CAPITAL UNIVERSITY OF SCIENCE AND
TECHNOLOGY, ISLAMABAD

A Multilayer Encryption Model To Protect Healthcare Data in Cloud Environment

by

Hasan Abbas Shah

A thesis submitted in partial fulfillment for the
degree of Master of Science

in the

Faculty of Computing
Department of Computer Science

2020

This thesis work is devoted to my beloved Teachers, Family and Friends. I have a special feeling of gratitude for my beloved parents, brothers, sisters and wife. I would like to thank my supervisor for his firm belief and confidence that enabled me to reach this milestone.

CERTIFICATE OF APPROVAL

A Multilayer Encryption Model to Protect Healthcare Data in Cloud Environment

by

Hasan Abbas Shah

(MCS173006)

THESIS EXAMINING COMMITTEE

S. No.	Examiner	Name	Organization
(a)	External Examiner	Dr. Munir Ahmad	BIIT Rawalpindi
(b)	Internal Examiner	Dr. Amir Qayyum	CUST Islamabad
(c)	Supervisor	Dr. Qamar Mahmood	CUST Islamabad

Dr. Qamar Mahmood
Thesis Supervisor
May, 2020

Dr. Nayyer Masood
Head
Dept. of Computer Science
May, 2020

Dr. Muhammad Abdul Qadir
Dean
Faculty of Computing
May, 2020

Author's Declaration

I, **Hasan Abbas Shah** hereby state that my MS thesis titled "**A Multilayer Encryption Model to Protect Healthcare Data in Cloud Environment**" is my own work and has not been submitted previously by me to obtain for taking any degree from Capital University of Science and Technology, Islamabad or anywhere else in the country/abroad.

If at any time at any time if my statement is found to be incorrect even after my graduation, the University has the right to withdraw my MS Degree.

(Hasan Abbas Shah)
Registration No: MCS173006

Plagiarism Undertaking

I solemnly declare that research work presented in this thesis titled "**A Multilayer Encryption Model to Protect Healthcare Data in Cloud Environment**" is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been dully acknowledged and that complete thesis has been written by me.

I understand the zero tolerance policy of the HEC and Capital University of Science and Technology towards plagiarism. Therefore, as an author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of MS Degree, the University reserves the right to withdraw/revoke my MS degree and that HEC and the University have the right to publish my name on the HEC/University website on which names of students are placed who submitted plagiarized work.

(Hasan Abbas Shah)
Registration No: MCS173006

Acknowledgements

In the name of Allah, the Most Merciful Alhamdulillah, all praises to the Owner of the universe for the strengths and the blessings bestowed upon me to help me complete this thesis. This study is nothing, but an effort to understand and articulate the principles of one of the several hundred thousand phenomena, with a tool called ,the brain,the most precious gift from the Almighty.

I would like to express my sincerest appreciation to my enthusiastic supervisor, **Dr. Qamar Mahmood** for his supervision, assistance, and immense knowledge. I am sincerely thankful to him for his constant support, motivation, and patience. His invaluable help of constructive comments and suggestions throughout the thesis work have contributed to the success of this research. It has been an amazing experience and I thank him wholeheartedly, not only for his tremendous support.

My deepest gratitude goes to my beloved parents, Wife and my children for tolerating my mood swings and bearing with me. I would also like to thank my friends and family for encouraging me and motivating me for completion of this research work.

(Hasan Abbas Shah)
Registration No: MCS173006

Abstract

This is the era of cloud computing and it has become an integral part for any organization. It is equally suitable for all the organizations e.g. education, government, public sector, health care department. Main features of cloud computing are broad network, shared resources, rapid elasticity and pay per use. Cloud computing is also providing highly potential services to IT based healthcare sector. In cloud computing model a patient can get consultancy from any doctor available in the world. There are two types of patient information i.e. protected/sensitive health information and general information. Protected information (Phone no, ATM, Security no, MR no etc.) requires more confidentiality as compared to general information. Therefore, for some protected health information without patient association (general disease name, symptoms) will be very helpful for research experiments. Health information is protected by achieving confidentiality, integrity and availability, when data is stored in cloud environment.

There can be many types of attacks possible on protected health information stored on cloud e.g. if patient credit card information is hacked by a hacker than he may lose his all money. Similarly, if the disease information of a celebrity is leaked out than he/she may lose the career. Thats why protected/sensitive information requires protection in cloud environment. Cryptography methods provide different techniques to protect the data stored in cloud environment. In this thesis, we have suggested a multilayer encryption technique to ensure the confidentiality of data stored in cloud environment. This suggested technique will improve the security of cryptographic techniques when used in multilayered format. We have set up a local system for the experiment. We have used the RDBMS (Microsoft SQL Server) and Framework 4.5. A set of 500 dummy patient records is used to test the proposed techniques. The experiment was performed to check the confidentiality of the suggested techniques. This experiment shows us that multilayer encryption techniques is more suitable for public health sectors when data is in cloud environment.

