Data Security in Wireless Communication using Multiple Keys

A Dissertation Submitted in Partial Fulfillment of the Requirement for the Award of the Degree of

MASTER OF ENGINEERING

in

Wireless Communication

Submitted by

Lovpreet Kaur

Roll No: 801563012

Under the Guidance of

Dr. Ajay Kakkar

Assistant Professor, ECED

Thapar University, Patiala

Electronics and Communication Engineering Department

Thapar University

(Established under the section 3 of UGC Act, 1956) Patiala – 147004 (Punjab)

July, 2017

DECLARATION

I hereby declare that the work which is being entitled **"Data Security in Wireless Communication using Multiple Keys"** in fulfilment of the requirements for the Masters of Engineering in Wireless Communication submitted at Electronics and Communication Engineering Department of Thapar University Patiala, is an authentic record of my own work carried out under the guidance of **Dr. Ajay Kakkar** (Assistant Professor), Electronics and Communication Engineering Department and refers others research's work which are duly listed in reference section.

The matter presented in this dissertation has not been submitted in any other University/ Institute for the award of degree.

Date: 14/7/17

Lovpreet Kaur

Roll No: 801563012

It is certified that the above statement made by the candidate is correct to the best of my knowledge and belief.

Date: 14/7/17

Dr. Ajay Kakkar

Assistant Professor, ECED

ACKNOWLEDGEMENT

First of all, I would like to express my gratitude to **Dr. Ajay Kakkar,** Assistant Professor, Electronics and Communication Engineering Department, Thapar University Patiala for his patient guidance and support throughout this report. I am truly very fortunate to have the opportunity to work with him. I found this guidance to be extremely valuable. I am also thankful to our Head of Department, **Dr. Alpana Agarwal** and P.G. Coordinator, **Dr. Hem Dutt Joshi.** I would like to thank the entire faculty and staff of Electronics and Communication Engineering Department and then friends who devoted their valuable time and help me in all possible ways towards successful completion of this work. I thank all those who have contributed directly or indirectly to this work.

Lastly, I would like to thanks my parents for their years of unyielding love and encourage they have always wanted the best for me and I admire their determination and sacrifice.

Lovpreet Kaur
ME (WC)
801563012

ABSTRACT

Encryption is the process to hide the data from plain text to cipher text. The encryption schemes are used to convert the plain text into cipher text. Encryption schemes are also used to transport the keys securely from transmitter to receiver. In this process, overheads are increased; therefore, the generation of keys has been done at the receiver side by the user. The processing of multiple keys from a pool having same data is not an easy task and may generate unreliable keys. The scheme is effective, if the bulk data is present in the pool for the encryption because the generation of multiple keys from the same data is not the effective solution in terms of security point of view. If multiple keys are selected from a small pool, there is always a chance of selection of duplicate key which ruins the encryption process. Comparison of different encryption algorithms has also been done on the basis of data length, key length, type of algorithms and number of iteration. In this work, we modify the key generation process for encryption algorithm and evaluate the processing time in encryption process based upon single and multiple keys. Single password is not efficient for security point of view; therefore, multiple keys have been used. Keys have been generated from the available data. Simulation results shows that the single of 8, 16, 32 and 64 bit key length has less processing time in comparison to multiple keys for 8, 16, 32 and 64 bit key length.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AN	Artificial Noise
AES	Advanced Encryption Standard
USK	Unshared Secret Key
OSN	Online Social Networks
PEC	Packet Erasure Channels
TDES	Triple Data Encryption Standard
PT	Plain Text
CT	Cipher Text
PCS	Public CloudServers
RSA	Rivest Shamir Adlema
MN	Multimode network
PGP	Pretty Good privacy
CPA	Chosen Plaintext Attacks
WSN	Wireless Sensor Network
IEEE	Institute of Electrical and Electronics Engineers
PKC	Public Key Cryptography
LAN	Local Area Network
EW	Electronic Warfare
IW	Information Warfare
DES	Data Encryption Standard-
CDMA	Code Division Multiple Access
GSM	Global System for Mobile Communication
TDMA	Time Division Multiple Access
WAP	Wireless Access protocol
OS	Operating System
HTML	Hyper Text Mark-up Language
WEP	Wireless Equipment Privacy
WPA	Wi-Fi Protected Access
MN	Multi Node
VC	Visual Cryptography
EVCS	Extended Visual Cryptography system
UWSN	Unattended Wireless Sensor Network

ECCE	Enhanced Cooperative Channel Establishment for Secure pair-wise
P2P	Point to point communication
SMT	Safe Message Transmission
RIP	Routing Information Protocol
EIGRP	Enhanced Interior Gateway Routing Protocols
OSPF	Open Shortest Path Fast
MIO	Multiple Inter image Obfuscation
IOLTS	Standard Input Output Label Transition System
D2D	Device-to-Device Communication
MIMO	Multi Input Multi Output

CHAPTER 1

INTRODUCTION

Remote messages travel through the free-space condition on certain range allotments, which are rare, vigorously controlled, and frequently unattainable assets. Remote gadgets, for example, PDAs, individual advanced partners (PDAs), and pagers are inalienably less secure than their wired partners. This is expected to some extent to their constrained data transmission, memory and preparing capacities [1]. Another reason is that they send their information into the air where anybody with the innovation can capture it. Privacy always has been a concern for modern society. In recent years our sensitivity to privacy has grown even as we have embraced technology capable of infringing on some of the privacy. Nowadays, security is the major concern in many areas. Everyone wants to send their data securely. Wireless communication is very much popular and commonly used like schools, industrial area, banks, home and other areas. In the wireless environment data can be hacked easily and it is not a very much secure way of communication [2].

The Internet and wireless are so closely related that whatever affects the Internet in one way or another affects the wireless environment. As wireless and Internet environments become truly interoperable, the threats and vulnerabilities affecting the Internet will face wireless networks in equal measure [1].

Regulatory Environment and issues: Next 20 years, the regulations and policies will development of the wireless security. Some areas where these regulations will include areas follow: (i) Difference between different networks (public and private), (ii) Difference between national and international rules for data protection, (iii) Security level in wireless communication and (iv) Security is the crucial issue facing by wireless industry. Security is not only about protection of data but also protection from monitoring [1].

Security-Related Regulations: In the wireless communication has no wired connection. So, they have better chance to survive under the condition of natural disasters. Digital encryption techniques can be used to protect the wireless transmissions, but public concerns about privacy will need to be addressed. The use of fiber and wireless technology are among the best available alternatives for ensuring high levels of system availability [2].

Guidelines for Security Measures: Security is the significant factor to understand for achieving its vast potential. Security is the combination of processes, procedures and systems

used to ensure the confidentiality, integrity, or availability of information. **Confidentiality** is the protection of information from unauthorized users. **Integrity** protects the data content from unauthorized modification. **Availability** is the process of ensuring that a system or data will be accessible when needed [3].

Within this model, some of the current security challenges for wireless devices that require security measures include lost and stolen devices, insider attacks, man-in-the-middle attacks, and device cloning. Additional security concerns include viruses, denial of service attacks, enhanced radio interception devices, and protection of wireless LANs. In general terms, a secure mobile solution is one with the following functionality: (i) Authentication validating: the identity of the user. (ii) Encryption shutting out: eavesdroppers on a data conversation. (iii) Access Control Ensuring that only authorized user can access the system. (iv) Theft and employee termination: disabling the devices when unauthorized user using the device. Mobile commerce customers must develop a good degree of trust that their communications and data are being adequately protected before they will embrace the technology. The significance of programming security is obvious since the disclosure that most assaults to genuine programming frameworks are started by inadequately composed and created programming [1].

Information Warfare (IW): It is a model that defines the security of wireless communication system. Martin Libicki (2) proposed seven categories of IW, two of which are Electronic Warfare (EW) and hacker warfare. The term Information Warfare (IW) is fundamentally a United States Military idea including the utilization and administration of information and correspondence innovation in quest for an upper hand over a rival. Electronic warfare (EW) is any activity including the utilization of the electromagnetic spectrum or directed energy to control the spectrum, attack of an enemy, or impede enemy assaults via the spectrum. The motivation behind electronic warfare is to deny the adversary the benefit of, and guarantee neighborly unimpeded access to, the EM spectrum. EW can be connected from air; sea, land, and space by kept an eye on manned and unmanned systems, and can target humans, communications, radar, or different resources [2].

It is useful in thinking about risk management to pose a tentative relationship. Risk is described as a notional relationship. Consider the following statement:

$$Level\ of\ Risk = \frac{(Threat \times Vulnerability)}{Countermeasures} \times Impact$$

Managers must consider the possible consequences of attacks from a wide variety of threats. Each attack may act on a tangential vulnerability. Vulnerabilities are characteristics of our situations, systems, or facilities that can be exploited by a threat to do us harm. A vulnerability for which there is no credible threat does not require a response by security processes. Countermeasures may abate the danger even if there are malevolent and capable threats, as well as vulnerabilities, which can be exploited by those threats. The impact of a successful attack depends upon the value of the target. If the impact of a security failure is small, allocation of scarce and expensive resources to security systems and processes can also be small [2].

1.1 CRYPTOGRAPHY ATTACKS

Cryptography has some attacks and threats. Hacker attempts the random attack on the system and data that is further classified in some categories system attacks which have the four categories and the data has also four categories. System attacks have four attacks as shown in figure 1.1 (i) interruption, (ii) intersection, (iii) fabrication, (iv) modification. And the data attacks have also four types of attacks (i) Certificate authentication (CA), (ii) known plaintext attack (KPA), (iii) chosen plaintext attack (CPA), (iv) chosen ciphertext attack (CCA) [1].

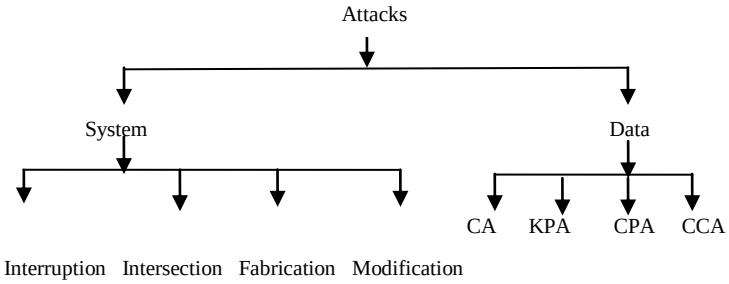


Figure 1.1 cryptography attacks

Send and receive data successfully over a secured channel to avoid unauthorized access known as the secured access. Secured channels are not practically possible; therefore, the suitable techniques are involved to protect the data from hackers. The data security also becomes prominent especially in wireless communication. In many areas we want to send our data securely, like online transactions, emails, booking of tickets etc. There are many ways to secure our data like passwords, multiple passwords and cryptography. Passwords of small length are easy to hack by hacker because passwords are the combination of alphabets, numbers and special characters. But single passwords still not very powerful from security point of view. Multiple passwords are more secure method then the single passwords but can be hack by hacker with small effort. So, we are using the best method for security that is cryptography. It is the process to hide the data with encryption and retrieve the original data

with the decryption process, showing in figure1.2. Encryption can be done by two types of keys called symmetric and asymmetric (or public and private key). If the both side's encryption and decryption using the same key, this is called the public key that is known to both sides, otherwise it is private key. Sometimes, combination of both public and private key can also be used in wireless communication [3].

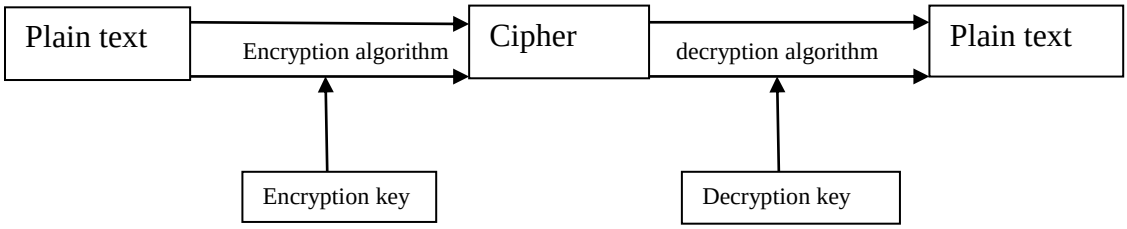


Figure 1.2 Cryptography process

In symmetric encryption, every PC has a mystery key that it can use to encode a bundle of data before it is sent over the system to another PC. It is basically the same as a mystery code that each of the two PCs must know keeping in mind the end goal to interpret the data. The code gives the way to interpreting the message [3].

Asymmetric Encryption: Two keys are utilized as a part of asymmetric cipher open and a private one. People in general one is accessible for everybody, except the private one is known just by the proprietor. When the message is encoded with the general population key, the relating private key used to decode it. The private key could not be gained from the general population one [5].

Multiple encryption: Multiple encryption is the process of encrypting an already encrypted data to multiple times, either using the same or a different algorithm. It is also known as cascade encryption. Super encryption refers to the outer-level encryption of a multiple encryption [2].

Online and offline attack or encryption: Online and offline have specific meanings in computer technology and telecommunications world. In which online indicates a state of connectivity, while offline indicates a disconnected state. If a person taking part in conversation, discussion or business meeting that is called the online. Those who are not participated in these places called the offline. Online is an activity that is connected to

computer or that is connected to internet. In other ways we can say that it is an activity or service that is performed by using internet [1].

1.2 WIRELESS SECURITY PROTOCOLS

Wireless Application Protocol: It is a safe particular which enables clients to get to data in a flash through handheld remote gadgets, cell phones, pagers, two-way radios, advanced mobile phones and communicators. These incorporate CDMA, GSM, PDC, PHS, and TDMA. Ones particularly designed for handheld gadgets incorporate Palm OS, Windows CE, FLEXOS, OS/9, and Java OS. WAPs that utilization shows and get to the Internet run what are called smaller scale programs. Programs with little record sizes that can suit the low memory limitations of handheld gadgets and the low-data transmission imperatives of a remote handheld system [1].

Despite the fact that WAP bolsters HTML and XML, the WML dialect (a XML application) is particularly conceived for little screens and one-hand route without a console. WML is adaptable from two-line content shows up through realistic screens found on things, for example, advanced mobile phones and communicators. WAP additionally bolsters WML Script. It is like JavaScript, yet makes negligible requests on memory and CPU control since it doesn't contain a considerable lot of the superfluous capacities found in other scripting dialects. Since, WAP is genuinely new, it is not a formal standard yet. It is as yet an activity that was begun by Unwired Planet, Motorola, Nokia, and Ericsson [2].

In the wireless world, we need more security for that, therefore, these following access techniques are required and descriptions of the WEP, WPA, and WPA2 wireless security protocols are detailed as follows:

- **Wired Equivalent Privacy (WEP):** The original encryption protocol developed for wireless networks. As its name implies, WEP was designed to provide the same level of security as wired networks. However, WEP has many well-known security flaws, is difficult to configure, and is easily broken [1].
- **Wi-Fi Protected Access (WPA):** Introduced as an interim security enhancement over WEP while the 802.11i wireless security standard was being developed. Most current WPA implementations use a pre-shared key, commonly referred to as WPA Personal, and the Temporal Key Integrity Protocol for encryption. WPA Enterprise uses an authentication server to generate keys or certificates [4].

- **Wi-Fi Protected Access version 2 (WPA2):** Based on the 802.11i wireless security standard, which was finalized in 2004. The most significant enhancement to WPA2 over WPA is the use of the Advanced Encryption Standard (AES) for encryption. The security provided by AES is sufficient for use by the U.S. government to encrypt information classified as top secret [4].

Entropy: Shannon defined the important concept of entropy to relate information to its carrier message. Let $M = (x1, x2, x3, \dots\dots)$be the set of all possible messages from the system X, which can take on n states, and define the information content of any message mi about the state of X as a function mi. Shannon defined entropy as the primary information relationship measure of each message, H as:

$$\boldsymbol{H = \sum_{i=1,n} pi\ log\ pi}$$

Where: H = Entropy in bits, pi = Probability that the random variable is in state i, n = Number of possible states of the system X [1].

Entropy is a measure of the chaotic value of the message. It is a measure of the disorder or uncertainty about X, the state of the system. Decreases in entropy of received messages may be used to measure information gain and efficiency. Waltz [1] suggests that the goal of sensing, communicating, and processing is to decrease uncertainty and increase information. However, from a cryptographic point of view; the goal is to increase the uncertainty or chaos in applied cryptographic keys. When all messages are equally likely, there is no prior statistical knowledge about which message may be received at any time, and the entropy is at a maximum and each message conveys the maximum potential of revealing the unknown. If the messages are not equally likely, it follows that there is prior knowledge about the state of the system, and the entropy of the system is less than the equally likely case [1].

Comparison of commonly used encryption algorithms has been done by considering data length, key length, type of algorithm and iterations. It is shown in table 1.1.

