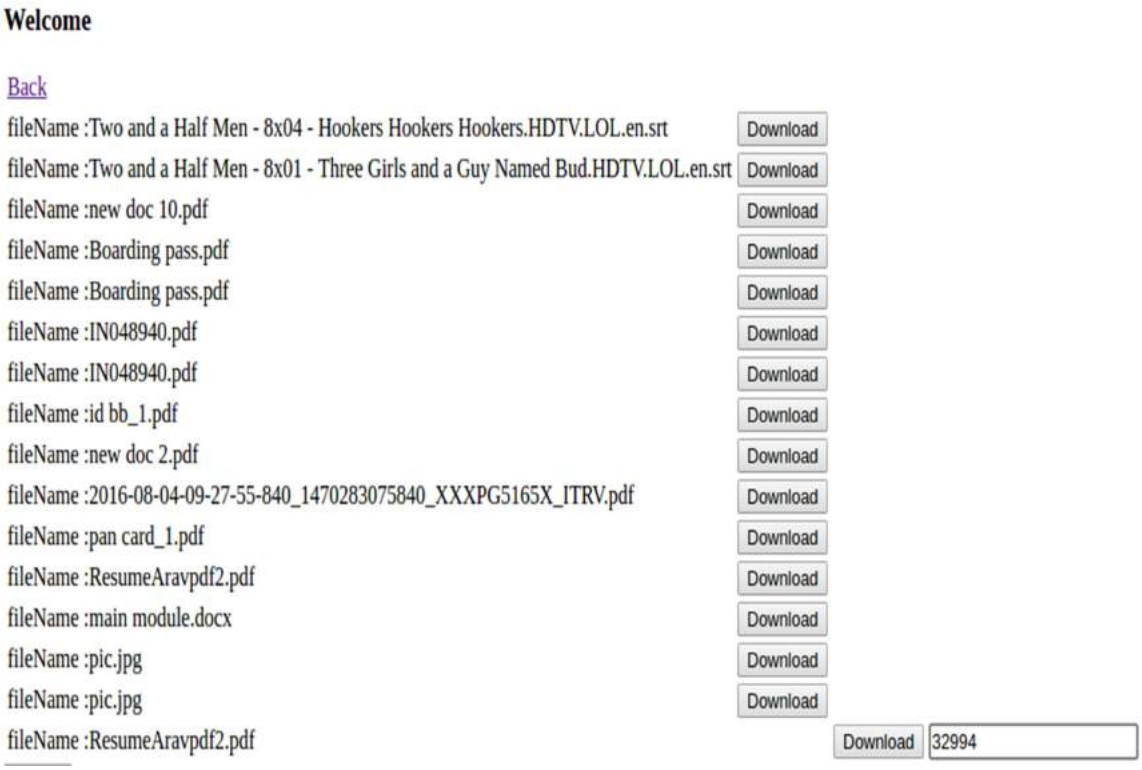

Figure 16: Website showing user prompted the OTP number

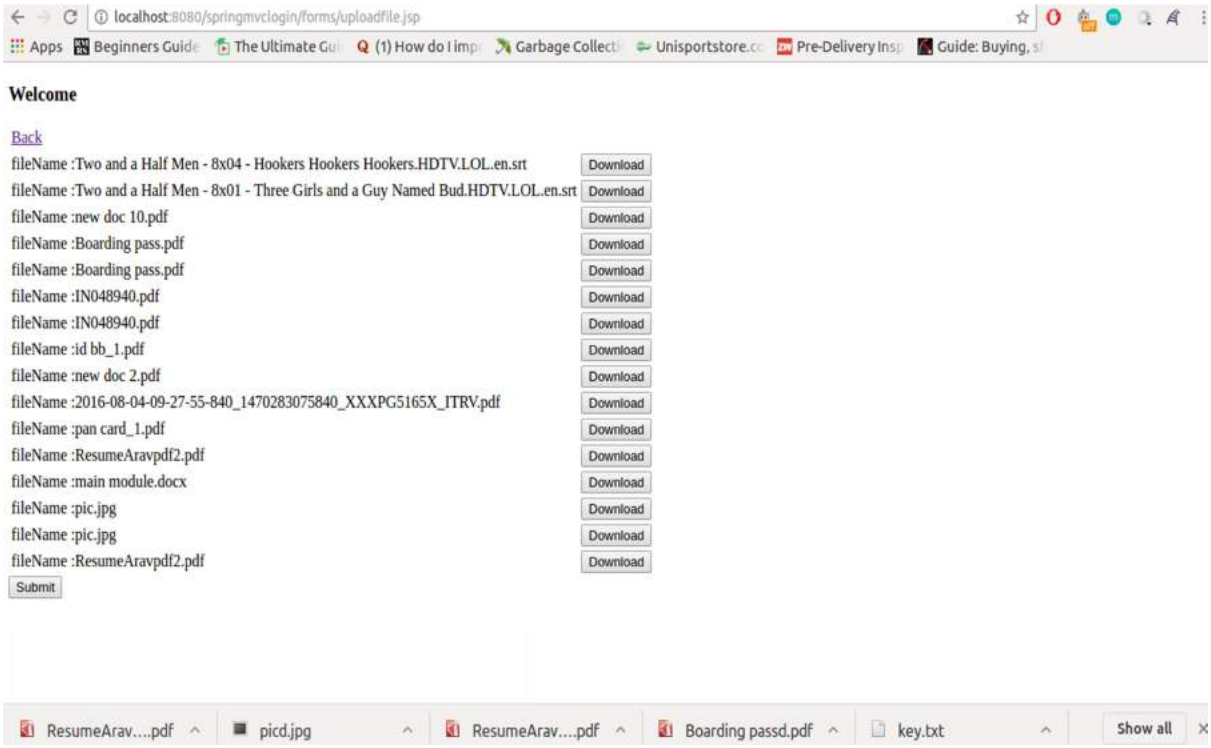

Figure 17: Download option

6.5 ENCRYPTION SECRET KEY

Encryption key is unique for each combination of file and user is generated when user uploads a file the same key is used to encryption at the time of upload and decryption at the time download, following is a snapshot of data model for the same, where encryption key is represented by passkey column.

```
mysql> select * from file;
+----+-----------------------------------------------------------------------+---------------------+----------+----------+
| id | file_name                                                             | time                | users_id | pass_key |
+----+-----------------------------------------------------------------------+---------------------+----------+----------+
|  1 | Two and a Half Men - 8x04 - Hookers  Hookers  Hookers.HDTV.LOL.en.srt  | 2017-04-19 06:51:08 |        1 | NULL     |
|  2 | Two and a Half Men - 8x01 - Three Girls and a Guy Named Bud.HDTV.LOL.en.srt | 2017-04-19 06:52:27 |        1 | NULL     |
|  3 | new doc 10.pdf                                                        | 2017-04-19 08:31:09 |        1 | NULL     |
|  4 | Boarding pass.pdf                                                     | 2017-04-19 08:46:05 |        1 | NULL     |
|  5 | Boarding pass.pdf                                                     | 2017-04-19 09:12:35 |        1 | NULL     |