Contents

List of Figures

List of Tables

Abbreviations

ABE	Attribute Based Encryption
AES	Advance Encryption Standard
DES	Data Encryption Standard
EGC	Elliptic Galois Cryptography
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
IFHDS	Intelligent Framework for Healthcare Data Security
LSB	Least Significant Bit
MSD	Mass storage Device
MR No	Medical Record No
PCEHR	Personal Control Electronic Health Record
PHI	Protected Health Information
RDBMS	Relational Database Management System
RSA	Rivest, Shamir, and Adelman
SHA	Secure Hash Algorithm
SNAP	Subnetwork Access Protocol
Three DES	Triple Data Encryption Standard

Chapter 1

Introduction

Cloud based environment is progressing day by day and a lot of organizations are shifting towards cloud environment. Similarly, IT based health care sector is also moving towards cloud environment because of its advantages e.g. available at anywhere, anytime and measured resources. Patient data is stored in electronic format in cloud. It can be accessible on Internet for further consultations and treatment [1]. A patient can get consultation from any doctor who is available on Internet and is from any part of the world. Digital data is providing a platform to doctors who can monitor their patients. So with the invention of Internet and cloud computing, quality of IT based health care sector services are also improving day by day. But there are a number of attacks e.g. protected/sensitive data theft, DoS, DDoS etc. exists in cloud computing environment. Thats why confidentiality and privacy of patient data has more concerned in cloud environment because of it is publically available. If patient confidential information is breach out then a patient may suffer many difficulties e.g. if a celebrity personal email id is hacked then he may loss his reputation etc. Similarly, if a credit card information or account information is leaked out then patient may loss all his money.These are the reasons which needs enhancement in security and protection of data [2] and that's why HIPAA and GDPR are playing there role for the protection of PHI attributes. We will discuss some benefits of cloud environment and then take a glimpse on the role of cryptography on healthcare data.

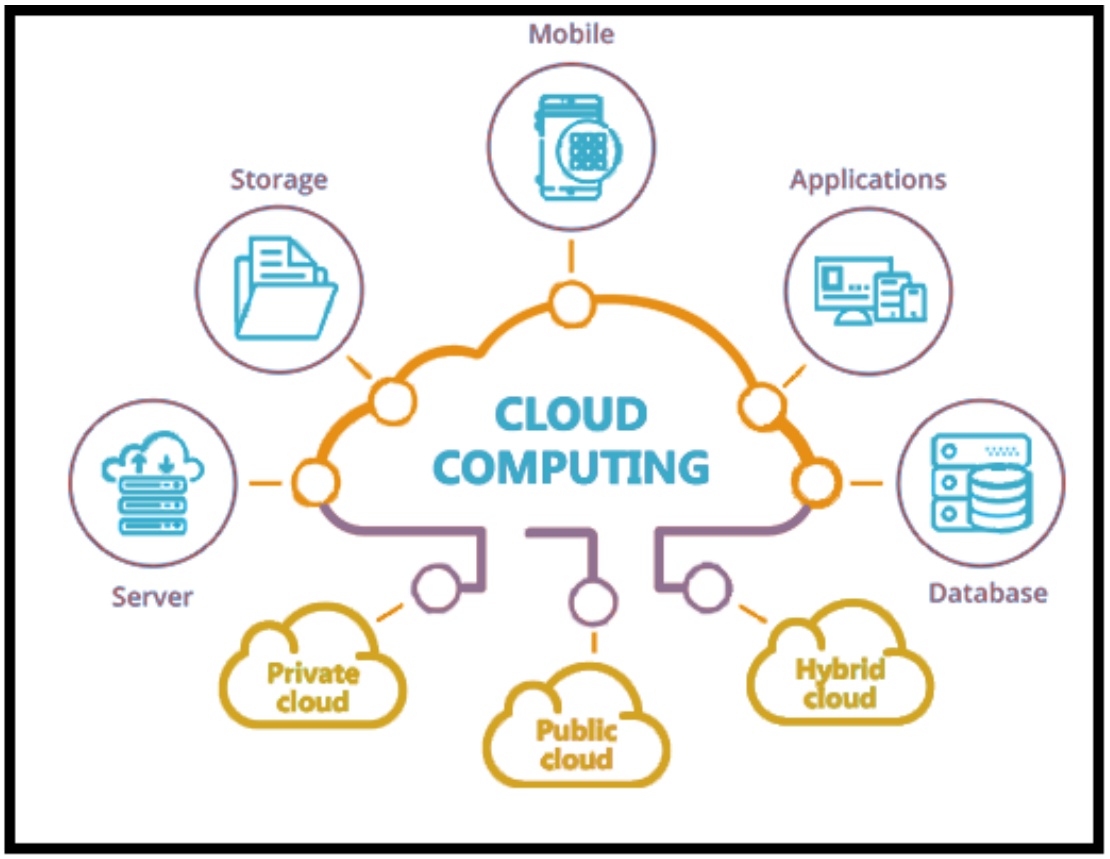

FIGURE 1.1: Cloud Computing[1]

1.1 Cloud Computing

Cloud computing [3] is an on demand computing services See Figure 1.1. It means computational resources are available on demand and as much as required. Now a days cloud computing is the biggest source of computing services especially in healthcare sector. It allows the e-health sector to store and access the data at remote locations with minimum management effort. General term for cloud computing is Data Centers are available on Internet which are providing different type of services on Internet. Hospitals do not need to maintain their own data centers. They just need to acquire the server or machine according to their demand and pay to data centers / providers according to usage. Cloud computing basic purpose is sharing of resources with ease and proper utilization of it.