Parameters	**DES**	**RSA**	**IDEA**	**TDES**	**AES**
Year	1970	1978	1991	1998	2001
Data Length	56	Variable	64	168	128
Key Length	64	Variable	128	112	128, 192, 256 bits

Type of Algorithm	Symmetrical	Private key is used to encrypt the data and decryption is done by public key	Symmetrical	Symmetrical	Symmetrical
Iterations	16	Depends upon data and key length	8	3 times to DES	Key size depends upon round functions

Table 1.1 Comparison of various encryption algorithms

Observations: The complex encryption algorithm takes more time to generate the keys; therefore, more encryption time has been observed.

The strength of cryptographic model relies on the key generation process; for a better security level TDES makes the use of three different keying options in comparison with DES. The method of employing multiple keying is effective from the security point of view but not good in terms of processing time. Overheads are more prominent in TDES due to triple padding [3].

Moreover, the processing the multiple keys from a pool having same data is not an easy task and may generate unreliable keys. The scheme is effective, if the bulk data is present in the pool for the encryption because the generation of multiple keys from the same data is not the effective solution in terms of security point of view. If multiple keys are selected from a small pool, there is always a chance of selection of duplicate key which ruins the encryption process.

The encryption schemes are used to convert the plain text into cipher text. Encryption schemes are also used to transport the keys securely from transmitter to receiver. In this procedure overheads are increased, therefore, the generation of keys was done at the receiver side by the user [2].

1.3 DIFFERENT CATEGORIES OF KEYS

We are defining the different categories of keys which are using to encrypt the data. Different categories are mentioned below:

Reliable keys: The keys which provides the high resistance from the internal as well as the external attacks. External attacks are generated by hacker. Internal attacks occur within the network by a user [4].

Unreliable keys: As we are aware that the key length defines the level of security. Key length can be measure on its combinations (single, multiple and dynamic). It is also a function of time. There are some cases mentions under this category defined below:

- Case 1- if the key length is small and only alphabets are used then the security level is very low.
- Case 2- if key length is same as case 1 but uses the combination of alphanumeric and special characters then the security level is increased (marginally accepted) by the case 1. It is also a function of time. With time it degrades that means the security level falls very rapidly. So, the case 2 is suitable for the short time.
- Case 3- alphanumeric combination is used. If key length is increased, get the more secured system.

Observations: from these cases, we can say that the events are function of time. With time key strength is degrade or falls. It means the encrypted data for system keys becomes unreliable.

Faulty keys: Due to the random attacks generated by hackers in the above sections, two cases might be possible**.** (i) Hacker gets hold of keys (partially or completely). (ii) The keys become unreliable.

Classification of keys: Keys are of two types: single and multiple as shown in figure1.3.

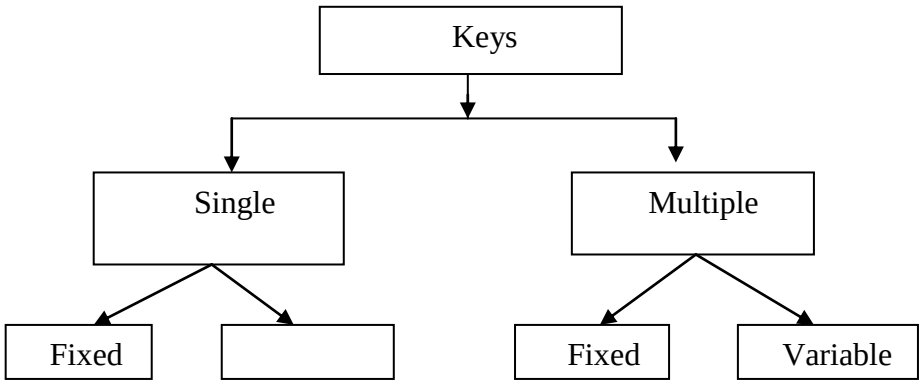


Figure 1.3 Classification of keys

Single and multiple key further classified into two categories: fixed and variable. If the single key is short and fixed length, the security level is very poor. It is a simple and easy method of security. If the single key using variable length then, the security level is moderate. If the multiple keys with fixed length, the security level is very good. If the multiple key is using with variable length, the security level is at its best level. But the complexity is increased and also a time consuming method [3].

Key Management: The generation, storage, distribution, and overall protection of keys are critical to the security of all cryptosystems public or private algorithms. Compromised keys provide the most direct means of unauthorized access. For this reason, physical, information, and perceptual layers of security must protect the key management functions, including those summarized as follows:

• Key security policy a specific security policy must define the controls for the full life cycle of keys (generation. distribution, activation, destruction, or lifetime escrow storage) and controls for usage [1].

• Key-layering hierarchy keys may be defined in layers in which higher level keys are used to encrypt lower level keys for distribution [2].

• Key separation keys may be separated into components for distribution on separate channels or for retention by separate parties (for added security), with provisions for construction of the complete key by the computing function of the individual components [2].

Cryptographic model is selected by keeping an eye on various parameters, which are as follows

- Level of security: It defines on numbers of attacks, processing time and padding.
- Complexity: It includes number of ways to generate the keys. Key generation process must be independent of environmental change with respect of time. For more secured model polynomial trigonometric functions used and all results are not same with respect to time. User's increases, number of keys increases and complexity also increases. Complexity makes overburden over the model [2].
- Overheads (failure): It includes financial overheads, less channel bandwidth, more heat dissipation, power consumption and delay. Overheads are reduced by reducing the number of overhead round function by 25%. More time for generating the data that is the time to hack the data for that time [1].

Processing time: It is the time taken by the processor complete a prescribed procedure. It is measured in nanoseconds.

Hacking time: It is the time available for hacker to generate the random attack. Hacking time measured in minutes. If the processing tie is increased by 10 times and hacking time decrease by some factor, system will be secure system. For a secured model processing time and hacking time should have their minimum value [3].

Round functions and S- boxes: S-box also called the summation box. S box and round function are same. Figure 1.4 shows how the round functions are generated.

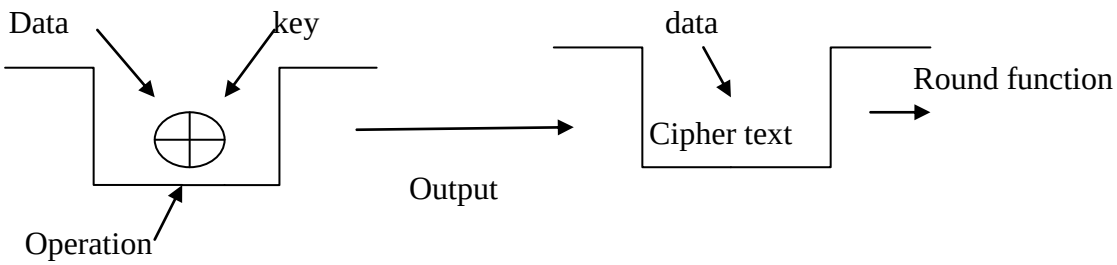


Figure 1.4 round functions

Many block ciphers are defined by specifying a round and then running that specification multiple times. For example, in AES, a round consists of the operations Sub-Bytes, Shift-Rows, Mix-Columns, Add-Round Key. That is one round and, to get AES, you run that multiple times (plus some setup and some post-processing). Thus, a round is defined by each cipher and typically consists of a number of building blocks that are composed together to create a function that is run multiple times.

1.4 ORGANIZATION

Chapter1 briefly discuss the introduction of cryptography, various attacks and encryption algorithms. Chapter 2 includes the literature survey; it involves the work done by the various researchers in the field of cryptography. From the literature survey, few observations have also been drawn and problem formulation has been stated. Chapter 3 includes the proposed work on single and multiple keys. Chapter 4 includes result and discussion. Chapter 5 includes the conclusion and future scope.

CHAPTER 2

LITERATURE SURVEY

This chapter involves the work done by various researchers in the field of cryptography, key generation process and authentication scheme. From the literature survey various observations have been drawn and listed at the end of this chapter. From the observations various objectives have also been derived.

2.1. CRYPTOGRAPHY

Eslami Yadollah *et al.* [6] worked on cryptography circuits for smart cards and the portable electronic devices that provide user authentication and secured data communication. These circuits have small chip area, and they consume low power. They also considered the hardware implementation of 3rd standard cryptography algorithms on universal architecture. This design presents that the smartcard applications supports both private and public key cryptography algorithms. They achieved this by expressing the primitives of three important algorithms for smart cards (DES, AES, and ECC) in terms of simple logical operations that maximize the number of common blocks among them.

Harrison k.Willie *et al.* [7] worked on the ability of channel codes to enhance cryptographic security. Toward that end, they also presented the secrecy metric of degrees of freedom in an attacker's knowledge of the cryptogram, which is similar to equivocation. They also showed how a channel coding system was used to hide the information about the ciphertext, thus increasing the difficulty of attacks. The system setup was the wire tap channel model, in that the transmitted data traverse through independent packet erasure channels with public feedback for authenticated automatic repeat-request. The system provides cryptographic security enhancement, even when eavesdroppers have an advantage over legitimate receivers in signal quality.

Bucci M *et al.* [8] worked on current measuring technique, which provides the substantially enhance power analysis attacks against cryptographic co-processors. They also proposed the technique, which exploits an active circuit to measure the current consumption of a device under attack while supplying, with a stable voltage. The work was based on the transimpedance of amplifier to provide a low impedance current input and an additional DC feedback loop to control the voltage at the input pin, thus supplying the device under attack with a stable voltage.

Khairnar A. G. *et al.* [9] worked on the password security, which was essential for user authentication on small networking system as well large networking system. Till today, many researchers introduced various methods to protect passwords on network. Passwords were prone to various types of attacks like brute force attack, password reuse attack, password stealing attack, and password cracking attack. Different methods were supported for protection of password on a network. They also considered the work done for protection of text passwords and graphical password, also described that how those methods were efficient.

Hu Chih-Ming *et al.* [10] worked on the cheating problem in VC and extended VC. They considered the attack that may deviate from the scheme in any way. They also introduced duping strategies and connected them on assaulting existent VC or augmented VC plans. They have also proposed conning techniques against VCS and EVCS. Further, they analyzed past cheat counteracting plans and found that they were either not sufficiently hearty or still improvable. They also introduced a change on one of these cheat anticipating plans. They finally proposed an effective change of VCS for duping counteractive action. Their change acquires least overhead on difference and pixel extension. It just included two sub pixels for every pixel in the picture and the difference was decreased just marginally.

Ni Ming *et al*. [11] worked on online hazard based security appraisal gives quick online evaluation of a security level related with a current or determined working condition. One noteworthy preferred standpoint of this approach over deterministic online security evaluation was that it gathers possibility probability and seriousness into lists that reflect probabilistic hazard. Utilization of these files in charge room basic leadership prompts expanded comprehension of potential system issues, including overload, falling over-burden, low voltages, and voltage flimsiness, bringing about enhanced security-related basic leadership. Test comes about on expansive scale transmission models recovered from the vitality administration arrangement of a U.S. service organization were portrayed.

Khiabani S. Yahya *et al*. [12] worked on the issue of end to end security improvement by depending on ponder clamor infused in cipher texts. The primary objective was to create a corrupted wiretap divert in the application layer over which Wyner-sort mystery encoding was conjured to convey extra secure data. They ensures a very secured and solid correspondence utilizing wiretap divert coding in application layer over different edges.

Goel Satashu *et al.* [13] worked on wireless medium which make the communication over this medium vulnerable to eavesdropping. They have also additionally considered the issue of mystery correspondence between two hubs; it was successful over a blurring remote medium and the nearness of an aloof meddler was likewise considered. The transmitter guarantees mystery of correspondence using a portion of the accessible energy to deliver 'fake clamour', with the end goal that exclusive the spy's channel was debased. Diagnostic outcomes were exhibited for the numerous radio wire situation; in the administration of huge number of reception apparatuses.

P. Vilela Joao *et al.* [14] worked on information theoretic security; they had considered the transmission of classified messages over remote systems, in which the genuine correspondence accomplices were helped by well disposed jammers. They also described the security level of a bound district in a semi static blurring condition by registering the likelihood of mystery blackout regarding two new measures of physical-layer security. The sticking scope and the sticking effectiveness were also considered. Their investigation for different sticking methodologies of various levels of channel state data gives knowledge into the outline of ideal sticking arrangements was also demonstrated that a solitary jammer was not adequate to amplify both figures of legitimacy all the while. Besides, a solitary jammer requires full channel state data to give security picks up in the region of the authentic beneficiary.

Khisti Ashish *et al.* [15] dealt with the issue of broadcasting private messages to different collectors under a data theoretic secrecy limitation. Two situations were considered: (i) all beneficiaries were to acquire a typical message; and (ii) every beneficiary was to get an autonomous message. Also, two models were viewed as, parallel channels and quick blurring channels. They likewise demonstrate that a straightforward astute transmission system was ideal for the solid and secure transmission of autonomous messages in the point of confinement of substantial number of recipients.

Junbeom Hur *et al.* [16] worked on the most difficult issues in information sharing frameworks was the implementation of get to strategies and the support of approaches updates. Ciphertext strategy characteristic based encryption was turning into a promising cryptographic answer for this issue. They provide a novel CP-ABE conspires for an information sharing framework by misusing the normal for the framework engineering. The

execution and security investigations showed that their proposed plan was productive to safely deal with the information circulated in the information sharing framework.

Pietro Di Roberto *et al.* [17] worked on Unattended WSNs (UWSNs) portrayed by discontinuous sink nearness and operation in threatening settings. They used a top to bottom examination of security issues exceptional to UWSNs and proposed some straightforward and successful countermeasures for a specific class of assaults. The utilization of cryptography in their depicted system was investigated.

Conti Mauro *et al.* [18] worked on the ECCE protocol to build up a safe pair wise correspondence channel between any combine of sensors in a remote sensor arrange (WSN). The primary commitments of the ECCE convention were, to permit the set up of a safe channel between two sensors that don't share any pre-conveyed key. This element was gotten including an arrangement of sensors in the channel foundation convention; to provide probabilistic validation of the principals and the co-operators.

Yeh Lo-Yao *et al*. [19] worked on online social networks (OSNs) e.g., Facebook and MySpace suggested the fact that an ever increasing number of individuals were utilizing OSNs to impart their interests to companions. Since, security and protection issues on OSNs were real concerns, they proposed a security structure for verifying various clients to enhance the proficiency and security of shared (P2P) based OSNs. The hash-based verification convention requires bring down computational cost and reasonable for asset restricted gadgets. The intermediary construct convention was based with respect to awry encryption and can be utilized to trade more data among clients. The authentication based convention ensures non-denial of exchanges by marks. Without a concentrated validation server, the proposed structure could encourage the expansion of an OSN with clumped confirmations.

Lee Uichin *et al.* [20] worked on P2P content circulation convention configuration was intensely affected by the qualities of Bluetooth, which was a principle takeoff from Internet-based substance dissemination. Be that as it may, little was done to comprehend the execution of general Bluetooth operations, extending from companion disclosure to information downloading, in powerful situations with versatility, obstruction, and diverse Bluetooth adaptations/chipsets. They provide broad estimation study and find that Bluetooth-based substance dissemination experiences time/vitality expending asset disclosure and restricted transfer speed, even with the upgraded elements of the most recent Bluetooth rendition.

Tseng Yuh-Min *et al*. [21] proposed verified gathering key protocol convention, which was appropriate for asymmetric remote system. They also proposed convention which was proficient as well as meets solid security prerequisites. They exhibit that the proposed convention was a genuine contributory gathering key protocol one and gives forward mystery and also understood key verification. It was provably secured against detached enemies and impersonator's attacks. A recreation result demonstrates that the convention was appropriate for cell phones with constrained registering capacity.

Fan Chun-I *et al.* [22] worked on three factor authentication scheme joins biometrics with passwords and brilliant cards to give high-security remote verification. Most existing plans depend on keen cards to check biometric attributes. The upside of this approach was that the client's biometric information was not imparted to remote server. The impediment was that the remote server must trust the brilliant card to perform appropriate confirmation which prompts different vulnerabilities. To accomplish genuinely secure, three-calculate confirmation, a technique must keep the client's biometrics mystery while as yet enabling the server to play out its own particular verification. The proposed conspire completely protects the security of the biometric information of each client. The plan does not uncover the biometric information to any other individual, including the remote servers.

Gupta Gunjan *et al*. [23] worked on the hazardous development in the Internet; arrange security had turned into an unavoidable worry for any association whose inward private system was associated with the Internet. Organize security was setup to make preparations for unapproved get to, (i) adjustment, (ii) change of data, and (iii) unapproved disavowal of administration. When any system is associated with the system which was vulnerable to potential interruptions and attacks, security of information should be possible by a method called cryptography. So, one could state that cryptography was a rising innovation, which is vital for system security. They cover the different figure era calculations of cryptography which were useful in system security.

Breveglieri Luca *et al.* [24] proposed a general structure for blunder identification in symmetric operation-focused approach. They have displayed an operation-focused way to deal with the consolidation of blame identification into cryptographic gadget usage using EDCs. They selected an EDC, with the minimum equipment overhead. They examined 11 figures and prescribed an EDC for each and, for four of them (specifically, AES, DES, RC5, and IDEA). They assessed exchange off between the check point recurrence and the blunder

scope. In spite of the fact that their investigation was limited to symmetric square figures, their approach could be stretched out to open key cryptosystems, (for example, RSA) too.