|  6 | IN048940.pdf                                                          | 2017-04-19 09:31:25 |        1 | NULL     |
|  7 | IN048940.pdf                                                          | 2017-04-19 09:37:52 |        1 | NULL     |
|  8 | id bb_1.pdf                                                           | 2017-04-19 09:51:52 |        1 | NULL     |
|  9 | new doc 2.pdf                                                         | 2017-04-19 10:14:55 |        1 | NULL     |
| 10 | 2016-08-04-09-27-55-840_1470283075840_XXXPG5165X_ITRV.pdf             | 2017-04-25 06:34:38 |        1 | 34221    |
| 11 | pan card_1.pdf                                                        | 2017-04-25 07:30:12 |        1 | 34251    |
| 12 | ResumeAravpdf2.pdf                                                    | 2017-04-25 10:02:02 |        1 | 45451    |
| 13 | main module.docx                                                      | 2017-04-25 10:11:41 |        1 | 80091    |
| 14 | pic.jpg                                                               | 2017-04-25 10:13:30 |        1 | 01191    |
| 15 | pic.jpg                                                               | 2017-04-25 10:33:28 |        1 | 91191    |
| 16 | ResumeAravpdf2.pdf                                                    | 2017-04-25 11:02:35 |        1 | 93329    |
+----+-----------------------------------------------------------------------+---------------------+----------+----------+
16 rows in set (0.06 sec)
```