[1] https://medium.com/@outrightsystems/cloud-computing-in-business-ab19f308221d

1.2 A Little History of Cloud Computing

In early 1960s client server architecture was used only for mainframe and it clients. At that time data storage was very expensive. Cost of CPU was also very high. Due to these reasons mainframe were used for storage and processing. Client/ Dump terminals were used to connect with these for data accessing and processing

- In 2006 Amazon launched it sub branch named Amazon web services and introduced
- Google released the testing version of Google App Engine in April 2008. In same year NASA also introduced the OpenNebula. This was the first open source project which was deployed for private an hybrid cloud
- In 2010 Microsoft Azure was realesed by Microsoft
- In 2012, Google Compute Engine was released in preview, before being rolled out into General Availability in December 2013

1.3 Cloud Computing Features for Health Care Sector

Cloud computing services are useful for health care sector due to following features

- Clouds computing services remain available by 24 X 7 and patient data can be access from any location wherever Internet service is available.
- Payment is according to requirement of storage and usage of patient data.
- No maintenance cost, extra payment and management cost is required e.g. Network Admin, Room, Electricity to e-Health Sector.
- Resource sharing means one server may be shared between multiple health organizations. Through this way resources utilization will be achieved maximum.

- Performance of servers will be measured by technically sound personnel.

NIST [4] defines the five benefits of cloud computing

- On demand and Self Service the service is available at demand
- Rapid elasticity means hardware and software requirements can be upgrade without too much effort
- Broad network Access capabilities are available on Internet and accessibilities methods are standards
- Resource Pooling means resources are shared
- Measure Services pay as you utilize like Internet usage or rent a car service..

1.4 Services Model of Cloud for E-Healthcare Sector

Cloud computing has become the vital sign for IT technology because of its infrastructure, speed and flexible budget. With self-service features any users can use scalable features and upgrade the usage depending upon the requirement. This technology offers some particular types of services mentioned below which a user can gain from cloud platform [5].

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Now for just for sake of basic knowledge we take a little review on these services which are allowed in cloud environment.

1.4.1 Software as a Service (SaaS)

Any healthcare service provider can use the built in application of hospital management system by using this resource from cloud service provider with very less management efforts.

1.4.2 Platform as a Service (PaaS)

PaaS is for those health sector who wants to develop their own customize software applications.

1.4.3 Infrastructure as a Service (IaaS)

As name implies any health organization can purchase the full hardware and keeps his software and data at cloud.

Challenges for healthcare data at cloud environment:

- A patient data is stored in digital format in RDBMS. If proper role is not assigned to different entities to access patient data then it may be modified or altered. Result is that confidentiality and integrity of data is lost.
- Data is located at outside the promise.
- Hardware is shared between different parties and party is an attacker the data may be compromised.

1.5 Overview of Cryptography

Generally term cryptography [6] refers to study of secrets and in todays world it is connected with encryption. Encryption is a process which converts plain text to hidden text / coded text. This makes plain text more secure. So when a patient

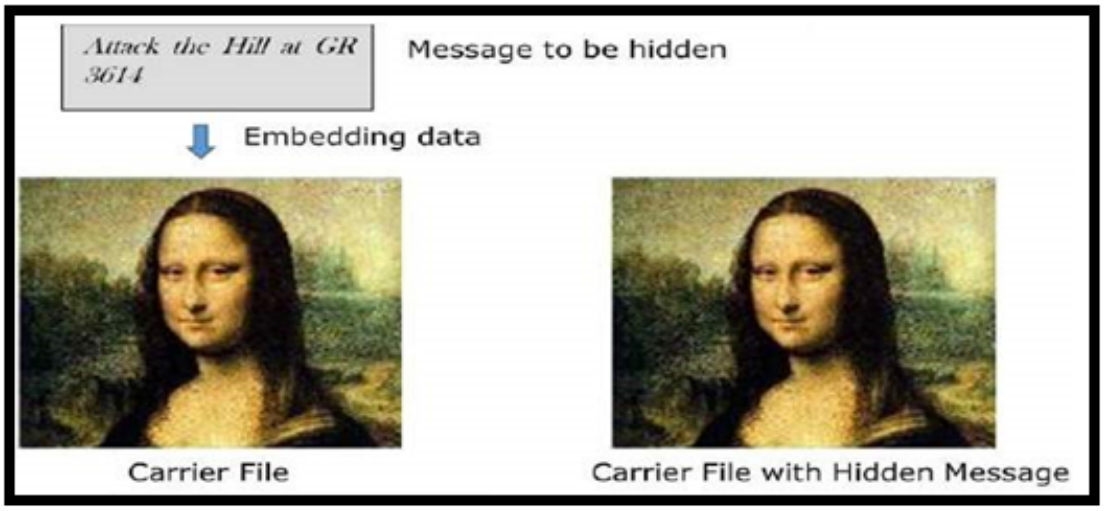

FIGURE 1.2: Steganography Encryption[2]

data is stored at cloud it needs protection. Cryptography techniques will improve the confidentiality and integrity level of the patient. Generally cryptography uses mathematical modeling [7] techniques. This techniques is implied on data to encrypt and decrypt by using some keys.

1.5.1 A Few Words About The History of Cryptography

It is closely connected with birth of writing. Some 4000 years ago Egyptians started there the communication in hidden words which is named hieroglyph. This language was only known to the scribers who transmits the message on behalf of the Kings. In between 500 and 600 BC the researchers started the simple substitution ciphers techniques. Romans introduced a new techniques known as Caesar cipher. In this method characters of words would be replaced with some other words and at second location again these character reserved which would become original message.