Gui Bo *et al.* [25] worked on fading characteristics and communicate nature of remote channels. They had concentrated on a multi hop connect with numerous transfers at each jump. Three steering procedures were intended to accomplish the full differing qualities pick up given by collaboration among the transfers. They also explored directing systems in a Mhop coordinate with *L* transfers at each jump, with the goal of limiting the end to end blackout.

Papadimitratos Panagiotis *et al.* [26] worked on the vision of roaming figuring with its pervasive for the (MANET). They also proposed the safe message transmission (SMT) convention to shield the information transmission against subjective pernicious conduct of system hubs. SMT is a lightweight convention that could work exclusively in a conclusion to end way. It exploits the repetition of multi way steering and adjusts its operation to stay proficient and viable even in profoundly unfriendly conditions. It was equipped for conveying up to 83% a greater number of information messages than a convention that does not secure the information transmission. In addition, SMT accomplishes up to 65% lower end to end delays and up to 80% lower defer changeability, contrasted and an option single way convention.

Tafaroji M *et al*. [27] worked on a standout amongst the most generally utilized remote air connect interfaces. Encryption calculation over spreading codes was proposed to enhance the security of CDMA. The security created along these lines was basically connected with the multifaceted nature of the utilized encryption calculation. Since, the encryption calculations security was profoundly solid, it is appropriate for any sort of information correspondences. The mix of scrambled and decoded M-succession was utilized as a spreading code to relieve the framework execution, and the benefit of this blend was considered from the obstruction level and the security perspective.

Bellovin M. Steven *et al.* [28] worked on classical cryptographic conventions in view of client picked keys allows an assailant to mount secret word speculating assaults. They also presented a novel mix of unbalanced (open key) and symmetric (mystery key) cryptography that allow two gatherings sharing a typical watchword to trade classified and confirmed data over an uncertain system. These conventions were secured against dynamic assaults, and had

the property that the secret word was ensured against on-line lexicon" assaults. There were various other helpful applications also, including secured open phones. Their principle objective was to ensure clients with powerless passwords.

Nazumudeen N *et al*. [29] worked on the performance of a system depends on steering conventions. RIPv1, RIPv2, EIGRP and OSPF were the dynamic directing conventions were utilized as a part of the functional systems to spread system topology data to the neighboring switches. There were an extensive number of static and dynamic directing conventions accessible yet decision of the correct convention for steering was reliant on numerous parameters basic being system merging time. They had showed that CISCO Packet Tracer was utilized by system organizers to select the most reasonable steering convention for different systems and to plan an ideal directing topology. Among the IGP sorts the best convention is EIGRP in light of the fact that it gives a superior execution than RIP and OSPF. It has a decent effect in the realm of systems administration because of its quick meeting time, enhanced versatility.

Wu Da-Chun *et al.* [30] worked on a novel and simple strategy to implant any type of mystery messages into a cover picture with controlled mutilation was proposed. Any lossy picture compressor might be connected first to a cover picture to create a lossily handled outcome as the reason for implanting information in the cover picture. The stego picture was delivered by implanting information in every pixel of a cover picture. It was done by changing its dim an incentive without excessing the scope of the dim esteem distinction of the comparing pixels of the cover picture and it’s lossily handled one. The amount of bending that was brought about by installing information was never in abundance of that was created by the lossy compressor.

Xiong Tao *et al.* [31] worked on communications security which was a basic and progressively difficult issue in remote systems. This approach requires a static channel condition for the transmitter and collector to create and counterbalance the controllable simulated clamor. They also investigated the attainability of image muddling to protect against the uninvolved listening in attack and fake parcel infusion assault amid the remote correspondences. They also proposed a Multiple Inter image Obfuscation (MIO) conspire, which uses an arrangement of fake uproarious (images key) to muddle the first information images in the physical layer.

Zhou Zhi *et al.* [32] worked on a novel strategy named halftone visual cryptography was proposed to accomplish visual cryptography. The technique uses the void and bunch calculation to encode a mystery parallel picture into halftone shares (pictures) conveying significant visual data. The new technique could be comprehensively utilized as a part of various visual mystery sharing applications which require fantastic visual pictures, watermarking, electronic money, and so on.

Zhao Wentao *et al.* [33] worked on device-to-device (D2D) communication that was esteemed as a promising innovation to enhance the range effectiveness of the cell frameworks. They concentrated on asset sharing plan for the D2D correspondence fundamental cell systems, where various D2D sets could share sub channels with numerous phone clients (CUs). There advancement errand was to boost the entirety rate of D2D sets while fulfilling the rate necessities of all CUs. They also proposed a productive power dissemination calculation for the D2D sets and the CUs. The numerical outcomes approve the viability and effectiveness of their proposed asset sharing plan. The framework range productivity could be improved significantly along these lines.

Wang Huaqun *et al.* [34] worked on an ever increasing number of customers might want to store their information to public cloud servers (PCSs) alongside the fast advancement of distributed computing. New security issues must be illuminated with a specific end goal to help more customer process their information out in the open cloud. At the point, when the customer was limited to get to PCS, they will assign its intermediary to process his information and transfer them. They also proposed the novel security idea of ID-PUIC out in the open cloud. The proposed ID-PUIC convention could be likewise acknowledged private remote information trustworthiness checking, designated remote information respectability checking and open remote information honesty checking in light of the first customer's approval.

Malik Shahzad *et al.* [35] worked on current PC systems creates significant volume of behavioral framework sign consistently. Such systems include numerous PCs with Internet availability, and numerous clients who get to the Web and use Cloud administrations make utilization of various gadgets associated with the system on a specially appointed premise. They built up a hazard appraisal structure which could be utilized by system heads and individuals in charge of overseeing system security hazard. It was to take an abnormal state perspective of the general system and instantly distinguish subnets at hazard to rapidly

recognize the reason for the hazard, making therapeutic move to redress the issue. They exhibited the utilization of the structure utilizing genuine information gathered from a Local Area Network to Internet portal.

Fu Yulong *et al.* [36] worked on Initially develop the standard Input Output Label Transition System (IOLTS) model to a safe and stuck IOLTS (SG IOLTS) demonstrate, which could be incorporate security properties and their related security capacities. They also proposed a general limited gatecrasher display, which made the last reachable diagram of the entire framework contains the pernicious activities from interlopers. A model based security confirmation approach of convention actualizes was displayed. The technique amplifies the exemplary IOLTS by characterizing the non-insignificant security properties as one a player in the Transition System, and models the conceivable system interlopers as the shaky medium to consolidate the different arranged parts. The model could help clients to produce the plausible move successions which contain the collaborations amongst interloper and the convention executions.

Rahbarinia Babak *et al*. [37] worked on Peer Rush, a novel framework for the recognizable proof of undesirable P2P movement. Peer Rush goes past P2P movement location and could be precisely order the recognized P2P activity. They also introduced Peer Rush, a novel framework for the recognizable proof of undesirable P2P activity. Further, they demonstrated that Peer Rush could be precisely order P2P activity and credit it to particular P2P applications, including pernicious applications, for example, P2P botnets.

Chan Haowen *et al*. [38] worked on sensor network security; an essential test is the outline of conventions to bootstrap the foundation of a protected correspondences framework from an accumulation of sensor hubs. Efficient bootstrapping of secure keys was of basic significance for secure sensor organizes applications. Three efficient irregular key pre distribution schemes for tackling the security bootstrapping issue in asset compelled sensor systems were displayed.

Park Min-Ho *et al.* [39] worked on the rise of differing gathering based administrations, various multicast gatherings were probably going to exist together in a solitary system, and clients may subscribe to different gatherings all the while. They also proposed another GKM plot for various multicast gatherings, called the ace key encryption based different gathering key administration (MKE-MGKM) conspire. A MGKM conspire was suggested that could

improve the administration execution of numerous gathering keys paying little heed to the progressive system of the clients or the information streams.

Li Jinguo *et al.* [40] worked on Machine type communication (MTC) which was an imperative versatile correspondence approach in the long haul assessment progressed (LTE-A) systems. To meet the MTC security prerequisites verification handling of MTC gadgets needs to take after the advanced parcel framework validation and key understanding (EPS-AKA). They also proposed a gathering based AKA (GR-AKA) convention with dynamic arrangement refreshing. Its execution was assessed as far as data transmission, calculation, and refreshing utilization.

Willie K. Harrison *et al.* [41] examined the capacity of channel codes to upgrade cryptographic mystery. They introduced the mystery metric of degrees of flexibility in an aggressor's information of the cryptogram, which was like quibble. They indicated that how a specific viable channel coding framework could be utilized to shroud data about the ciphertext, hence expanding the trouble of cryptographic assaults. The framework setup was the wire tap channel demonstrates where transmitted information cross through free bundle eradication channels (PECs) with open input. The framework provides cryptographic security upgrade, when meddlers have favourable position over real recipients in signal quality.

Maurer Ueli *et al.* [42] considered the special case where the legitimate partners already share a mutual string which was partially known to the adversary. The problem of generating a secret key in this case was well studied in the passive-adversary model. Results were based on novel techniques for authentications were secured even against adversaries knowing a substantial amount of the “secret” key. Their results were based on the combination of new message-authentication methods.

Bucci M *et al.* [43] worked on a present measuring strategy, which guarantees to upgrade control investigation attacks against cryptographic co-processors. The strategy misuses a dynamic circuit to quantify the momentary current utilization of a gadget under attack while providing. It depends on a transimpedance intensifier to give low impedance current information and an extra DC criticism circle to control the voltage at the info stick.

Liu Shuiyin *et al.* [44] investigated an option answer for MIMO wiretap channels. Motivated by the artificial noise (AN) strategy, they proposed the unshared secret key (USK)

cryptosystem, where the (AN) was upgraded as a onetime cushion mystery key adjusted inside the invalid space between a transmitter and a real collector. They have abused the part that artificial commotion plays in physical layer security to demonstrate that it could be utilized as an unshared one time cushion mystery key. They also proposed unshared secret key (USK) cryptosystem with an infinite grid input letter set gives Shannon's optimal mystery and ideal mystery by tuning the power designated to the artificial clamor segment.

Markelj Bla z *et al*. [45] the protected utilization of cell phones was an essential for fruitful and straightforward work, both on an individual and business level. The review displayed in the work demonstrates that work wellbeing in the internet relies on upon the client's information of dangers and their fitting reaction to them. Instruction and mindfulness rising among clients must be put at the centre of said arrangements. Clients must be made mindful of strategies for the protected utilization of cell phones, different dangers and potential results of their emergence, and the significance of utilizing security highlights.

Alsmadi Izzat *et al*. [46] provided a broad review on SDN security. They talked about the security dangers to SDN as indicated by their belongings, i.e., Spoofing, Tampering, Repudiation, Information revelation, Denial of Service, and Elevation of Privilege. They portrayed a few pathways of how SDN was developed. They have displayed a review of the current research in SDN security, concentrating on security dangers, and security controls. Note that the scene of SDN security changes with the advances in SDN was innovative work.

Page Daniel *et al*. [47] worked on the expanding pervasiveness of processing gadgets which was proceeding to offer energizing new applications to purchasers, additionally duplicates the quantity of security issues. Since, such gadgets were conveyed into and utilized as a part of threatening conditions and regularly house touchy data. They had also introduced the principal examination concerning the security of blending based cryptography against side channel assault. Despite the fact that the utilization of pairings in the sorts of condition where side-channel attack was most pervasive, the coupling of personality based cryptography with character mindful gadgets appears to be extremely alluring.

Atay Serap *et al*. [48] evaluated the present helplessness, danger and hazard examination strategies from the perspective of the new security necessities of NGNs. They proposed to utilize autonomic and self-versatile frameworks/applications for guaranteeing the security of NGNs. They had introduced the necessities for another and more viable security arrangement

approach of NGNs. Because of the attributes of the present and future security issues of NGNs, they contend that the present institutionalization endeavours may miss the mark regarding giving a thorough arrangement.

Verma S *et al.* [49] proposed an effective symmetric key cryptography calculation for data security. This square encryption calculation was substantially speedier and offers the upgraded security highlights contrasted with other symmetric key calculations. It helps in accomplishing classification and additionally message confirmation. It additionally creates prevalent execution than other regular encryption calculations utilized as a part of terms of time utilization, at whatever point there was an adjustment in parcel measure. It was additionally successful at whatever point there was an adjustment in information sort, for example, picture, sound or video rather than content. It likewise demonstrated that higher key size prompts change in the battery and time utilization.

Halkidis Spyros *et al*. [50] worked on the most attacks to programming frameworks depend on vulnerabilities brought on by inadequately composed and created programming. The objective was to perform investigation of programming frameworks in view of the security designs that they contain. The initial step was to decide to what degree particular security designs shield from known attacks. This data was encouraged to a numerical model in view of the fluffy set hypothesis and fluffy blame trees keeping in mind the end goal to figure the hazard for every class of attacks. An intriguing expansion to this work would be the programmed presentation of missing security designs either at the outline period of a framework was produced or in officially actualized programming frameworks.

O'Melia Sean *et al*. [51] worked on the direction set expansions for a decreased guideline set PC processor were displayed to enhance the product execution of the information encryption standard (DES), the triple DES, the worldwide information encryption calculation (IDEA), and the propelled encryption standard (AES) calculations. The most computationally serious operations of every calculation were off stacked to an arrangement of recently characterized directions. The extra equipment required to bolster these guidelines is incorporated into the processor's information way. For each of the focused on calculations, correlations were introduced between customary programming usage and new executions that exploit the expanded guideline set engineering.

Zhou Zhibin *et al.* [52] proposed another development of CP-ABE; named Privacy Preserving Constant CP-ABE (meant as PP-CPABE) that altogether decreases the ciphertext to a consistent size with any given number of properties. Besides, PP-CP-ABE uses a concealed approach development with the end goal that the beneficiaries' protection was safeguarded productively. To the extent they know, PP-CP-ABE was the primary development with such properties. They also demonstrated PP-AB-BE was moderate as far as capacity overhead. They were chipping away at more data hypothetical examination that considers both capacity correspondences overhead in BE plans.

Wong Chung Kei *et al*. [53] they worked on a novel answer for the versatility issue of gathering/multicast key administration. They formalized the thought of a safe gathering as a triple (u, k, r) where u means an arrangement of clients, an arrangement of keys held by the clients, and a client key connection. Then, acquaint key diagrams with determine secured gatherings. For an extraordinary class of key diagrams, they introduced three methodologies for safely appropriating rekey messages after a join/leave and indicate conventions for joining and leaving a protected gathering. The rekeying systems and join/leave conventions were executed in a model key server they have assembled. They had demonstrated that their gathering key administration benefit, utilizing any of the three rekeying systems, was versatile to substantial gatherings with regular joins and takes off. Specifically, the normal measured preparing time per join/leave increments directly with the logarithm of gathering size.

Kermani Mehran Mozaffari *et al.* [54] worked on AES, concentrated various blame recognition plans for the encryption and the decoding of the AES. New blame location plans which were autonomous of the structures of the S-boxes and the backwards S-boxes were proposed. One could utilize mixes of the displayed plots keeping in mind the end goal to have a great deal more dependable AES encryption and decoding structures.

Burns F *et al*. [55] worked on a new type of advanced encryption standard (AES) execution which utilizing a typical premise. The strategy depends on a query procedure that makes utilization of reversal and move registers, which prompts a littler size of query for the S-box than it’s relating usage. The lessening in the query size depends on gathering sets of inverses into conjugate sets which thus prompts a diminishment in the quantity of query esteems. An ease execution of the AES was displayed, which focuses on a negligible number of entryways. The quantity of look into gets to are lessened, in this way enhancing inactivity.

Olteanu Alina *et al*. [56] worked on Ultra-wideband (UWB) which was another innovation that empowers remote network with predictable high information rates over numerous gadgets, for example, top quality TV (HDTV) collectors, PCs, printers and computerized cameras, inside the advanced home, and the workplace. They also concentrated on UWB transmissions where various gets to the channel were composed by the IEEE 802.15.3 medium get to control component proposed in the IEEE 802.15.3a errand gathering. Propelled encryption standard (AES), the most prominent encryption figure utilized these days, was utilized to guarantee the security of the transmission. They also concentrated the overhead presented by applying the AES figure to the transmitted casings. In particular, they break down the exchange off between throughput, payload size, and channel blunder, when AES was utilized to scramble the edges.

Prodhan Uzzal *et al.* [57] worked on AES which was actualized with single processor. At that point the outcome was contrasted and parallel executions of AES with 2 shifting diverse parameters, for example, key size, number of rounds and broadened key size, and showed that how parallel usage of the AES offers better execution yet sufficiently adaptable for cryptographic calculations.