Table 9: Table showing Different passkey for different file

Chapter 7: Conclusion and Future Scope

7.1: CONCLUSION

- In this thesis, it has been shown that AES algorithm is the best security algorithm as compared to the ZUC and SNOW 3G algorithm which are used in the LTE Technology. Even AES encryption algorithm is available in smart phones for security purposes.
- This thesis provides three main applications such as timestamp, encryption and OTP number.
- Any authorized user can download and upload from any workstation (PCs, Mobile phones) but the user requires internet connection.
- Whole database is secure because the file is in encrypted and it is in hexadecimal format.
- Timestamp is also introduced in this research because we can account which user have logged on to the site, at what time did the user uploaded and downloaded the file.
- This thesis also makes sure that the user is authenticated by using OTP number. It is generated whenever the user request for the download and upload option.
- This thesis also helps in reduction in the size of the file is so many file can be kept inside the database.

7.2: FUTURE SCOPE

- The work can be expanded by modifying AES algorithm or using all the security algorithm and make a new algorithm which will be resistance to known threats as well as the future threats.
- Hash technique can be introduced into this research because it will prevent from any forged document.
- We can provide a user friendly pattern for the user by seeing and tracking there downloads and upload file or in other words suggestion can be given to the user which document is more suited for the user by their activity.
- Tracking also be introduced in which we can see from which network address more downloading and uploading process happened.
- We can also account from which mobile operator have used more often in the site.

REFERNCES

[1] Prerana Choudhari, Vikas kaul and S K Narayankhedkar, “Security Enhancement Algorithm for Data Transmission in 4G Networks’’, *Computing Communication Control and Automation (ICCUBEA)*,Vol. 3,Issue 12, December 2014.

[2] Ghizlane Orhanu, Said El Hajji and Youssef Bentaleb,”SNOW 3G stream cipher operation and complexity study”, *Contemporary Engineering Sciences*, Vol. 5, Issue 3, March 2010.

[3] Aleisa, Noura. "A Comparison of the 3DES and AES Encryption Standards." *International Journal of Security and Its Applications* 9.7, Vol. 30, Issue 1, pp. 241-246, Jan 2015.

[4] Macaulay, Tyson. "The 7 Deadly Threats to 4G." *VP Global Telco Strategy, McAfee* (2013).

[5] Ekene, Okoye Emmanuel, Ron Ruhl, and Pavol Zavarsky. "Enhanced User Security and Privacy Protection in 4G LTE Network." *Computer Software and Applications Conference (COMPSAC), 2016 IEEE 40th Annual*. Vol. 2. IEEE, 2016.

[6] Aiash, Mahdi, et al. "Providing security in 4G systems: Unveiling the challenges." *Telecommunications (AICT), 2010 Sixth Advanced International Conference on*. IEEE, 2010.

[7] Kaul, Vikas, Bhushan Nemade, and Vinayak Bharadi. "Next Generation Encryption Using Security Enhancement Algorithms for End to End Data Transmission in 3G/4G Networks." *Procedia Computer Science* 79, pp. 1051-1059, 2016.

[8] Ghanim, Alyaa, and Imad Fakhri Taha Alshaikhli. "Comparative study on 4G/LTE cryptographic algorithms based on different factors." *International Journal of Computer Science and Telecommunications,* 2014.

[9] Krishnamoorthy, Vidya, and Senthilkumar Mathi. "Security enhancement of handover key management based on media access control address in 4G LTE networks." *Computational Intelligence and Computing Research (ICCIC),* Vol. 40, Issue 7,Aug 2015.

[10] Tu, Guan-Hua, et al. "How voice call technology poses security threats in 4G LTE networks." *Communications and Network Security (CNS), 2015 IEEE Conference on*. IEEE, 2015.

[11] Orhanou, Ghizlane, and Said El-Hajji. "The new LTE cryptographic algorithms eea3 and eia3." *Appl. Math* 7.6, pp. 2385-2390,2015.

[12] Choudhari, Prerana, Vikas Kaul, and S. K. Narayankhedkar. "Security Enhancement Algorithms for Data Transmission in 4G Networks", *International Journal of Engineering and Innovative Technology,* 2014.