Steganography It is another form of cryptography. In this form of cryptography, information not only become protected See Figure 1.2 but it would brought more confidentially the no unauthorized person could get a clue of information e.g invisible watermarking. In steganography, an intruder or unintended recipient do not know that information which is in front of him contains hidden information.

1.5.2 Revolution in The Field of Cryptography

In 15th BC the European, Italian and papal state brought further enhancement in cryptography. Different techniques of cryptanalysis and attacks had become under consideration in this era.

- Vigenere coding techniques is introduced in this era
- But in 19th century cryptography has changed from ad hoc approaches to more modern art techniques.
- In 20th century Enigma rotor machine was introduced.
- But after the Second World War modern cryptography techniques has been introduced and now it is an oxygen for the computer sciences fields.

A little comparison between classical and modern cryptography is shown in Table 1.1

TABLE 1.1: Comparison between Classical and Modern Cryptography

Classical	Modern
It works with on alphabets and digits	It works with binary oriented data
In classical techniques only sender and receiver can communicate who knew to each other	In modern techniques algorithms are known publically but secrete key protects the data.
In classical, for secure communication entire cryptosystem is required	But in modern techniques only secret key is required not whole cryptosystem

In the above table we have compared some basic features of classical and modern cryptographic techniques. This shows that a place for the enhancements in existing techniques as well as research of new ones remains always present.

[2]https://www.tutorialspoint.com/cryptography/cryptosystems.htm

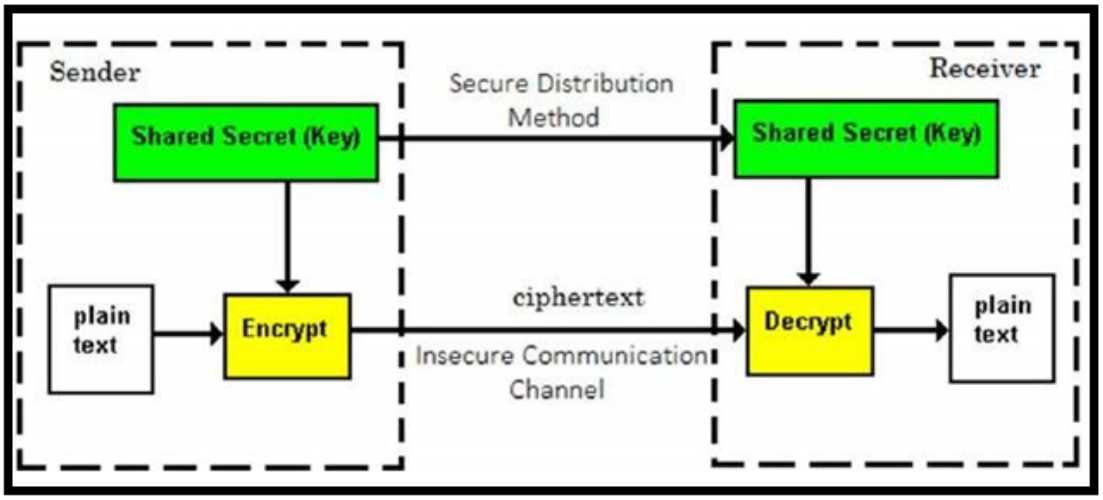

FIGURE 1.3: Symmetric Key Encryption [3]

1.5.3 Types of Cryptography Schemes

Following two general types of encryption is used in cipher systems [6]:

- Symmetric Encryption
- Asymmetric Encryption

1.5.3.1 Symmetric Key Encryption

In this type of encryption only one or single key is see Figure 1.3 used for both encryption and decryption. Famous symmetric encryption algorithms are Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.

It has following features

- Length of the key makes its encryption and decryption process faster or slower
- Less Computer processing consumption is used.
- A fast communication mechanism between two parties for secure communication.