Wang Mao-Yin *et al*. [58] worked as systems administration innovation progresses, the hole between system data transfer capacity and system handling power enlarges. Data security issues add to the requirement for growing superior system preparing equipment, especially that for constant handling of cryptographic calculations. This paper introduces a configurable engineering for Advanced Encryption Standard (AES) encryption, whose significant building pieces are a gathering of AES processors. Each AES processor furnishes square figure plans with a novel on-the-fly key extension outline for the first AES calculation and an augmented AES calculation. In this multicore engineering, the memory controller of each AES processor was intended for the most extreme covering between information exchange and encryption, decreasing intrude on taking care of heap of the host processor.

Baek Chung Hun *et al*. [59] white box cryptography introduced that was an obscurity method for securing mystery enters in programming usage regardless of the possibility that an enemy had full access to the usage of the encryption calculation and full control over its execution stages. In spite of its useful significance, advances were not considerable. It was rehashed that as a proposition for a white box usage was accounted for, an assault of lower many-sided quality was reported. In this paper, they had introduced a diagnostic tool

compartment on white-box executions of the Chow et al's. Style utilizing query tables. Subsequently, their white-box AES usage has up to 110-piece security against our tool kit, near that of the first figure. All the more by and large, they may considers a white box usage of the parallel encryption of AES to expand security.

Shang D *et al*. [60] presented a novel circuit usage of the propelled encryption standard utilizing self-planned double rail innovation. The plan diminishes spillage of inward data through adjusted power utilization, which was accomplished by evasion of glitches and by information autonomous exchanging conduct. The outline uses a pipeline structure with inherent controllers and novel, exceptionally adjusted security locks. The outline was actualized utilizing self-coordinated circuits, which evacuate the worldwide clock totally. They feel this was a fitting procedure for security outline.

Wang Mao-Yin *et al.* [61] worked on the gap between system data transfer capacity and system preparing power augments. Data security issues add to the requirement for growing elite system preparing equipment, especially that for ongoing handling of cryptographic calculations. AES chip, called tasteful, which upgrades security over standard AES outlines. The understood configurability enables the client to switch among AES-expanded square figures.

Bouillaguet Charles *et al.* [62] worked on the dominant part of current attacks on diminished round variations of piece figures looks to amplify the quantity of rounds; they seek after an alternate approach, confining the information accessible to the enemy to a couple plaintext/ciphertext sets. They displayed attacks on up to four rounds of AES that require at most three known/picked plaintexts. At that point, they had applied these attacks to tomb dissect an AES-based stream figure and to mount the best known plaintext attacks on six-round AES.

Zhang Xinmiao *et al*. [63] worked on the equipment usage of the Advanced Encryption Standard (AES) calculation, utilizing composite field math decreases the multifaceted nature as well as empowers profound sub pipelining with the end goal that higher speed could be accomplished. The ideal developments are chosen by considering the complexities of both the included sub field operations and this was omorphic mappings. Their work would address composite field developments utilizing irreducible polynomials in different structures.

Yen Chih-Hsu *et al.* [64] worked on the Advanced Encryption Standard (AES) from misery from differential blame attacks, the procedure of mistake recognition could be received to distinguish the blunders amid encryption or decoding and after that to give the data to making further move, for example, intruding on the AES procedure or re-trying the procedure.

W. Deng *et al*. [65] worked on a structure which was used to concentrate the security of key pre-dissemination plans, proposed another key pre-circulation plot which considerably enhances the strength of the system contrasted with past plans, and give an inside and out investigation of their plan as far as system versatility and related overhead. This displayed another combine insightful key predistribution plot for remote sensor networks. There plan had various engaging properties. To start with, plan was adaptable and adaptable, and hubs don't should be sent in the meantime; they could be included.

Hsiao S.-F *et al.* [66] worked on an effective basic sub expression disposal calculation was introduced to decrease the territory cost of understanding the XOR-based operations for Mix Columns, Inv Mix Columns, Sub Bytes, and in v Sub Bytes changes in the Rijndael Advanced Encryption Standard (AES). This calculation contains four streamlining needs to extricate the normal figures the bit-level conditions. They also proposed somewhat level CSE calculation to diminish the territory cost of XOR-based operations and apply the calculation to the plan of an iterative AES processor with joined MC/IMC and SB/ISB, all communicated in bit-level Boolean capacities.

Bertoni Guido *et al.* [67] worked on the objective of the Advanced Encryption Standard (AES) is to accomplish secured correspondence. The utilization of AES does not, ensure dependable correspondence. Earlier work had demonstrated that even a solitary transient mistake happening amid the AES encryption process will probably bring about countless in the encoded/decoded information. Simultaneous blame recognition was vital not exclusively to secure the encryption/unscrambling process from irregular issues. It would likewise ensure the encryption/decoding hardware from an aggressor who may perniciously infuse blames with a specific end goal to discover the encryption mystery key.

Bouillaguet Charles *et al.* [68] worked on the alternate approach, confining the information accessible to the enemy to a couple plaintext/ciphertext sets. They contend that thought of such attacks enhances their comprehension of the security of square figures and of other cryptographic primitives in view of piece figures. These attacks could be utilized to more

mind boggling attacks, either on the square figure itself or on different primitives that utilization few rounds of the piece figure as one of their parts. These attacks to crypt- analyze an AES-based stream figure and to mount the best known plaintext assault on six-round AES.

2.2. KEY GENERATION SCHEME

Wallace Jon *et al*. [69] worked on the data theoretic points of confinement of key era plans were examined in view of the level of estimation blunder, worldly relationship, and reliance of the meddler and true blue channels. Three pragmatic applicant key era plans were additionally considered, channel quantization and channel quantization with protect band. Three straightforward key era strategies were introduced, and enhancing the effectiveness and mystery of these techniques was the subject of progressing work.

Oliveira Paulo F *et al*. [70] worked on the issue of mystery key circulation in a sensor coordinate with various scattered sensor hubs and a cell phone that could be utilized to bootstrap the system. There fundamental commitment was an arrangement of secure conventions that depend on straightforward system coding operations to give a vigorous and low-multifaceted nature answer for sharing mystery keys among sensor hubs. A few security augmentations that adventures organize coding to give mystery enter circulation in extensive and dynamic sensor systems.

Zhou Heng *et al.* [71] worked on the reviews the key era issue in the two-way hand-off channel, in which there was no immediate channel between the key producing terminals. They proposed a viable key era plot that accomplishes a significantly bigger key rate than that of an immediate channel emulate approach. Dissimilar to existing plans, there was no requirement for the key creating terminals to get corresponded perceptions in their plan. They likewise examined the impacts of a dynamic aggressor on the proposed key era convention. They also described the ideal aggressor's procedure that limits the key rate of the proposed plot. Moreover, they set up the maximal aggressor's energy under which their plan could at present accomplish a nonzero key rate.

Chen Dajiang *et al*. [72] worked on the remote multipath channel as the wellspring of basic haphazardness, many key era strategies were also proposed by the data hypothesis security. Nonetheless, existing plans endure a low era rate and low entropy, and for the most part depend on hubs' portability. To defeat this confinement, they introduce a key era convention with known counterfeit impedance, named Smoke Grenade, another physical layer approach

for mystery enter era in a narrowband blurring channel. Their plan uses counterfeit impedance to add to the change of measured esteems on channel states. Their hypothetical investigation demonstrates that the key era rate increments with the augmentation of the impedance control. Reproduction comes about additionally exhibit that Smoke Grenade accomplishes a higher era rate and entropy contrasted and some state-of the-workmanship approaches.

Wang Qian *et al*. [73] worked on few intriguing methodologies were created and shown for their attainability. The cutting edge, be that as it may, even now has much space for enhancing their reasonableness. This was on the grounds that (i) the key piece era rate bolstered by most existing methodologies is low which fundamentally confines their handy utilization given the irregular availability in versatile situations;(ii) existing methodologies experience the ill effects of the adaptability and adaptability issues, i.e., they could not be specifically stretched out to bolster proficient gathering key era and sometimes fall short for static conditions. Because of these perceptions, they introduced another mystery key era approach that uses the consistently dispersed stage data of channel reactions to separate shared cryptographic keys under narrowband multipath blurring models. The proposed approach appreciates a high key piece era rate because of its proficient presentation of numerous randomized stage data inside a solitary soundness time interim as the keying sources. Contrasted with existing work that attention on pair wise key era, their approach was profoundly adaptable and could enhance the scientific key piece era rate by two or three requests of greatness.

Lai Lifeng *et al*. [74] worked on the issue of all the while setting up various keys, one for every client in an arrangement of clients, was considered with conceivable help from a gathering of committed assistants. For the case in which all clients were required to create keys, they build up a plan that is total rate ideal. For the case with devoted assistants, they build up an achievable plan and determine an external bound. They distinguish conditions under which the created conspire accomplishes the full limit area and conditions under which it was aggregate rate ideal. Further, they had practiced the review to a pair wise autonomous system show, for which they change over the key era issue to a solitary source multi-product stream over a system issue. Coupling comes about because of diagram hypothesis; they completely described the limit locale for the general instance of producing different keys with numerous aides under the PIN display, in which they have completely portrayed the limit district for the general instance of creating various keys with different committed assistants.

Lai Lifeng *et al*. [75] worked on the issue of all the while producing various free keys for different sets of clients are considered. This issue was persuaded by the way that ordinarily in remote systems, various sets of clients need to build up mystery keys for secure correspondences between these sets. They also proposed a safe steering based key dissemination way to deal with buildup keys for the terminals. This approach interfaces the issue at the hand to that of multi-ware stream issue examined in chart hypothesis. Utilizing the Max Bi-Flow Min Cut Theorem in the diagram hypothesis and building up a coordinating external bound, they demonstrate that the proposed approach accomplishes the key limit area for the instance of setting up two keys. For the general instance of building up more than two keys, an upper bound on the achievable whole rate was determined in light of the idea of multi-cut and their proposed approach could accomplish aggregate rate equivalents to the upper bound partitioned by a steady element.

Zhang Huishuai *et al*. [76] worked on the issue of at the same time producing a secret key (SK) and private key (PK) combine among three terminals by means of open exchange was researched. In this issue, every terminal watches a segment of corresponded sources. Every one of the three terminals were required to produce the regular SK to be disguised from a meddler that approaches people in general talk, while two assigned terminals are required to create an additional PK to be hidden from both the spy and the staying terminal. An external bound on the SK–PK limit area was set up and was appeared to be achievable for an exceptional case. They also proposed the SK–PK limit district is built up as a rule by creating plans to accomplish the external headed for the staying two cases. The fundamental system lies in the novel plan of an arbitrary binning-joint interpreting plan that accomplishes the current external bound.

Tavangaran Nima *et al*. [77] worked on the secret key era which was considered where the acknowledgment of the source measurement was obscure. The convention ought to ensure the security and unwavering quality of the created secret key, for every single conceivable acknowledgment of the compound source. A solitary letter bring down bound of the secret key limit with regards to a limited compound source was inferred as an element of people in general correspondence rate limitation. A multi-letter limit equation was additionally registered for a limited compound hotspot for the case in which people correspondence was unconstrained. At long last a solitary letter limit recipe was determined for a corrupted compound source with a discretionary arrangement of source states and a limited arrangement of minimal states.

Xu Peng *et al*. [78] worked on the group secret key era issues for various sorts of remote systems, by misusing physical layer qualities of remote channels. Another gathering key era system with low-unpredictability was proposed, which consolidates the entrenched indicate point combine shrewd key era strategy, the multi-portion plot, and the onetime cushion. This gathering key era process was studied for three sorts of correspondence systems: (i) the three hub arrange, (ii) the multi-hub ring system and (iii) the multi hub work organize. Three gathering key era calculations were created for these correspondence systems, separately. The investigation demonstrates that the initial two calculations yield ideal gathering key rates, though the third calculation accomplishes the ideal multiplexing pick up. Numerical outcomes were additionally given to approve the execution of the key era calculations and the time assignment calculation.

Portmann Christopher *et al*. [79] worked on the original work on verification, Wegman and Carter recommended that to confirm different messages, it was adequate to reuse a similar hash work the length of each tag was encoded with a one-time cushion. They contend that on the grounds that the one-time cushion was flawlessly concealing, the hash work utilized remains totally obscure to the enemy. Since their evidence was not composable, they return to it utilizing a composable security system. For reasons unknown the above contention was inadequate: if the foe learns whether a debased message was acknowledged or dismisses, data about the hash capacity was spilled, and after a limited measure of rounds it was totally known.

Ye Chunxuan *et al*. [80] worked on the pair-wise independent network where each terminals in the system watches a typical match savvy source that was autonomous of the considerable number of sources open to alternate sets. A strategy for secret key agreement in such a system, to the point that depends on settled indicate point methods and rehashed use of the one-time cushion. The conventions for the first two issues were ideal and the convention for the third issue was proficient, regarding the subsequent mystery key rates.

Nitinawarat Sirin *et al*. [81] worked on the secret key generation for a pair wise independent network model in which each match of terminals watches associated sources that were autonomous of sources seen by every other combine of terminals. The terminals were then permitted to discuss freely with all such correspondence were seen by every one of the terminals. The goal was to produce a mystery key shared by a given subset of terminals at the

biggest rate conceivable, with the collaboration of any residual terminals. At the point when just two of the terminals or when every one of the terminals look to share a mystery key, the said calculation accomplishes mystery enter limit in which case the bound was tight.

Gharout Saıd *et al*. [82] worked on the key administration concerns the circulation and updates of the key material each time a part joins or leaves the gathering. The dynamic part of gathering applications because of free enrolment joins and leaves notwithstanding individual's portability makes troublesome the plan of productive and versatile key administration conventions. They also proposed an instrument that abstains from re-establishing the TEK when the part moves from a territory to another. Re-enactment comes about demonstrated that their conventions accomplishes a superior execution exchange offs contrasting with different conventions.

Li Fagen *et al*. [83] worked on the confidentiality and verification which were two fundamental security objectives in secured electronic mail (email). Really great protection (PGP) and secure/multipurpose web mail expansions (S/MIME) were two celebrated secure email arrangements. Both PGP and S/MIME utilized advanced envelope to give message confidentiality and computerized mark to give message validation. They also proposed another idea called deniably validated encryption that could accomplish confidentiality and deniable verification in a legitimate single stride. They had additionally planed a protected email convention utilizing the proposed deniably confirmed encryption conspires.

Seo Seung-Hyun *et al.* [84] proposed a certificateless-effective key management (CL-EKM) convention for secured correspondence in unique WSNs portrayed by hub versatility. The convention likewise underpins effective key renouncement for traded off hubs and limits the effect of a hub bargain on the security of other correspondence joins. A security examination of their plan demonstrates that their convention was powerful in guarding against different attacks. CL-EKM underpins effective correspondence for key updates and administration when a hub leaves or joins a bunch and thus guarantees forward and in reverse key mystery.

Kakkar Ajay *et al*. [85] worked on a new approach for producing keys from the accessible information. The examination of different circumstances, for example, encryption, decoding, key setup, preparing, and key moving circumstances, was finished. The model sets aside least opportunity to supplant the broken keys with the new keys. The security additionally increments, if the key size was expanded and the key moving time (δ) was reduced; the

above blend might be received for secure transmission. This work could be developed, if more number of S-Boxes (64 and 128) was utilized for a similar assignment, and the key length would be decreased with ostensible preparing time.

Menesidou Sofia Anna *et al*. [86] proposed a framework for evaluation of key exchange protocols in a DTN setting. Their commitment was twofold as the proposed structure could be utilized as a basic leadership device for mechanized assessment of different correspondence situations with respect to steering choices and as a component of a technique for convention assessment in DTNs. They also proposed a strategy for all intents and purposes assessing key trade conventions in systems of unfriendly feline particle conditions. The apparatus was intended to suit a plenty of intelligent conventions for key trade as well as key foundation. The apparatus was acknowledged as a convention parser that could be utilized either as a basic leadership instrument running on a DTN hub or a strategy for convention assessment in DTN conditions.

Koyluoglu O. Ozan *et al*. [87] worked on accomplishing data theoretic security with down to earth coding multifaceted nature was of unequivocal intrigue. This work initially concentrates on the key assention issue. For this issue, another traverse square blurring channels was proposed. The proposed plot requires just the measurable learning about the meddler channel state data (CSI), and, using a protection enhancement procedure, diminishes the issue of key consent to a provably secure coding issue per square.

2.3. AUTHENTICATION SCHEME

Tsai Jialing *et al.* [88] worked on smart card based authentication scheme which was broadly used for different exchange arranged administrations, for example, electronic money trade, social protection instalment and online business instalment charge in present day society. To begin with presents a security display for mysterious verification and after that proposed another unknown validation plot utilizing keen card. Another security demonstrates for mysterious verification is first exhibited. In view of this security display, a brilliant card based verification conspire with client untraceability was presented. As far as calculation cost, their plan was almost productive as the most proficient plans created.

Cheng Chi *et al.* [89] worked on the homomorphic message authentication code (MAC) plans was proposed to oppose against contamination attacks in system coding. Nonetheless, existing techniques confront a typical test: the produced MAC technique had a place with a

little limited field, which implies that an enemy could assault by arbitrarily speculating the estimation of t, and prevail with likelihood $1 = q$. Since q was a foreordained framework parameter which is normally set as 28, they came about security $1 = 256$ could be unacceptable. In this paper, they proposed an effective homomorphic MAC for validation in system coding. The proposed technique accomplished a dependable security parameter $1 = ql$ utilizing just a single key, where l could be picked by various security necessities. Contrasted and past methodologies that utilizing various labels, they proposed homo-morphic MAC had both low calculation and correspondence overheads.