[13] Bikos, Anastasios N., and Nicolas Sklavos. "LTE/SAE security issues on 4G wireless networks." *IEEE Security & Privacy* 11.2, pp. 55-62, 2013.

[14] Tu, Guan-Hua, et al. "How voice call technology poses security threats in 4G LTE networks." *Communications and Network Security (CNS),* 2015.

[15] Krishnamoorthy, Vidya, and Senthilkumar Mathi. "Security enhancement of handover key management based on media access control address in 4G LTE networks." *Computational Intelligence and Computing Research (ICCIC)*, 2015.

[16] Orhanou, Ghizlane, Said El Hajji, and Youssef Bentaleb. "SNOW 3G stream cipher operation and complexity study." *Contemporary Engineering Sciences-Hikari Ltd* 3.3, pp. 97-111, 2010.

[17] Ekene, Okoye Emmanuel, Ron Ruhl, and Pavol Zavarsky. "Enhanced User Security and Privacy Protection in 4G LTE Network." *Computer Software and Applications Conference (COMPSAC)*, Vol. 2, 2016.

[18] Rajani Muraleedharan and Lisa Ann Osadciw," Increasing QoS and Security in 4G Networks Using Cognitive Intelligence", *IEEE journel*, November 26 2007.

[19] Nugroho, Eddy Prasetyo, Rizky Rachman Judhie Putra, and Iman Muhamad Ramadhan. "SMS authentication code generated by Advance Encryption Standard (AES) 256 bits modification algorithm and One time Password (OTP) to activate new applicant account." *Science in Information Technology (ICSITech),* 2016.

[20] Pammu, Ali Akbar, Kwen-Siong Chong, and Bah-Hwee Gwee. "Highly secured arithmetic hiding based S-Box on AES-128 implementation." *Integrated Circuits (ISIC), 2016 International Symposium on*. IEEE, 2016.

[21] Sadikin, Mohamad Ali, and Rini Wisnu Wardhani. "Implementation of RSA 2048-bit and AES 256-bit with Digital Signature for Secure Electronic Health Record Application." *CommIT (Communication and Information Technology) Journal* 10.2 , pp.63-69,2016.

[22] Soni, Shraddha, Himani Agrawal, and M. Sharma. "Analysis and comparison between AES and DES Cryptographic Algorithm." *International Journal of Engineering and Innovative Technology* 2.6 ,pp. 362-365, 2012.

[23] Shady Mohamed Soliman, Baher Magdy and Mohamed A. Abd El Ghany," Efficient implementation of the AES Algorithm for Security Application", *29th IEEE international Conference on system-on-Chip*, 9 Sept. 2016.

[24] Ariffi, Suriyani, et al. "SMS Encryption Using 3D-AES Block Cipher on Android Message Application." *Advanced Computer Science Applications and Technologies (ACSAT),* 2013.

[25] Katkade, Pradnya, and G. M. Phade. "Application of AES algorithm for data security in serial communication." *Inventive Computation Technologies (ICICT), International Conference on*. Vol. 3. IEEE, 2016.

[26] Challita, Nicole, and Bassem Bakhache. "Enhancement of S-AES using chaos for the support of biomedical applications." *Advances in Biomedical Engineering (ICABME),*2013.

[27] Wang, Qiu-xia, Tie Xu, and Pei-zhou Wu. "Application research of the AES encryption algorithm on the engine anti-theft system." *Vehicular Electronics and Safety (ICVES),* 2011.

LIST OF PUBLICATION

[1] Harikrishnan, L, and Komal Arora, "Implementation of Advance Encryption Standard (AES) to Securely Store and Maintain Research Data", *International Journal of Engineering Technology, Management and Applied Sciences,* Vol. 5, Issue 4, pp. 2349-4476, April 2017.

ORIGINALITY REPORT

%17	%13	%8	%5
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.webtorials.com Internet Source	%4
2	ijarcsse.com Internet Source	%3
3	www.ijcst.org Internet Source	%1
4	Okoye Emmanuel Ekene, Ron Ruhl, Pavol Zavarsky. "Enhanced User Security and Privacy Protection in 4G LTE Network", 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), 2016 Publication	%1
5	Submitted to Kaplan University Student Paper	%1