[3] https://www.tutorialspoint.com/cryptography/cryptosystems.htm

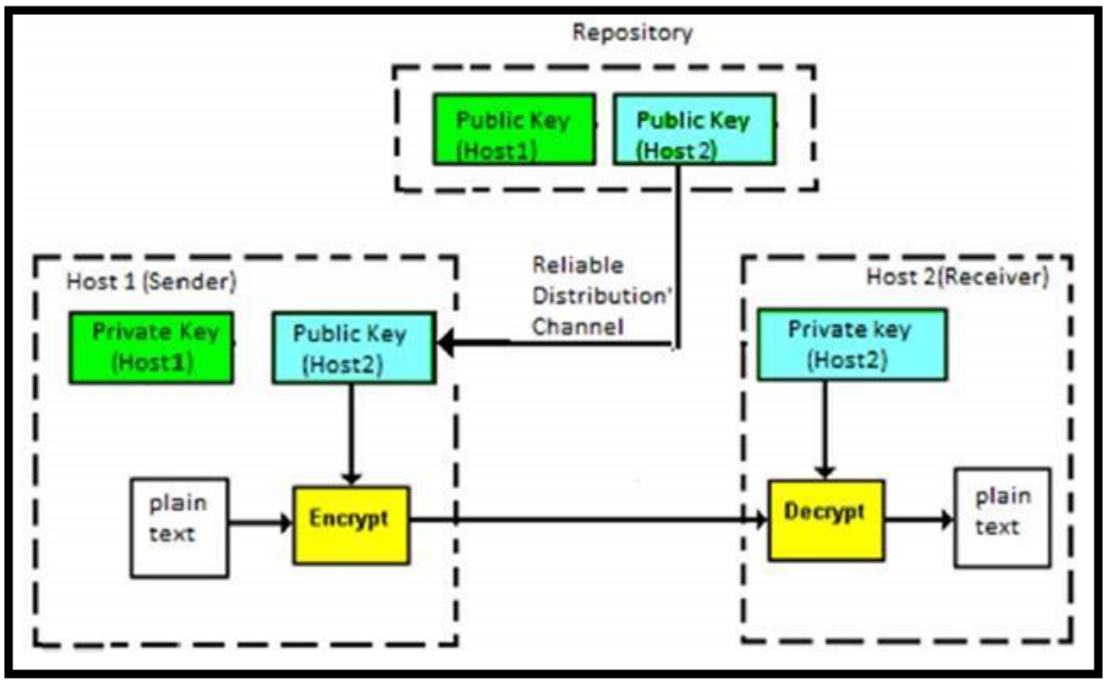

FIGURE 1.4: Asymmetric Key Encryption [4]

- Keys can be changes periodically or on requirement basis
- Single key can be shared before communication started between the parties

1.5.3.2 Asymmetric Key Encryption

It is also known as public key cryptography. It implies two keys for encryption and decryption See Figure 1.4. Any message or data can be encrypted by using public key which is known to everybody publically. But decryption process requires the private key. This key has only the receiver who only wants to decrypt it. Asymmetric encryption has following features

- Two key private and public are used for encryption and decryption
- Pubic key is on Internet and anybody who wants to encrypt data for that particular person can get it. This key is mathematically linked with private key and only the authorized person can decrypt it.

[4] https://www.tutorialspoint.com/cryptography/cryptosystems.htm

- When Person A needs to send data to Person B, he obtains the public key of Person B from repository, encrypts the data, and transmits.
- Person B uses his private key to extract the plaintext.
- Length of Keys is large and hence, the process of encryption-decryption is slower
- Processing power is required higher to run asymmetric algorithm.

1.5.4 Security Service gained from Cryptography for Healthcare

These below feature can be gained from cryptography regarding patient data[9].

1.5.4.1 Confidentiality

Confidentiality is the most fundamental and basic security services which is required from cryptography. It keeps the patient medical information hidden from an unauthorized access. It is also known as secrecy and privacy. It ensures that on one can reads the message except the original users. Different mathematical algorithms are used for data encryption. By using these algorithms level of confidentiality can be achieved.

1.5.4.2 Integrity

It deals with the modification of data. The service authenticates that patient data is not modified by any unauthorized person either by consciously or unconsciously. It also ensures the data is unaltered after its creation. Integrity cannot stop modification in information. It just provides an evidence for detection whether the information is tampered or not. Both these points of security play very important role in security specially when the data in cloud environment because more protection is require at cloud.

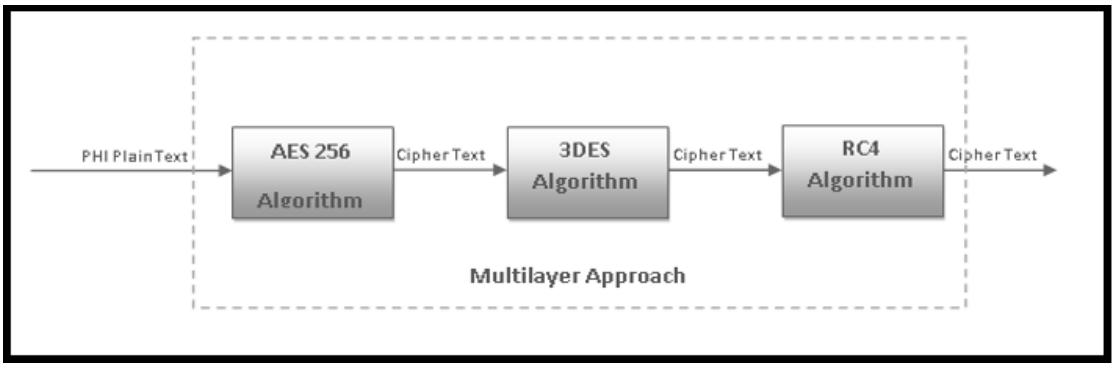

FIGURE 1.5: Multilayer Encryption Technique

1.5.4.3 Authenticity

Authenticity provides that information is from sender. It assures to the receiver that the received information is from the actual users. It has further two variants:

Entity Authentication: it provides the assurance that message or information has been received from a specific entity.

Message Authentication: it provide the information about the originator of the message without describing the rout or system which has send this information

1.5.4.4 Multilayer Encryption

In multilayer encryption See Figure 1.5 we will pass the plaintext to one algorithm with a key and output of that algorithm will be passed to second algorithm with some different key. Such layers can be consist two or more algorithms. So that, a healthy confidentiality level can be achieved.

1.6 Working of Algorithms Used in Proposed Scheme

Data Encryption Standard DES is a symmetric algorithm. It was published by NIST. It implementation is baesed on Feistel Cipher which consist on 16 rounds.