Nicanfar Hasen *et al.* [90] worked on the proficient plan that commonly confirmed a keen meter of a home territory organize and a validation server in SG by using an underlying secret key, by diminishing the quantity of ventures in the safe remote watchword convention from five to three and the quantity of traded bundles from four to three. They also proposed an effective key administration convention in view of their improved personality based cryptography for secured SG interchanges utilizing the general population key framework. They have displayed novel shared validation and key administration systems custom fitted for the SG correspondences.

Saxena Neetesh *et al.* [91] worked on the short message service (SMS) was being utilized as a part of numerous day by day life applications, including medicinal services observing, versatile managing an account, portable business, et cetera. Be that as it may, when they send a SMS starting with one cell phone then onto the next, the data contained in the SMS transmit as plain content. They also proposed an effective and secure convention called EasySMS, which gives end to end secure correspondence through SMS between end clients. This convention produces lesser correspondence and calculation overheads, uses data transmission proficiently, and lessens message traded proportion amid confirmation than SMSSec and PK-SIM conventions.

Dasari Nagamalleswara Rao *et al.* [92] proposed novel multi server verification and key understanding plans with client assurance in system security. They initially proposed a solitary server plan and after that apply this plan to a multi-server condition. The fundamental benefits include: (i) The security of clients could be guaranteed; (ii) a client could be unreservedly pick his own watchword; (ii) the calculation and correspondence cost is low; (iv) servers and clients could confirm each other; (v) it creates a session key concurred by the

server and the client; (vi) Their proposed plans were Nonce-based plans which does not have a genuine time synchronization issue.

Yang Hung-Wen *et al*. [93] worked on a result of the explosive growth in development for computer networks and information technologies in recent years, different exercises happen on the Internet, for example, the interactive media administrations. The conveyance of huge scale advanced substance had turned out to be less demanding and more proficient than any other time in recent memory. An innovation of advanced rights administration (DRM) alludes to any of a few encryption advances used to secure computerized substance against unapproved replicating, and to control the dispersion. Once the aggressor acquired the right secret word, the session key between the client and the server would be bargained.

Sayed Bassam *et al*. [94] worked on another mouse flow examination structure that utilizations mouse signal progression for static validation. The caught motions were investigated utilizing a learning vector quantization neural system classifier. The proposed structure utilized a measured outline of the LVQ neural system for classification. The outcomes gotten with four motions demonstrate that more work must be done to expand the precision of their proposed plot before it could be utilized as a part of practice for static verification.

Kumar Sangeeth *et al*. [95] worked on any of the processing condition running from a conventional figuring to the rising administration based registering, security and protection was an imperative thought in the design. Especially client confirmation was a passage indicates every single application and administrations distributed. Broad research work in client verification had yielded a few validation conspires however the current plans concentrates to a great extent on the advantages as opposed to their drawback as far as security, convenience and sending capacity, which were observed to be ineffectual when sent in this present reality. To defeat this issue, a positioning model was proposed in this paper dissects the confirmation conspire in view of their confinements and gives an organized plan in light of which the best instrument at a specific occasion of time could be picked and actualized

Fouda Mostafa M *et al.* [96] worked on the smart grid (SG) communication had as of late gotten critical considerations to encourage wise and disseminated electric power transmission frameworks. Nonetheless, correspondence trust and security issues still present down to earth

worries to the organization of SG. In this paper, to adapt to these testing concerns, they had proposed a lightweight message validation conspire includes as an essential yet urgent segment for secure SG correspondence system. In particular, the savvy meters which were appropriated at various progressive systems of the SG could first accomplish common validation and build up the mutual session key with Diffie-Hellman trade convention. At that point, with the mutual session key between shrewd meters and hash-based verification code system, the consequent messages could be confirmed lightweight. Later on work, they will additionally investigate other testing security issues, for example, foreswearing of administration attacks, in SG condition.

Kakkar Ajay *et al*. [97] worked on the quantity of security attacks against system was expanding significantly with time. To ensure the model against these attacks; procedures like passwords, cryptography, and biometrics were utilized. They had managed the parameters, for example, number of clients, disappointment rate of different keys, recuperation component, encryption, transmission, decoding and inactivity time, and so forth. The point was to build up an encryption calculation which gives numerous keys created from the information itself and must be overhauled naturally.

Yang Guomin *et al*. [98] investigated the security necessities of this sort of plans, and proposed another plan and a bland development system for shrewd card-based secret key confirmation. Brilliant card-based watchword confirmation was a standout amongst the most helpful approaches to give two-consider verification to the correspondence between a customer and a server. They had characterized an arrangement of attractive properties for secured smartcard-based secret word validation plans. They gave proof to bolster the need of each of the properties.

2.4 OBSERVATIONS

From the work done by the various researchers in the field of data security, following observations have been drawn:

- If single key of short length is used to encrypt data, the security level is very poor. Key management should optimize in order to reduce the processing time.
- Existing conference schemes are vulnerable to many attacks; therefore, there is always a chance of eavesdropping, non-repudiation and unauthorized access of data.
- Random attacks also ruin the cryptographic model and hacker gets hold of the system.

- Multiple keys of fixed or variable length are more resistive to random attacks. Few protocols were used for security improvement, but these were denied for practical use due to various flaws such as lack of mutual authentication and vulnerable to random attacks.

2.5 GAPS AND PROBLEM FORMULATION

From the above observations, it has been observed that various encryption algorithms which have been used by different researchers are not so much effective from security point of view, that's why there is still need to either modify an algorithm or which key management provides more data security and provides efficient key management system for utilizing the multiple keys to increase the data security. The strength of cryptographic model relies on the key generation process; for a better security level TDES makes the use of three different keying options in comparison with DES. The method of employing multiple keying is effective from the security point of view but not good in terms of processing time. Overheads are more prominent in TDES due to triple padding. The newly generated keys by the user are handled by the CA; if any user wants to leave the pool then the keys are withdrawn from him and are destroyed by the CA. The keys used by the higher classes must be derived from lower classes; therefore, the reliability of higher level keys depends upon the lower level keys. Transmission of keys in a pool requires certain protocols and these are responsible for the replacement of faulty keys.

Finally, from the previous section, objectives have been drawn and are as follows:

- To study the various encryption algorithm and key generation techniques.
- To modify the key generation process from the available data.
- To evaluate the processing time in encryption process based upon single and multiple keys.

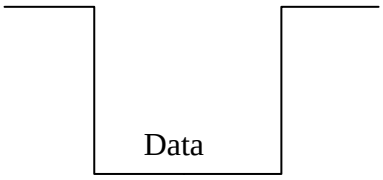
CHAPTER 3

PROPOSED WORK

Encryption has been done using sub bytes where we replace of every byte with another byte. Keeping in mind the importance of multiple keys for secure data transmission, this work incorporated the use of multiple keys. Multiple keys were generated from the available data to reduce the overheads such as the need of sending additional bits along with the data. The proposed flowchart has been shown in figure 3.4 Key generations has been done which is based upon hex to decimal conversion. We can generate the multiple keys for more secure data transmission and generate the results. As similar to that we generate multiple key. After the generation of both single and multiple keys (8, 16 and 32 bit key length), we compare the processing time and the level of security.

3.1 GENERATION OF KEYS FROM THE AVAILABLE DATA

The proposed calculation utilizes the accessible information to generate keys and furthermore avoids the need of transmitting extra bits alongside the figure content. It enhances the transfer speed and execution of the model, which improves the information rate. The key era component was utilized to know both the sides, so that, the mix of keys has been utilized for recovering the information. The key era prepare additionally relies on the information stream to generate the keys. It likewise speaks to the different conditions for the operation to be performed by the S-Boxes, keeping in mind the end goal to outline a multi node having single or numerous keys of a fixed and variable length. On the off chance that the key size is small and has a fixed length, at that point it is disposed of because of its poor security reaction. There is a need to decide the disappointment rate of all the keys in a multi node for secure information transmission. The calculation checks the information stream, and further key era handle was utilized to plan the different keys utilizing S-Boxes.



A= 01010110- first block size

B=10110101- second block size

Figure 3.1 Pool to generate the keys from the available data

Generate the keys from the available data with S-Boxes.

Key(s) have been generated using the table 3.1. These are based upon the data available in the pool. For the alphabets, numbers, alphanumeric and hybrid data type, we are taking input data

from the pool and as shown in the table we apply some conditions on the input data and then perform some operations to generate single or multiple keys for comparing the security level. As that, we are generating the key from the available data using S-boxes.

Data type	Conditions	Operations performed by S-Boxes	Key length (KL)	Round functions (RFs)
Alphabets	A>B A=B A<B	A+B A-B A*B	An 8-bit KL is used if the input data stream is ≤16 bits; otherwise a 16-bit KL is used	8 RFs are used if the input data stream is≤16 bits; otherwise 16 RFs are used
Numbers	A>B A=B A<B	A+B A-B A*B	An 8-bit KL is used if the input data stream is≤8 bits; otherwise a 16-bit KL is used	8 RFs are used if the input data stream is≤8 bits; otherwise 16 RFs are used
Alphanumeric	A>B A=B A<B	A+B A-B A*B	An 8-bit KL is used if the input data stream is ≤16 bits; otherwise a 16-pbit KL is used	8 RFs are used if the input data stream is≤16 bits; otherwise 16 RFs are used
Hybrid	A>B A=B A<B	A+B A-B A*B	An 8-bit KL is used if the input data stream is ≤32 bits; otherwise a 16-bit KL is used	8 RFs are used if the input data stream is≤32 bits; otherwise 16 RFs are used

Table 3.1 Generate the keys from the available data with S-Boxes

3.1.1 Single key

Single key has been generated from the pool on the basis of condition shown in table 3.1. Initially take the input from the pool and applying conditions on the data using S-boxes. Further, we generate the single key from the available data. Single keys are not very effective for security point of view. It is of short length and easily hacked by hacker.

Once the key was produced, the encryption was done utilizing the fixed and variable length keys. The variable length key was favoured because of less overhead, and it additionally gave a more secure model. The cushioning overheads were less for this situation. The disappointment rate of a key was checked utilizing numerical devices; for feeble hubs, there-encryption was finished utilizing the second key, which under goes a strategy the same as that experienced by the first key. The second key is required; if there is a hub disappointment or the information arrangement is extremely large. The key quality is high on account of half breed information successions since, more mixes are accessible for the era of keys.

3.1.2 Multiple keys:

Multiple keys were generated from the available data. Initially, data were placed in a pool and divided into nearly two sections. Both the sections were compared, and further based upon the conditions, proper operations were performed. If A > B and the data are in the terms of alphabets only, then the A+B operation has been performed in the initial phase and is named as the first round function. The output of this operation is used by the second round operation, which requires another operation for its working. These operations are randomly selected and they provide different outputs, even if the pool has the same data for multiple keys. This procedure continues for 8 and 16 iterations depending upon the required security level for a given multi node. For A > B and data stream greater than 16 bits, a16-bitkeycanbe used for the encryption of data. The first key was generated using the following method: assume that A=1000001011000101 and B=0101100100101010 are the two data streams available in the pool, then the first round function uses the first operation, which is given as follows:

$$A = 1000001011000101,$$
$$\underline{B = 0101100100101010,}$$
$$C = 1101101111101111$$

C is the output of the first round function, which is further used by the second round function, which is based upon the left shifting of the stream by 1 bit and is given as

$$C = 1101101111101111,$$
$$D = 1011011111011111$$

The output of the second round function is further used by the next S-Box and the process continues for 8 or 16 iterations. Similarly, the second key was generated by keeping an eye on the length and type of input data.

Algorithm for conversion

Initially, input in hex values has been taken and then converted into the decimal numbers with the MATLAB code and simple way hex2dec conversion. This is the way to assign code to the values; we can say that the key is generated.

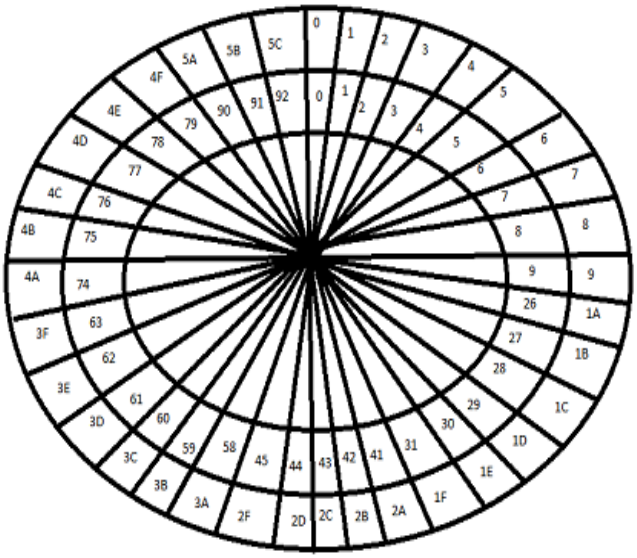


Figure: 3.2 Conversion of alphabets into their equivalent codes.

Figure 3.2 is showing the alphabets and their equivalent codes. The results of this code have been shown by the screen short (3.3). MATLAB code hex2dec simple conversion 0 to 9 having same equivalent codes and the alphabets A to Z has been used. (we assign the numbers 1a,1b,1c,1d,1e,1f then 2a,2b,2c and so on up to z) having their equivalent decimal values respectively. Algorithm for the conversion of the data into decimal value in MATLAB is explained below:

a. Algorithm for conversion

- *Take the input value.*
- *Input value is in the form of hexadecimal number.*
- *Convert the hexadecimal number to decimal number.*
- *Now, use the hex2dec command in MATLAB to convert values.*

Command window results

```
Enter the hexadecimal number:2A

STR =

2A

value =

    42
```

Figure 3.3 command window results for conversion

This figure 3.3 shows the command window results which is run in the MATLAB. In this the STR shows input value and 2A is the hex value which we want to convert into decimal value and the value is the output which is the decimal value of the 2A i.e. 42. As this the conversion is completed.

Coding for the special character used in the hybrid: The special symbols were also processed, in the proposed scheme. The key strength is very high in the case of hybrid structure.

!	@	#	^	/	&	*	(	)	!	,
110	111	112	113	114	115	116	117	118	119	120
$	%	`	~	-	_	+	=	[	]	.
121	122	123	124	125	126	127	128	129	130	131
{	}	\	|	;	:	“	‘	<	>	?
132	133	134	135	136	137	138	139	140	141	142

Table 3.2 special characters and their equivalent codes

It offers more resistance to the hacker, and as a result, the model remains secure for more time. To protect the data from intruders, powerful encryption algorithms with multiple keys

were used. After the encryption process, it is desirable to transmit the cipher text over the channel. The secure model was examined on the basis of its design, mode of transmission of data, and number of nodes. With an increase in the number of nodes, key length, number of keys, and data length, the model consumes more power and takes more time to generate keys from the available data. A new approach in which keys are generated and processed in the cryptographic model with the help of S-Boxes in order to reduce the processing time has been proposed.

b. Algorithm for Key Generation

- *Take two binary inputs (8, 16, 32) a & b.*
- *Then and both the inputs a & b.*
- *Results of and both inputs generate the key.*
- *Now X-OR the key and a input this will give the cipher text.*
- This is for the single key.

c. For the multiple key generations:

- *Same 4 steps performed like single key.*
- *Next step is to invert the key with 1s complement.*
- *And then bit-or the inverted key and cipher text that will re-encrypt the data.*
- *Then again generating key with performing the 2s complement on the already generated key.*
- *Then bit-and the new key with cipher text to get the re-encrypted data.*
- *Next step is to invert the cipher text.*
- *Then bit-shift and dec2bin is used to generate the key.*
- *Finally bit-or the new key with re-encrypts data last time and finally the cipher text is ready to send.*

3.2 PROPOSED FLOWCHART

Figure 3.4 shows the multiple key generation flowchart. As shown above the steps of multiple key generations are discussed. First the key is generated, which is the result of two binary inputs. C is the cipher text that is encrypted with key. Again perform functions on key and generate the keys and encrypt the cipher text that is called the re-encryption.