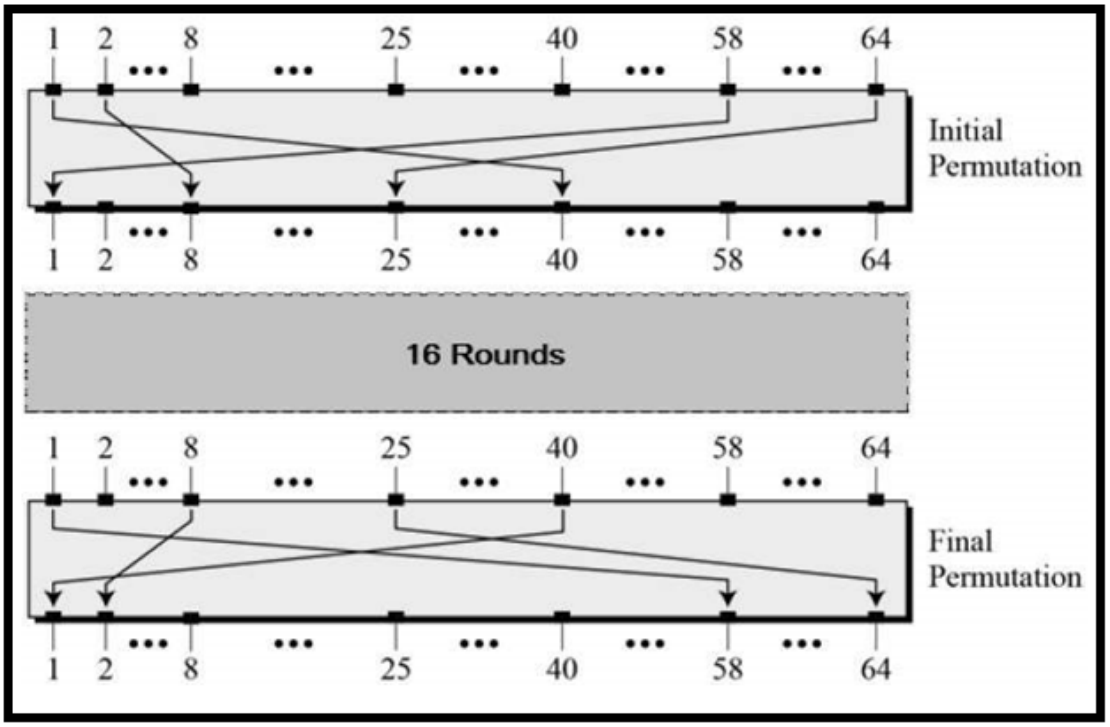

FIGURE 1.6: Initial Permutation [5]

Block size and key size of this algorithm is 64 bits but key length is 56 bits and 8 bits are not used in encryption. Following operations are used in DES.

- Initial Permutation
- Round function
- Scheduling of Key
- Final Permutation

Initial Permutation Working of initial permutation can be understand by using the See Figure 1.6

Round Function Round function is the core of DES function. This function consist of 48 bit key. 32 bits of key which are the rightmost produces the output of 32 bit. Detail is shown Figure 1.7

Expansion of Permutation Box In Round key is 48 bits and input of 32 bits is from right side extracts 48 bits. Graphically of this process is shown Figure 1.8