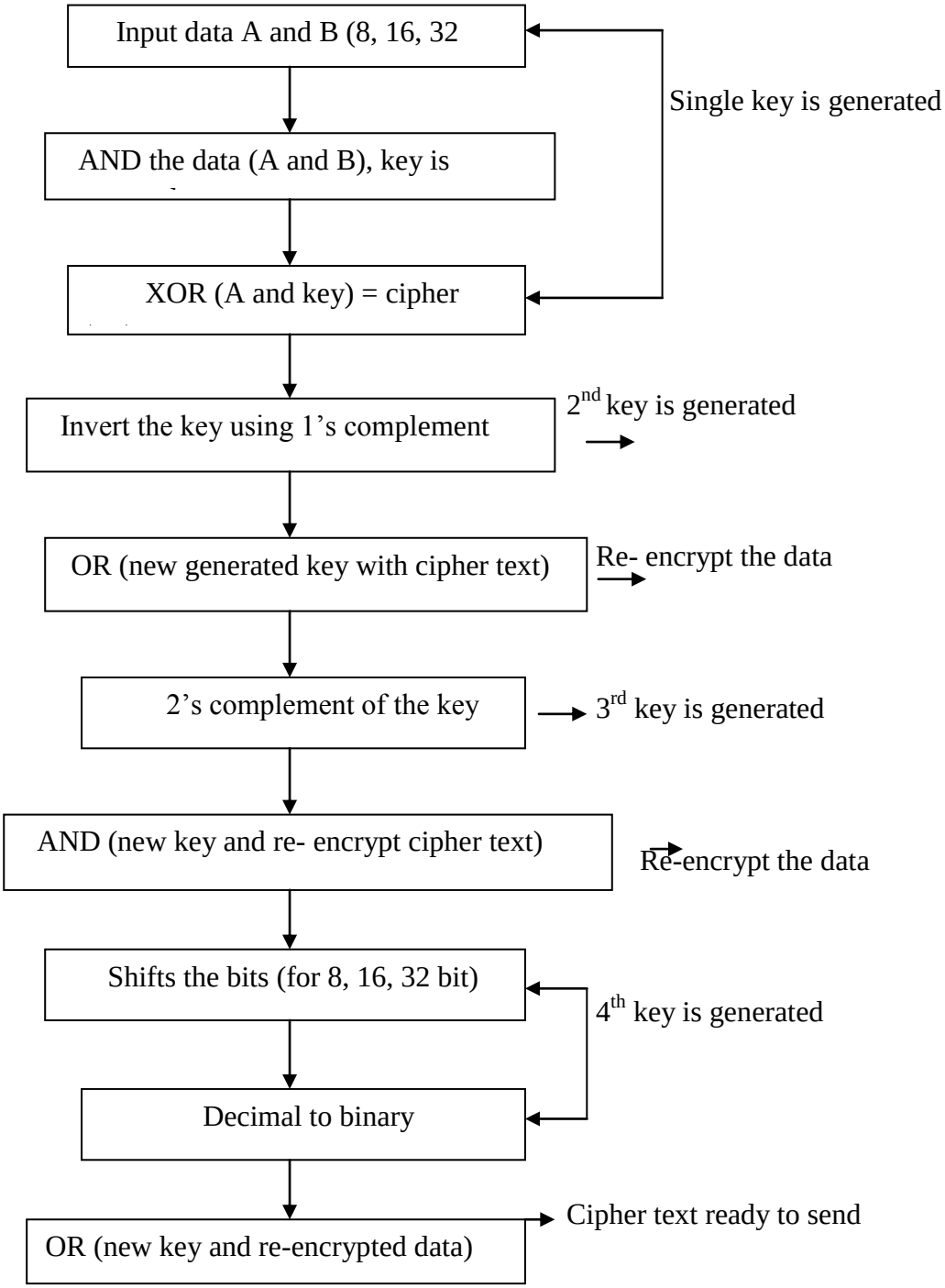


Figure 3.4 Proposed flowchart

CHAPTER 4

RESULTS AND DISCUSSION

This chapter shows the results of data security with single and multiple keys which have been obtained using MATLAB. Further, comparison of single and multiple keys has also been done.

4.1 SINGLE KEY

Single key of 8, 16, 32 and 64 bit key length has been used to encrypt the data block which is of 8, 16, 32 and 64bit length. There are four cases which are as follows:

Case1 – 8 bit key length with different data lengths (8, 16, 32 and 64)

In this, 8 bit key length is used to encrypt the different block data lengths. It is very easy and fast response method. When encryption of 8 bit data has been done with 8 bit key length which is of very short length, the system is very much open to the hacker. Hence, it does not provide the data security. When same key is used to encrypt the 16 bit data length, the system takes more processing time; therefore, it becomes very easy job for the hacker. When we are using 8 bit key length with 32 bit data length, processing time further increased and it does not offered good security level. For 64 bit data length processing time is very high and it is the worst combination from security point of view.

Case2 – 16 bit key length with different data lengths (8, 16, 32 and 64)

In the second case, we are using the 16 bit key length to encrypt the different block lengths of 8, 16, 32 and 64 bits. 16 bit key length is better than 8 bit key length. The security level is slightly better than the 8 bit key length but not suitable for the data transmission over web. When 8 bit data block is encrypted with 16 bit key length, better security level has been observed but the overheads bits are increased. As a result, the cost of system will increase. 16 bit data and 16 key length combinations provide marginal acceptable security level. When 32 bit data length has been encrypted with same key, overheads are further increased, which ruin the system. As a result, processing time increases, therefore, hacker gets more time to generate the random attacks. It does not provide more resistance to the hacker. Finally this combination is rejected. When 64 data block have been encrypted by 16 bit key length, the processing time is very large; therefore, this combination is not accepted. The security level does not provide enough resistance to the hacker.

Case3 – 32 bit key length with different data lengths (8, 16, 32 and 64)

In this case, we are using the 64 bit key length to encrypt the different data lengths. 32 bit key length in single key offers the good security method for 8 bit data sequence. Because it has the large key length; therefore, it is difficult to hack the data but still not treated as the best method. When 32 bit key length is used to encrypt the 16 bit data, the security level falls a bit. This combination is marginally acceptable for smaller groups. When 32 bit key used to encrypt 32 bit data, the security level further degraded. This combination has more overheads and more processing time; therefore, it is rejected. Last combination is 32 bit key with 64 bit data. This combination is rejected due to high processing time and poor security level, although we have more data bits in the pool to generate the key.

Case4 – 64 bit key length with different data lengths (8, 16, 32 and 64)

64 bit key length in single key is the best security method. Because it has large key length so it is difficult to hack. This gives the best security at this point. First combination 64 bit key is used to encrypt the 8 bit data. This combination offers the best security. Second case 64 bit key length is used to encrypt the 16 bit data. The security level slightly falls as compared to previous value but still acceptable. Third combination is 32 bit data and 64 bit key length which offers moderate security. Last combination is 64 bit data and 64 but key length. This offers poor security level.

Single and multiple key generations using arithmetic operations:

8 bit key and 8 bit data length: Figure 4.1 shows the MATLAB results for 8 bit data key length. These results are performed by the arithmetic operations. In the figure 4.1, a and b are 8 bit input data. C is the result of comparison of both the input i.e. greater than, equal and less than. Result of c is the key that we are using for encrypting the data. At the end, key is used with the one input to encrypt the data. So, d is the cipher text that is encrypted with the key. Same process followed for the generation of 16, 32, and 64 bit data using 8 bit key length. Their MATLAB results have also been shown in figure 4.1, 4.2, 4.3, 4.4 respectively:

```
a =

    10100110

b =

    10110010

c =

  1.0211e+014

d =

  1.0313e+021
```

Figure 4.1 8 bit key and data length

Single key generation- 16 bit data and key length: Figure 4.2 shows the MATLAB results for 16 bit data key length. These results are performed by the arithmetic operations.

```
a =

  1.1100e+015

b =

  1.1110e+015

c =

  1.2332e+030

d =

  1.3689e+045
```

Figure 4.2 16 bit key and data length

Single key generation- 32 bit data and key length: Figure 4.3 shows the MATLAB results for 32bit data key length. These results are performed by the arithmetic operations

```
a =

  1.0100e+031


b =

  1.1010e+031


c =

  1.1120e+062


d =

  1.1232e+093
```

Figure 4.3 32 bit key and data length

Single key generation- 64 bit data and key length: Figure 4.4 shows the MATLAB results for 64 bit data key length.

```
a =

  1.1001e+062


b =

  1.1010e+062


c =

  1.2112e+124


d =

  1.3325e+186
```

Figure 4.4 64 bit key and data length

Single and multiple key generations using logical operations:

Figure 4.5 shows the 8 bit key length single key generation MATLAB results. In this we are generating the single key with 8 bit key length using logical operations.

```
key =

     0     0     0     0     1     0     1     1

c =

     0     0     0     1     0     0     0     0
```

Figure 4.5 8 bit key length single key generation

Initially, we had taken two inputs a data bit which is of 8 bit each. Then, perform the logical operation on the inputs that is AND operation, that will generate the key for the 8 bit of data. At the end, key and first input performed another logical operation to encrypt the data i.e. called the cipher text. This is shown by c here. Figure 4.5 shown the key and cipher text that is generated in MATLAB, and it shows the command window results. Same process followed for the generation of 16 and 32 key length. Their MATLAB results are shown in figure 4.6 and 4.7 respectively.

The 16 bit key length single key generation MATLAB results: In this, we are generating the single key with 16 bit key length using logical operations.

```
key =

  Columns 1 through 13

     0     0     0     0     1     0     1     1     0     0     0     0     1

  Columns 14 through 16

     0     1     1

c =

  Columns 1 through 13

     0     0     0     1     0     0     0     0     0     0     0     1     0

  Columns 14 through 16

     0     0     0
```

Figure 4.616 bit key length single key generation

The 32 bit key length single key generation MATLAB results: In this, we are generating the single key with 32 bit key length using logical operations.

```
key =

  Columns 1 through 13

     0     0     0     0     1     0     1     1     0     0     0     0     1

  Columns 14 through 26

     0     1     1     0     0     0     0     1     0     1     1     0     0

  Columns 27 through 32

     0     0     1     0     1     1


c =

  Columns 1 through 13

     0     0     0     1     0     0     0     0     0     0     0     1     0

  Columns 14 through 26

     0     0     0     0     0     0     1     0     0     0     0     0     0

  Columns 27 through 32

     0     1     0     0     0     0
```

Figure 4.7 32 bit key length single key generation

4.2 MULTIPLE KEY

Multiple key generation using logical operations: The 8 bit key length for multiple keys generation, results are shown in the figure 4.8 similar results for 16 and 32 bit key length have been obtained.

```
key =

     0     0     0     0     1     0     1     1

c =

     0     0     0     1     0     0     0     0

key1 =

     1     1     1     1     0     1     0     0

c1 =

     1     1     1     1     0     1     0     0

key2 =

     1     1     1     1     1     1     1     1

d =

     1     1     1     1     0     1     0     0

d =

     1     1     1     1     0     1     0     0

ct =

     0     0     0     0     1     0     1     1

e =

  255

f =

  248

g =

11111000

ct1 =

     1     1     1     1     1     0     1     1
```

Figure 4.8 8 bit multiple key generations.

Three keys have been generated using the table 3.1 (Chapter 3).

Case1 – 8 bit key length with different data lengths (8, 16, 32 and 64)

Multiple keys have been generated using the table 3.1, which are based upon conditions. 8 bit key length is a short length but its security is equal to the 32 bit key length of single key. In this data are encrypted 2 or 3 times, this is called the re-encryption. It is a good method from security point of view. Second combination is 8 bit key length with 16 bit data. Due to multiple encryptions all the combinations are offered good security level. Processing time is slightly increased but security level is good. Third combination is 8 bit key length with 32 bit data. Key length is small but we are using the re-encryption due to that processing time is further increased and security level is marginal acceptable. Last combination is the 64 bit data sequence with 8 bit key length. In this security level is poor due to large amount of data.

Case2 – 16 bit key length with different data lengths (8, 16, 32 and 64)

16 bit key length is large then 8bit, the security level is slightly better than the 8 bit key length. When 8 bit data is encrypted with 16 bit key using multiple keys it offers very good security level. When the 16 bit data sequence is encrypted with 16 bit key, it also offers good security due to multiple encryptions but processing time is marginally increased. Third combination, when 32 bit data is encrypted with 16 bit key, due large size, it offers the marginal acceptable security level. Finally, when 64 bit data sequence has been encrypted with 16 bit key length, the poor security level has been observed.

Case3 – 32bit key length with different data lengths (8, 16, 32 and 64)

Encryption with 32 bit key length with multiple keys is considered as good method for data security. Due to large key length, it takes more processing time but it is not prominent. Hence, it is still treated as the good data security method compared to case1 and case2. Firstly, we are using the 32 bit key to encrypt the 8 bit data. For small groups this combination offers the good security. For the second combination, 32 bit key length with 16 bit data sequence, it offers good security but processing time is large in this combination. For the same key size and 32 data length, security level slightly falls and processing time is also increased. For the last combination, when 32 bit key length is used to encrypt the 64 bit data block, the security level is degraded as compared to other combination, hence this combination is not acceptable.

Case4 – 64 bit key length with different data lengths (8, 16, 32 and 64)

64 bit key length is the best method due to its large key length. For 8 bit data this offers the best security than all the other combination and cases. Large key size offers the best security level for all the combination and also using the multiple key so, that it provides more security and large processing time. Second combination is 16 bit. 64 bit key offers very good security to the 16 bit data length. Processing time increased but still a good security method. Further in the 32 bit data length data is increased so the security level is degraded but we are using multiple keys so, processing time increased but security level is marginal accepted. For the last combination data and key both are of same size. In this combination security falls a bit but due to multiple keys still offers better security.

Multiple key generation

Initially we are taking two inputs data bits of 8 bit. Second step is to perform the function on the inputs that is AND operation. This will generate the key for the 8 bit of data. This is first generated key and this key is used to encrypt the cipher text. Then, again perform a second function on the first key that is inverting the bits. Now, the second is used to re encrypt the cipher text that is called the re encryption. Keys are shown by key 1 and key 2. And c is the cipher text here in the figure 4.9. Again performing function on the key and cipher text for more security. At the end, cipher text is ready to send, figure 4.9 shows the command window results. Same process and same steps used to generate keys for 16bit and 32 bit key length.

Multiple key generation - 8 to 8

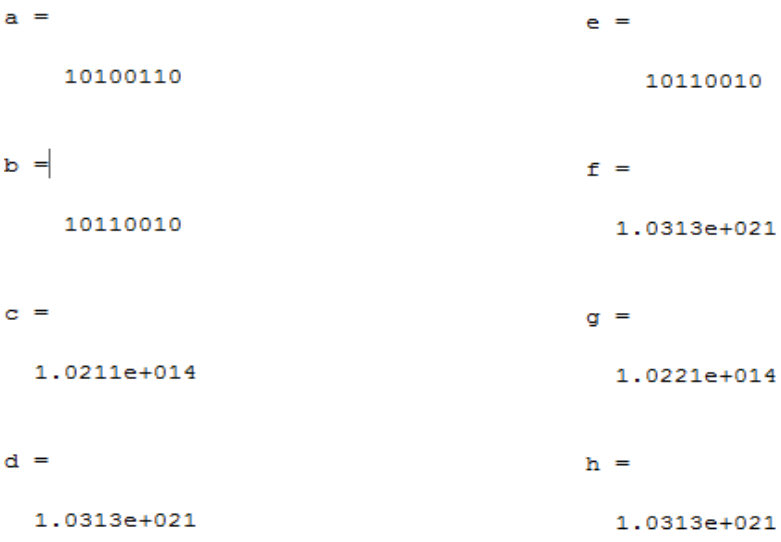


Figure 4.9 8 bit key and data length for multiple key generation

Multiple key generation - 16 to 16: Figure 4.10 shows the MATLAB results for 16 bit data key length. These results are performed by the arithmetic operations.

```
a =

   1.1011e+013

b =

   1.0110e+015

c =

   1.1132e+028

d =

   1.2258e+041

e =

   1.0110e+015

f =

   1.2258e+041

g =

   1.0221e+030

h =

   1.2258e+041
```

Figure 4.10 16 bit key and data length for multiple key generation

Same steps follows for the multiple key generations for 16 to 8, 32 and 64 data length and other cases.

Different keys and their processing time using logical operations

Key length	**Data length**	**Processing time (s)**
8 bit single key generation	8	0.057
16 bit single key generation	16	0.079
32 bit single key generation	32	0.081
8 bit multiple key generation	8	0.422
16 bit multiple key generation	16	0.214
32 bit multiple key generation	32	0.188

Table 4.1 Different keys and their processing time using logical operations

4.3 COMPARISON OF SINGLE AND MULTIPLE KEYS (2, 3)

Table 4.2 shows the comparison of single and multiple keys of (2, 3). Comparison of keys has been done by data, key, processing time and security level.

Single key				Multiple keys (two keys)				Multiple keys (three keys)			
Data length (bits)	Key length (bits)	Processing time (s)	Security Level	Data length (bits)	Key length (bits)	Processing time (s)	Security Level	Data length (bits)	Key length (bits)	Processing time (s)	Security Level
8	8	0.73	Poor	8	8	0.77	Slightly improved	8	8	0.79	Good
8	16	0.74	Slightly increased	8	16	0.80	Marginal acceptable	8	16	0.81	Slightly improved
8	32	0.76	Marginally acceptable	8	32	0.83	Good	8	32	0.84	Very good
8	64	0.78	Good	8	64	0.84	Best	8	64	0.85	V.V. good
16	8	0.74	Very poor	16	8	0.82	Very poor	16	8	0.85	Poor
16	16	0.75	Poor	16	16	0.83	Poor	16	16	0.86	Slightly improved
16	32	0.77	Slightly improved	16	32	0.84	Improved	16	32	0.87	Good

16	64	0.79	Good	16	64	0.86	Good	16	64	0.87	Very good
32	8	0.76	Poor	32	8	0.82	Very poor	32	8	0.84	Very poor
32	16	0.71	Slightly improved	32	16	0.84	Poor	32	16	0.86	Poor
32	32	0.83	Marginal acceptable	32	32	0.85	poor	32	32	0.88	Good
32	64	0.87	Good	32	64	0.88	Improved	32	64	0.89	Marginally acceptable
64	8	0.89	Good	64	8	0.90	Very poor	64	8	0.91	Very poor
64	16	0.90	Better	64	16	0.91	Poor	64	16	0.92	Poor
64	32	0.93	Acceptable	64	32	0.95	Acceptable	64	32	0.97	Good
64	64	0.95	poor	64	64	0.97	Improved	64	64	0.99	Very good

Table 4.2 Comparison of single and multiple keys (2, 3)

4.4 COMPARISON OF KEYS: PROCESSING TIME WITH SINGLE AND MULTIPLE KEYS

Figure 4.11 shows the relationship between processing time and keys (single, two and three). This is for the 8 bit key length compared with 8, 16, 32, 64 bit data length. In this, we are using 8 bit key length and comparing its processing time with different data lengths. In the single key processing time is very fast but security level is poor. In the multiple keys (2, 3) processing time is increased but security level is also increased. Same for the 16, 32 and 64 bit key length. Their graphs results showed in the figure 4.11, 4.12, 4.13, 4.14 respectively.

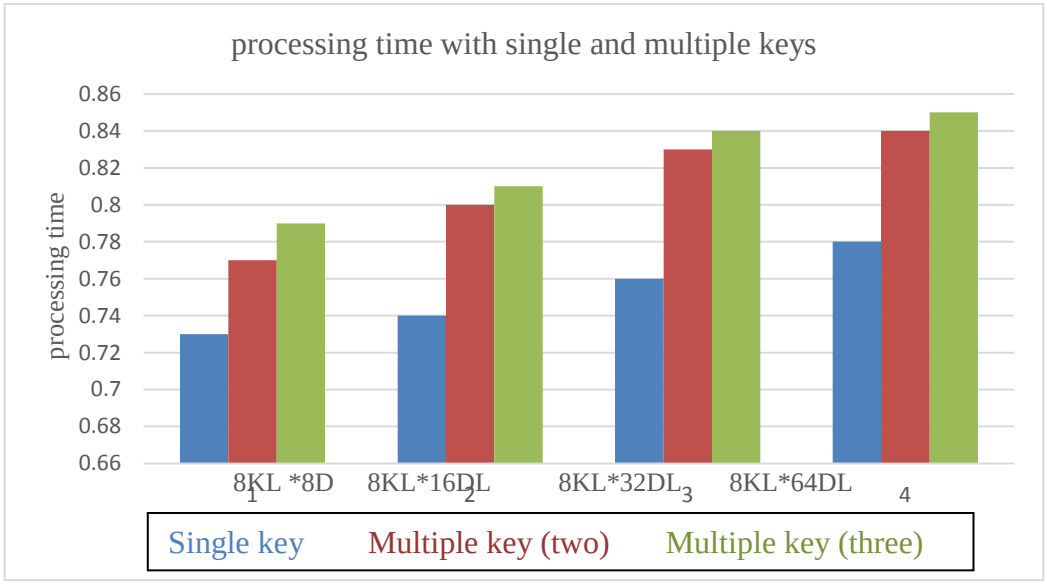


Figure 4.11 Processing time with 8 bit key length and different data lengths

In this 8 bit single key generation processing time is less. In the multiple (2) key generation processing time is increased than the single key but security level is also increased than the single key. In the three key generations processing time is more than both the cases but security level is also increased.

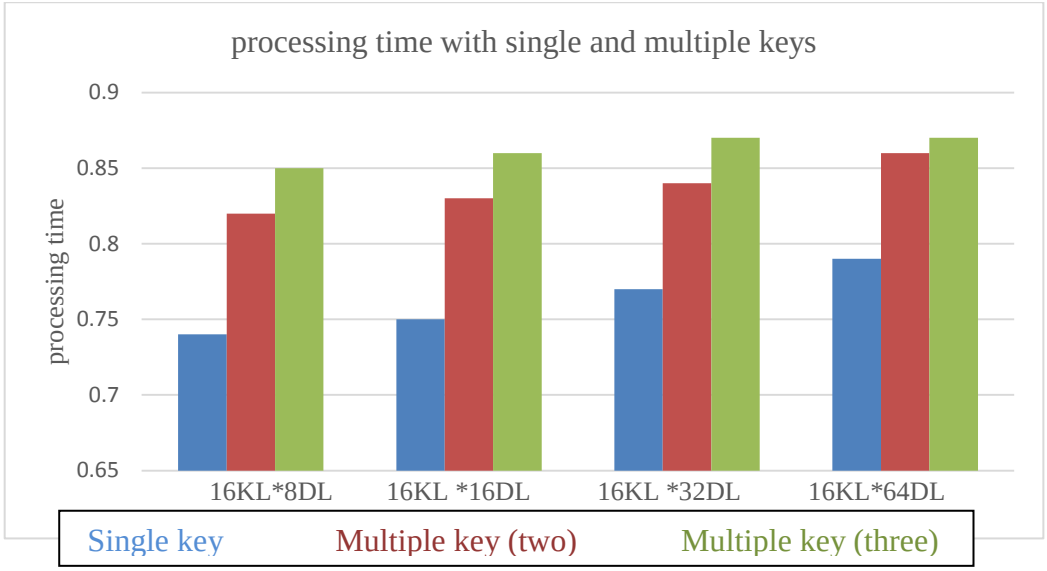


Figure 4.12 Processing time with 16 bit key length and different data lengths

It draws the relationship between processing time and keys (single, two and three). This is for the16 bit key length compared with 8, 16, 32, 64 bit data length. 16 bit key length is better

than the 8 bit key length. In the single key generation of all the cases processing time is less but when we are generating multiple keys of two and three than the processing time is increased but security in multiple key is better than the single key.

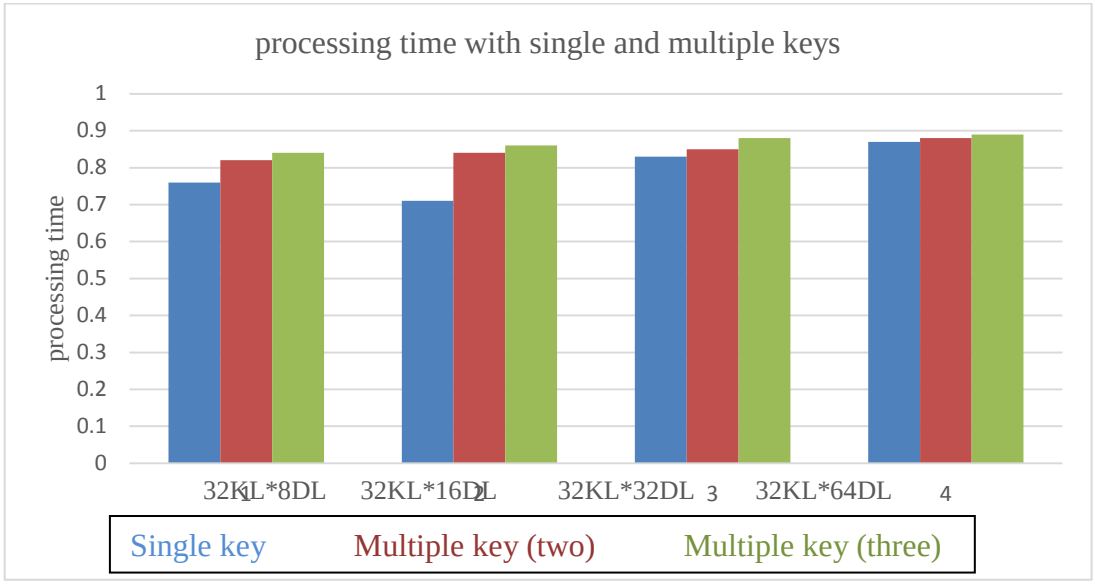


Figure 4.13 Processing time with 32 bit key length and different data lengths

Figure 4.13 draws the relationship between processing time and keys (single, two and three). This is for the 32 bit key length compared with 8, 16, 32, 64 bit data length. As we are increasing the key length processing time increased in the both cases but due to larger key size security level is also increased than the other cases.

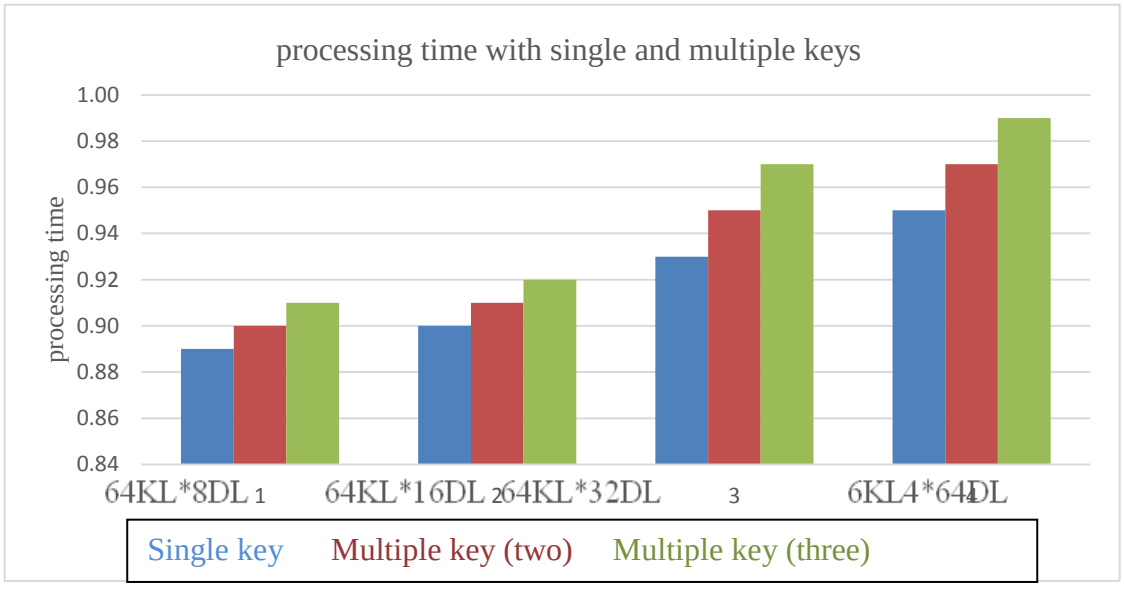


Figure 4.14 Processing time with 64 bit key length and different data length

Figure 4.14 shows the relationship between processing time and keys (single, two and three). This is for the 64bit key length compared with 8, 16, 32, 64 bit data length. 64 bit key length is the best key length for all the cases it gives the best security in single and multiple keys also. In multiple keys generation processing time increased but security level is best than all other cases.

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

Data security is important for many organizations. Our major concern in the key generation process is the fast processing with minimum time. In this work, we generate the single and multiple key from the available data, and also compare the single and multiple key generations. Also we have compared the processing time for single and multiple keys. After this we know that multiple keys are best for the security point of view, Multiples keys have the large processing time. In this we are evaluating the time for single and multiple (two and three) keys. We want to enhance the security with multiple keys in less time. It has been proved that the multiple keys are the best for the security purpose with comparison to single keys. In future work, we will work to reduce processing time of the multiple keys. It will provide the best security. Keys have been generated with logical and arithmetic operations.

.

REFERENCES

[1] Randall K. Nichols, Panos C. Lekkas (2002). Wireless Security Models, Threats, and Solutions, *McGraw-Hill Companies*, Edition 1.

[2] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone (1996). Handbook of Applied Cryptography, CRC Press, Edition 5.

[3] Bruce Schneier (1996). Applied Cryptography, *John Wiley and Sons*, Edition 2.

[4] William Stallings (2011). Cryptography and Network Security, Principles and Practice, *Pearson Prentice Hall, Pearson Education*, Edition 5.

[5] Data Encryption Standard (DES) (1999). *Federal Information Processing Standards Publication (FIPS)*, 46(3).

[6] Eslami Yadollah, Sheikholeslami Ali, P. Gulak Glenn, Masui Shoichi, and Mukaida Kenji (2006). An Area-Efficient Universal Cryptography Processor for Smart Cards, *IEEE Transactions on Very Large Scale Integration (VLSI)*, 14(1), 43-56.

[7] Harrison K. Willie, Almeida Joao, W. Steven McLaughlin and Barros Joao (2011). Coding for Cryptographic Security Enhancement Using Stopping Sets, *IEEE Transactions on Information Forensics and Security*, 6(3), 575-584.

[8] Bucci M, Giancane L, R. Luzzi, Marino M, Scotti G, Trifiletti A (2008). Enhancing Power analysis attacks against cryptographic devices, *The Institution of Engineering and Technology 2008 IET Circuits Devices System*, 2(3), 298-305.

[9] Khairnar A. G. and Bhale N. L. (1956). A Survey on Password Security Systems, *International Journal of Electronics and Computer Science Engineering*, 7(1), 546-548.

[10] Hu chih and Tzeng Wen-Guey (2007). Cheating Prevention in Visual Cryptography, *IEEE Transactions on Image Processing*, 16(1), 36-45.

[11] Ni Ming, McCalley James D, Vitta Vijay l, Tayyib Tayyib (2003). Online Risk Based Security Assessment, *IEEE Transactions on Power Systems*, 18(1), 258-265.

[12] Khiabani S. Yahya, Wei Shuangqing, Yuan Jian, and Wang Jian (2012). Enhancement of Secrecy of Block Ciphered Systems by Deliberate Noise, *IEEE Transactions on Information Forensics and Security*, 7(5), 1604-1613.

[13] Goel Satashu, Negi Rohit (2008). Guaranteeing Secrecy using Artificial Noise, *IEEE transactions on Wireless Communications*, 7 (6), 1536-1276.

[14] Vilela P. Joao, Bloch Matthieu, Barros Joao, and M. Steven McLaughlin (2011). Wireless Secrecy Regions with Friendly Jamming, *IEEE Transactions on Information Forensics and Security*, 6(2), 256-266.

[15] Khisti Ashish, Tchamkerten Aslan, and Wornell Gregory W. (2008). Secure Broadcasting Over Fading Channels, *IEEE Transactions on Information Theory*, 54 (6), 2453-2469.

[16] Hur Junbeom (2013). Improving Security and Efficiency in Attribute-Based Data Sharing, *IEEE Transactions on Knowledge and Data Engineering*, 25(10), 2271-2282.

[17] Pietro Roberto Di, Mancini Luigi V, Soriente Claudio, Angelo Spognardi, and Tsudik Gene (2009). Data Security in Unattended Wireless Sensor Networks, *IEEE Transactions on Computers*, 58 (11), 1500-1511.

[18] Conti Mauro, Pietro Roberto Di, Luigi V. Mancini (2007). ECCE: Enhanced Cooperative Channel Establishment for Secure pair-wise Communication in Wireless Sensor Networks, *Ad Hoc Networks*, 4(2), 49-62.

[19] Yeh Lo-Yao, Huang Yu-Lun, Joseph Anthony D, Shieh Shiuhpyng Winston, Senior, and Woei-Jiunn Tsaur (2012). A Batch-Authenticated and Key Agreement Framework for P2P-Based Online Social Networks, *IEEE Transactions on Vehicular Technology*, 61(4), 1907-1924.

[20] Lee Uichin, Jung Sewook, Cho Dae-Ki, Chang Alexander, Choi Junho, and Gerla Mario (2010). P2P Content Distribution to Mobile Bluetooth Users, *IEEE Transactions Vehicular Technology*, 59 (1), 356-367.

[21] Tseng Yuh-Min (2007). A secure authenticated group key agreement protocol for Resource-limited mobile devices, *Oxford University published* on July 21, 4(5), 41-52.

[22] Fan Chun-I and Lin Yi-Hui (2009). Provably Secure Remote Truly Three-Facto Authentication Scheme with Privacy Protection on Biometrics, *IEEE Transactions on Information Forensics and Security*, 4(4), 933-945.

[23] Gupta Gunjan and Chawla Rama (2012). Review on Encryption Ciphers of Cryptography in Network Security, *International Journal of Advanced Research in Computer Science and Software Engineering*, 2(7), 122-126.

[24] Breveglieri Luca, Koren Israel, and Maistri Paolo (2007). An Operation-Centered Approach to Fault Detection in Symmetric Cryptography Ciphers, *IEEE Transactions on Computers*, 56(5), 635-649.

[25] Gui Bo (2009). Routing Strategies in Multihop Cooperative Networks, *IEEE Transactions on Wireless Communications*, 8(2), 303-313.