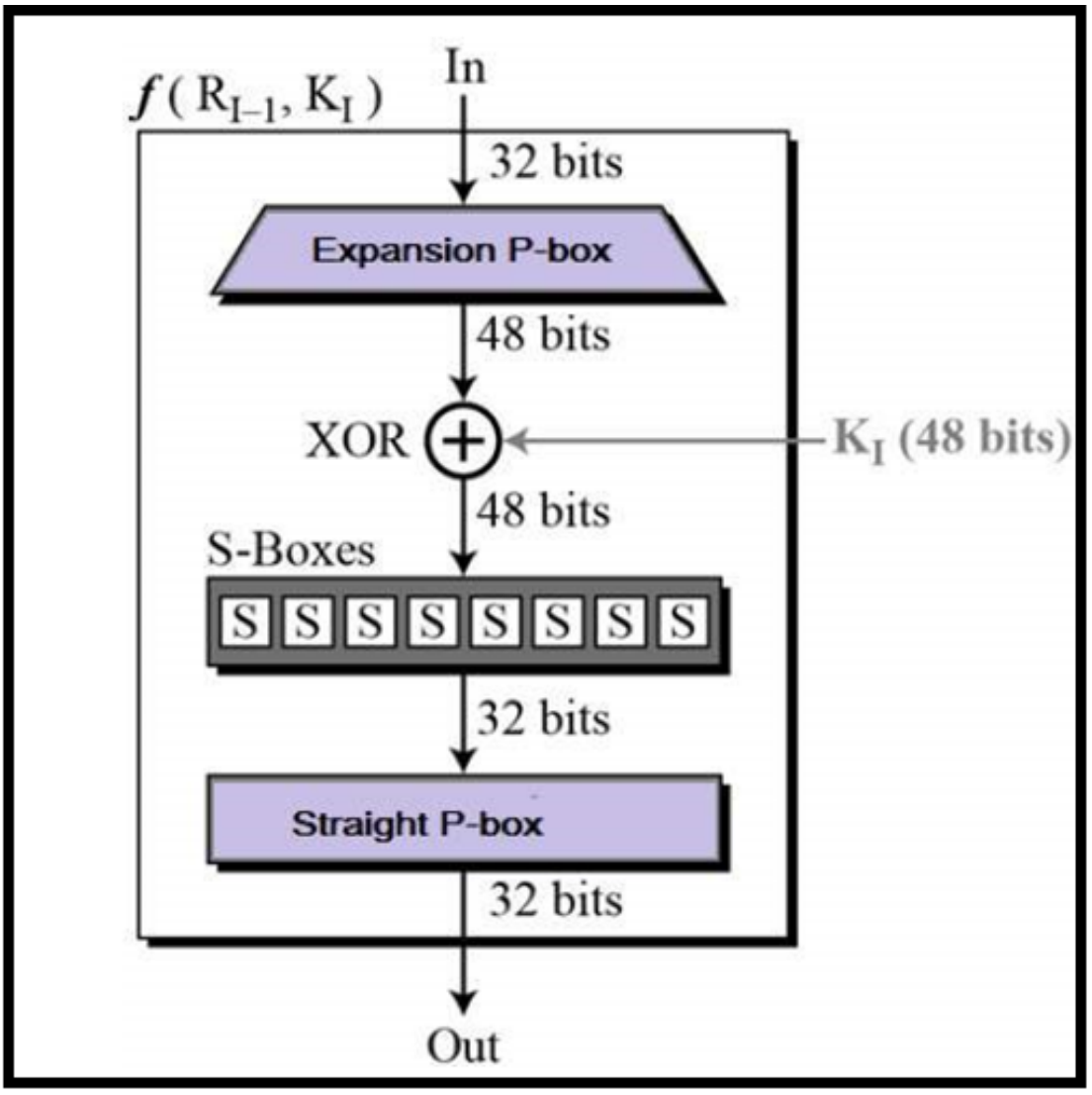

FIGURE 1.7: Round Function [6]

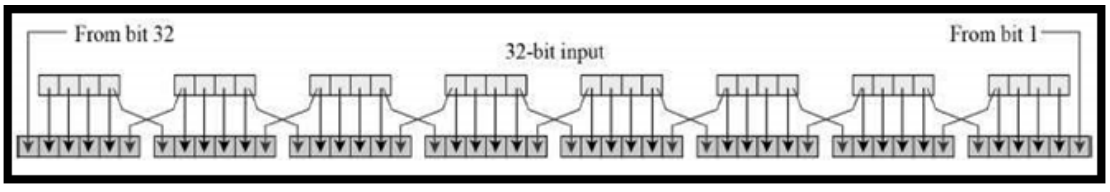

FIGURE 1.8: Expansion of Permutation Box [7]

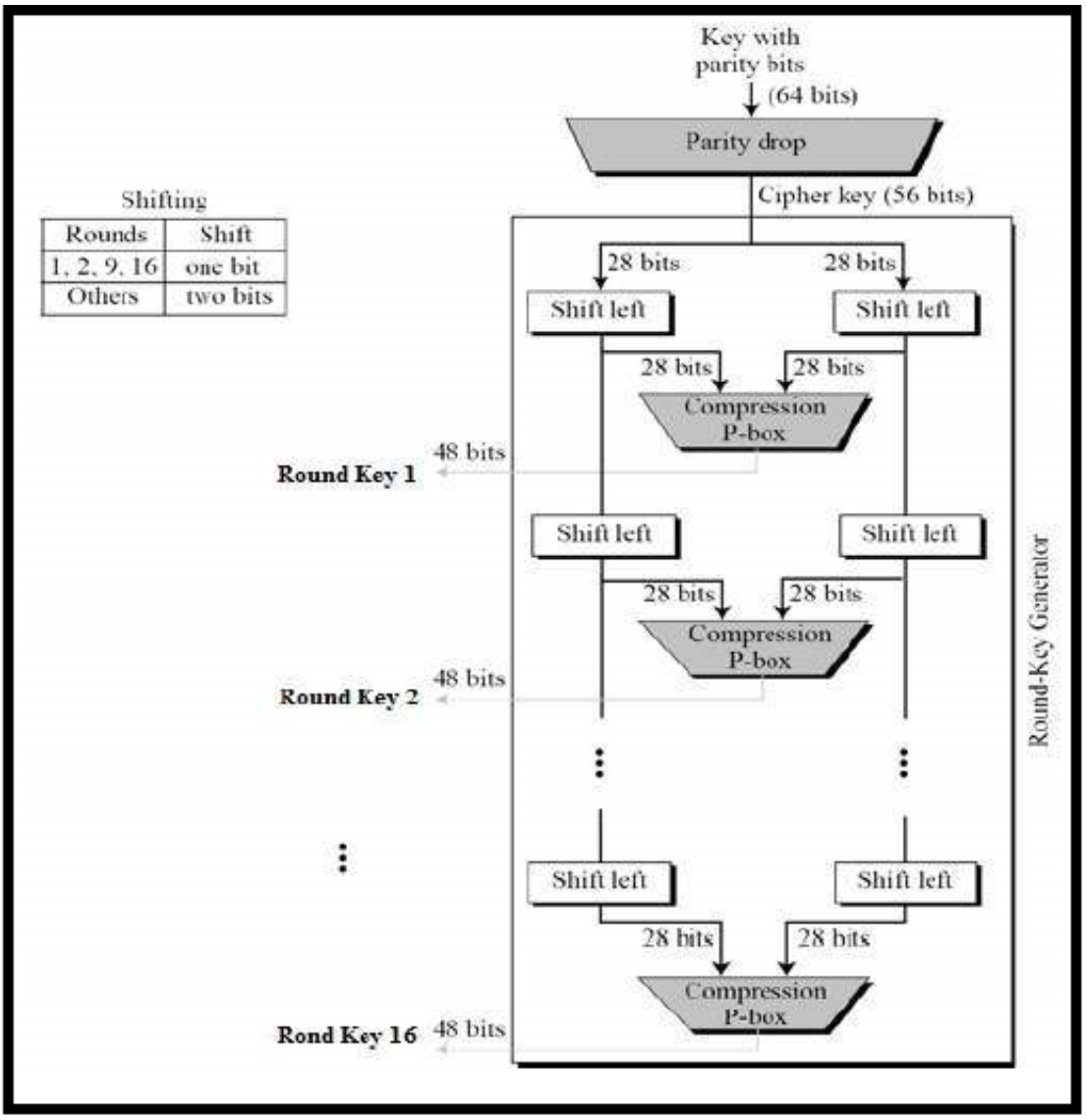

FIGURE 1.9: Key Generation [8]