[26] Papadimitratos Panagiotis, Haas Zygmunt j (2003). Secure Message Transmission in Mobile Ad hoc networks, *Ad hoc Networks*, 2(4), 193-209.

[27] Tafaroji M, and.Falahati A (2007). Improving code division multiple access security by applying encryption methods over the spreading codes, *The Institution of Engineering and Technology*, 3(4), 398-404.

[28] Bellovin Steven M and Merritt Michael (1992). Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks, *IEEE Symposium on Research in Security and Privacy, Oakland*, 61(2), 55-63.

[29] N.Nazumudeen , C.Mahendran (2014). Performance Analysis of Dynamic Routing Protocols Using Packet Tracer, *International Journal of Innovative Research in* Science, *Engineering and Technology*, 3(1), 6747-6757.

[30] Da-Chun Wu and Wen-Hsiang Tsa (1998). Data Hiding in Images via Multiple-Based Number Conversion and Lossy Compression, *IEEE Transactions on Consumer Electronics*, 44 (4), 1406-1412.

[31] Xiong Tao, Wei Lou, Zhang Jin, and Tan Hailun (2014). MIO: Enhancing Wireless Communications Security through Physical Layer Multiple Inter-symbol Obfuscation, *IEEE Transactions on Information Forensics and Security*, 4(3), 23-33.

[32] Zhou Zhi, Gonzalo R, and Crescenzo Giovanni Di (2006). Halftone Visual Cryptography, *IEEE Transactions on Image Processing*, 15(8), 2441-2453.

[33] Zhao Wentao and Wang Shaowei (2007). Resource Sharing Scheme for Device-to-Device Communication Underlying Cellular Networks, *IEEE Transactions on Communications*, 58(3), 4838-4848.

[34] Wang Huaqun, He Debiao, and Tang Shaohua (2016). Identity-Based Proxy Oriented Data Uploading and Remote Data Integrity Checking in Public Cloud *IEEE Transactions on Information Forensics and Security*, 11(6), 1165-1176.

[35] Shahzad Malik Kaleem Awan, Pete Burnap, Rana Omer (2016). Identifying cyber risk hotspots: A framework for measuring temporal variance in computer network risk, *Journal Computers & Security*, 4(7), 31-46.

[36] Fu Yulong, Kone Ousmane (2015). Model based security verification of protocol Implementation, *Journal of Information Security and Applications*, 12(14), 17-27.

[37] Rahbarini Babak, Perdisci Roberto, Lanzi Andrea, Li Kang (2014). Peer Rush: Mining for unwanted P2P traffic, *Journal of Information Security and Applications*, 54(4), 194-208.

[38] Chan Haowen, Perrig Adrian, Dawn Song (2003). Random Key Predistribution Schemes for Sensor Networks, *Department of Electrical and Computer Engineering, Carnegie Institute of Technology*, 54(4), 89-95.

[39] Park Min-Ho, Park Young-Hoon, Jeong Han-You, and Seo Seung-Woo y (2013). KeManagement for Multiple Multicast Groups in Wireless Networks, *IEEE Transactions on Mobile Computing*, 12 (9), 1712-1723.

[40] Li Jinguo, Wen Mi, and Zhang Tao (2016). Group-Based Authentication and Key Agreement with Dynamic Policy Updating for MTC in LTE-A Networks, *IEEE Internet of Things Journal*, 3(3), 408-417.

[41] Harrison Willie K., Almeida Joao, Steven W. McLaughlin, and Barros Joao (2011). Coding for Cryptographic Security Enhancement Using Stopping Sets, *IEEE Transactions on Information Forensics and Security*, 6(3), 575-584.

[42] Maurer Ueli and Wolf Stefan (2003). Secret-Key Agreement over Unauthenticated Public Channels-Part III: Privacy Amplification, *IEEE Transactions on Information Theory*, 49(4), 839-851.

[43] Bucci M, L. Giancane, R. Luzzi, M. Marino, G. Scotti, A. Trifiletti (2008). Enhancing power analysis attacks against cryptographic devices, *The Institution of Engineering and Technology 2008 IET Circuits Devices System*, 2(3), 298-305.

[44] Liu Shuiyin, Yi Hong, and Viterbo Emanuele (2014). Unshared Secret Key Cryptography, *IEEE Transactions on Wireless Communications*, 13(12), 6670-6683.

[45] Markelj Blaz, Bernik Igor (2015). Safe use of mobile devices arises from knowing the threats, *Journal of Information Security and Applications*, 4(7), 84-89.

[46] Alsmadi Izzat, Xu Dianxiang (2015). Security of Software Defined Networks: A survey, *Journal computers & security* 53(3), 79-108.

[47] Page Daniel and Vercauteren Frederik (2006). A Fault Attack on Pairing-Based Cryptography, *IEEE Transactions on Computers*, 55 (9), 1075-1080.

[48] Atay Serap, Masera Marcelo (2011). Challenges for the security analysis of Next Generation Networks, *Information Security Technical Report,* 16(3), 3-11.

[49] Verma S, Choubey and Soni R (2012). An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security, *International Journal of Emerging Technology and Advanced Engineering*, 2(7), 18-21.

[50] Halkidis Spyros T, Chatzigeorgiou Alexander and Stephanides George (2007). A Practical Evaluation of Security Patterns, *Applied Informatics University of Macedonia,* 56(5), 34-42.

[51] O'Melia Sean, and Adam J. Elbirt (2010). Enhancing the Performance of Symmetric-Key Cryptography via Instruction Set Extensions, *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 18(11), 1505-1518.

[52] Zhou Zhibin, Huang Dijiang, and Wang Zhijie (2006). Efficient Privacy-Preserving Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption, *IEEE Transactions on Computers*, 12(7), 22-31.

[53] Wong Chung Kei, Gouda Mohamed, and Lam Simon S (2000). Secure Group Communications Using Key Graphs, *IEEE/ACM Transactions on Networking*, 8(1), 16-30.

[54] Kermani Mehran Mozaffari, and Masoleh Arash Reyhani (2010). Concurrent Structure-Independent Fault Detection Schemes for the Advanced Encryption Standard, *IEEE Transactions on Computers,* 59(5), 608-622.

[55] Burns F, Murphy J, Koelmans A, Yakovlev A (2008). Efficient advanced encryption standard Implementation using lookup and normal basis, *Published in IET Computers & Digital Techniques,* 55(3), 270-280.

[56] Olteanu Alina, Xiao Yang, and Zhang Yan (2009). Optimization between AES Security and Performance for IEEE 802.15.3 WPAN, *IEEE Transactions on Wireless Communications*, 8912), 1536-1546.

[57] Prodhan Uzzal , A.H.M. Parvez Shahariar, Md. Ibrahim Hussain, Yeasir Fathah Rumi, Md. Ali Hossain (2012). Performance Analysis of Parallel Implementation of Advanced Encryption Standard (AES) over serial Implementation, International *Journal of Information Sciences and Techniques (IJIST)*, 2(6), 45-52.

[58] Wang Mao-Yin, Su Chih-Pin, Horng Chia-Lung, Wu Cheng-Wen, and Huang Chih-Tsun (2010). Single and Multi-core Configurable AES Architectures for Flexible Security, *IEEE Transactions on Very Large scale Integration (VLSI) Systems*, 18(4), 541-552.

[59] Baek Chung Hun, Cheon Jung Hee, and Hong Hyunsook (2016). White-Box AES Implementation Revisited, *Journal of Communications and Networks*, 18(3), 273-287.

[60] Shang D, Burns F, A. Bystrov, A. Koelmans, D. Sokolov and A. Yakovlev (2006). High-security asynchronous circuit implementation of AES, *IEE Proceeding Computer Digital Technical*, 153(2), 71-77.

[61] Wang Mao-Yin, Su Chih-Pin, Chia-Lung Horng, Cheng-Wen, and Chih-Tsun Huang (2010). Single- and Multi-core Configurable AES Architectures for Flexible Security, *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 18(4), 541-552.

[62] Bouillaguet Charles, Nathan Keller, and Rijmen Vincent (2012). Low-Data Complexity Attacks on AES, *IEEE Transactions on Information Theory*, 58(11), 7002-7017.

[63] Zhang Xinmiao and Parhi Keshab K. (2006). On the Optimum Constructions of Composite Field for the AES Algorithm, *IEEE Transactions on Circuits and Systems—ii: express briefs*, 53(10), 1153-1157.

[64] Yen Chih-Hsu and Wu Bing-Fei (2006). Simple Error Detection Methods for Hardware Implementation of Advanced Encryption Standard, *IEEE Transactions on Computers*, 55(6), 720-731.

[65] Du W, Deng J, Y. S. Han, P. K. Varshney, J. Katz, and Khalili A (2005). A Pair wise Key Pre-Distribution Scheme for Wireless Sensor Networks, *ACM Transactions on Information and System Security*, 8(2), 228-258.

[66] Hsiao S.F., M.C. Chen, M. Y. Tsai and C.C. (2005). System-on-chip implementation of the whole advanced encryption standard processor using reduced XOR-based sum-of-product operations, *IEE Proceedings online*, 11(3), 21-30.

[67] Bertoni Guido, Breveglieri Luca, and Vincenzo Piuri (2003). Error Analysis and Detection Procedures for a Hardware Implementation of the Advanced Encryption Standard, *IEEE Transactions on Computers,* 52(4), 492-505.

[68] Bouillaguet Charles, Nathan Keller and Rijmen Vincent (2012). Low-Data Complexity Attacks on AES, *IEEE Transactions on Information Theory,* 58(11), 7002- 7017.

[69] Wallace Jon (2005). Secure Physical Layer Key Generation Schemes: Performance and Information Theoretic Limits, *School of Engineering and Science, Jacobs University Bremen Campus Ring 1, 28759 Bremen, Germany*, 67(2), 212-223.

[70] Paulo F. Oliveira and Joao Barros (2008). A Network Coding Approach to Secret Key Distribution, *IEEE Transactions on Information Forensics and Security*, 3(3), 414-423.

[71] Heng Zhou, Lauren M. Huie and Lifeng Lai (2014). Secret Key Generation in the Two-Way Relay Channel with Active Attackers, *IEEE Transactions on Information Forensics and Security*, 9(3), 476-488.

[72] Chen Dajiang, Qin Zhen, Xufei Mao, Panlong Yang, Zhiguang Qin and Wang Ruijin (2013). Smoke Grenade: An Efficient Key Generation Protocol with Artificial Interference, *IEEE Transactions on Information Forensics and Security*, 8(11), 720-731.

[73] Wang Qian, Su Hai (2011). Fast and Scalable Secret Key Generation Exploiting Channel Phase Randomness in Wireless Networks, *IEEE Infocom*, 12(3), 11-20.

[74] Lai Lifeng, Huie Lauren (2013). Simultaneously Generating Multiple Keys in Many to one Network, *IEEE International Symposium on Information Theory*, 22(2), 24-31.

[75] Lai Lifeng and Ho Siu-Wai (2012). Simultaneously Generating Multiple Keys and Multi-Commodity Flow in Networks, *IEEE Information Theory Workshop*, 5(2), 34-42.

[76] Zhang Huishuai, Lai Lifeng, Yingbin Liang, and Wang Hua (2014). The Capacity Region of the Source-Type Model for Secret Key and Private Key Generation, *IEEE Transactions on Information Theory,* 60(10), 6389 - 6398.

[77] Tavangaran Nima, Boche Holger, and Schaefer Rafael F (2009). Secret-Key Generation Using Compound Sources and One-Way Public Communication, *IEEE Transactions on Information Forensics and Security*, 57(4), 227- 241.

[78] Xu Peng, Kanapathippillai Cumanan, Zhiguo Ding and Xuchu Dai and Kin K. Leung (2003). Group Secret Key Generation in Wireless Networks: Algorithms and Rate Optimization, *IEEE Transactions on Information Forensics and Security*, 52(4), 1831-1846.

[79] Portmann Christopher (2014). Key Recycling in Authentication, *IEEE Transactions on Information Theory*, 60(7), 4383- 4396.

[80] Ye Chunxuan and Reznik Alex (2007). Group Secret Key Generation Algorithms, *Inter Digital Communications Corporation King of Prussia*, 19(4), 21-29.

[81] Nitinawarat Sirin, Ye Chunxuan, Barg Alexander, Narayan Prakash, and Reznik Alex (2010). Secret Key Generation for a Pair wise Independent Network Model, *IEEE Transactions on Information Theory*, 56(12), 14-22.

[82] Gharout Saıd, Bouabdallah Abdelmadjid, Yacine Challal, Achemlal Mohammed (2012). Adaptive Group Key Management Protocol for Wireless Communications, *Journal of Universal Computer Science*, 18(6), 874-888.

[83] Li Fagen, Di Zhong, and Takagi Tsuyoshi (2016). Efficient Deniably Authenticated Encryption and Its Application to E-Mail, *IEEE Transactions on Information Forensics and Security*, 11(11), 2477- 2486.

[84] Seo Seung-Hyun, Jongho Won, Salmin Sultana, and Elisa Bertino (2015). Effective Key Management in Dynamic Wireless Sensor Networks, *IEEE Transactions on Information Forensics and Security*, 10(2), 371-383.

[85] Kakkar Ajay, Singh M.L. and P.K. (2012). Mathematical analysis and simulation of multiple keys and S-Boxes in a multi-node network for secure transmission, *International Journal of Computer Mathematic*s, 89(16), 2123-2142.

[86] Sofia Anna Menesidou, Dimitrios Vardalis, Vasilios Katos (2016). Automated key exchange protocol evaluation in delay tolerant networks, *Journal Homepage Computers & Security*, 59(3), 1-8.

[87] Koyluoglu O. Ozan and El Gamal, Hesham (2012). Polar Coding for Secure Transmission and Key Agreement, *IEEE Transactions on Information Forensics and Security*, 7(5), 1472-1483.

[88] Tsai Jia-Lun, Lo Nai-Wei, and Wu Tzong-Chen (2013). Novel Anonymous Authentication Scheme Using Smart Cards, *IEEE Transactions on Industrial Informatics*, 9(4), 2004-2013.

[89] Cheng Chi and Jiang Tao (2013). An Efficient Homomorphic MAC with Small Key Size for Authentication in Network Coding, *IEEE Transactions on Computers*, vol. 62(10), 2096-2100.

[90] Nicanfar Hasen, Jokar Paria, Beznosov Konstantin, and Victor C. M. Leung (2014). Efficient Authentication and Key Management Mechanisms for Smart Grid Communications, *IEEE Systems Journal*, 8(2), 629-640.

[91] Saxena Neetesh, and Chaudhari Narendra S (2014). EasySMS: A Protocol for End-to-End Secure Transmission of SMS, *IEEE Transactions on Information Forensics and Security*, 9(7), 1157-1168.

[92] Rao Nagamalleswara. Dasari and Sreenivasarao Vuda (2010). Performance of Multi Server Authentication and Key Agreement with User Protection in Network security, *International Journal on Computer Science and Engineering*, 2(5), 1705-1712.

[93] Yang Hung-Wen, Yang Chou-Chen, Lin Woei (2012). Enhanced digital rights management authentication scheme based on smart card, *published in IET Information Security*, 12(7), 189-194.

[94] Sayed Bassam, Issa Traor´e, Isaac Woungang, and Obaidat Mohammad S (2013). Biometric Authentication Using Mouse Gesture Dynamics, *IEEE Systems Journal*, 7(2), 262-274.

[95] S Sangeeth Kumar and Venkatesan R (2014). Ranking of Authentication Schemes based on Critical Limiting Factors, *International Journal of Computer Applications*, and 92(7), 8875-8887.

[96] Fouda Mostafa M and Fadlullah Zubair (2011). A Lightweight Message Authentication Scheme for Smart Grid Communications, *IEEE Transactions on Smart Grid*, 2(4), 675-685.

[97] Kakkar Ajay, M. L. Singh, Bansal P. K. (2012). Secure Communication by using multiple keys having variable length in a real time environment for multiple stations, *Journal of Engineering Science and Technology*, 7(4), 505-516.

[98] Yang Guomin, Wonga Duncan S, Wangb Huaxiong, Deng Xiaotie (2008). Two-factor mutual authentication based on smart cards and passwords, *Journal of Computer and System Sciences*, 87(12), 1160-1172.

LIST OF PUBLICATIONS

- Kaur Lovpreet and Kakkar A (2017). Data security in wireless communication using multiple keys, *International Journal of Computer Application* (communicated)

- Kaur H, Kaur L and Kaur T (2017). Triple security of data using encryption keys and image steganography, *International Journal of Computer Application*(published)

Lovepreet_14.7.17

ORIGINALITY REPORT

%18	%10	%7	%10
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Thapar University, Patiala Student Paper	%1
2	jestec.taylors.edu.my Internet Source	%1
3	data.conferenceworld.in Internet Source	%1
4	www.julieryan.com Internet Source	%1
5	dspace.thapar.edu:8080 Internet Source	%1
6	www.sgi.ac.in Internet Source	%1
7	www.it.pt Internet Source	<%1
8	Submitted to Sreenidhi International School Student Paper	<%1
9	www.ijcaonline.org Internet Source	<%1