Key Generation Round function of DES algorithm creates 16 blocks of 48 bit keys our of 56 bit cipher key. This process is shown Figure 1.9 **Avalanche effect** means a big change in cipher text when a small change is made in plaintext. But during the last few years, cryptanalyst have said that DES is a weak algorithm because of it keys size. Thats why NIST enhances from DES to 3DES algorithm.

3DES Algorithem Working 3DES Figure 1.10 first generate the three keys K1, K2, K3. Each key size is 56 bits and total size of 3 keys is 3 * 56 =168 bits and the encryption process is described below: Encryption and decryption process is

[7]https://www.tutorialspoint.com/cryptography/cryptosystems.htm
[8]https://www.tutorialspoint.com/cryptography/cryptosystems.htm

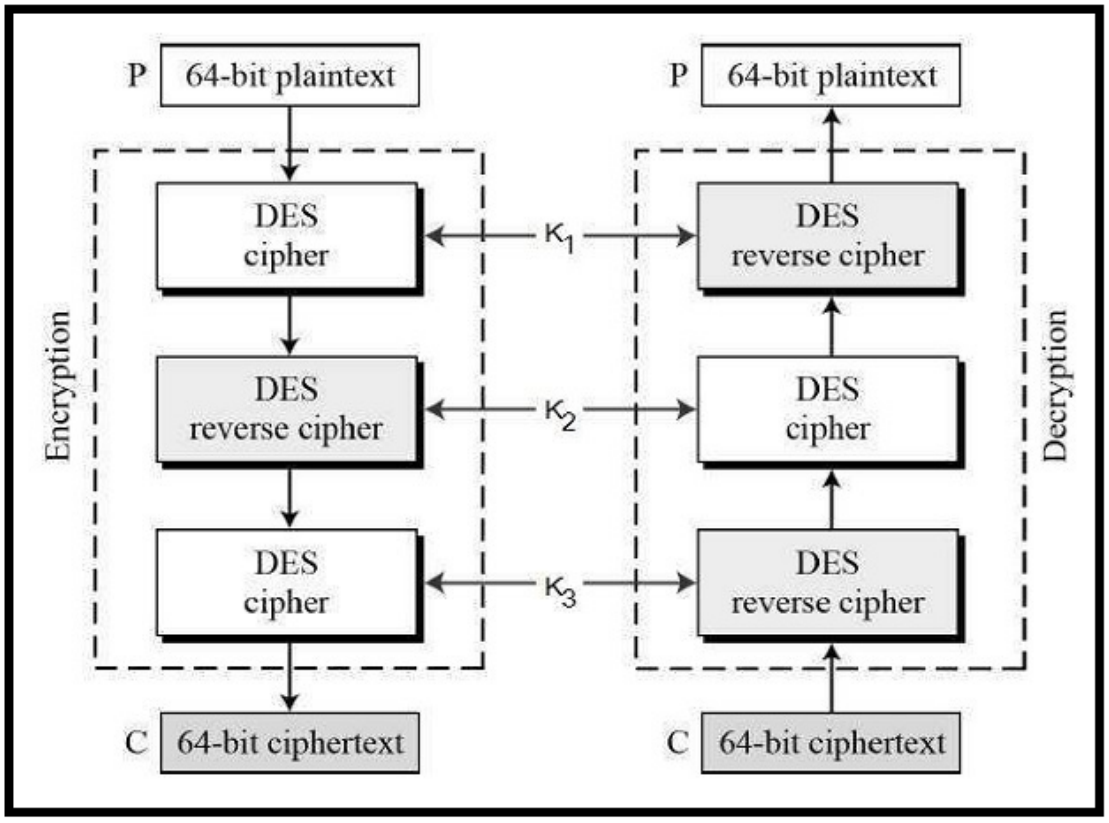

FIGURE 1.10: Architecture diagram of 3DES [9]

as follows

- K1 encrypts the plaintext
- Output of first is decrypted by K2
- And at last step the output of second block is again decrypted with K3
- This is this final cipher text
- Decryption is the reverse process

If same key K1, K2, K3 are used then it works same like DES.

Advance Encryption Standards NIST introduced another algorithm symmetric algorithm with the name AES See Figure 1.11 . Vincent Rijmen, Joan Daemen published this in 1998. It uses three key sizes 128,192, 256 bits and block size is 256 bits. Keys features of AES are as follows:

[9] https://www.tutorialspoint.com/cryptography/cryptosystems.htm

- It is block cipher
- Symmetric key algorithm (encryption and decryption can be done with single key)
- Multiple key sizes can be used according to requirement e.g 128,192, 256 but 256 key size is more secure.
- Computation power is faster
- Architecture is open and can be easily design in any computer languages

Working of AES Algorithem

- AES does not work on Feistel architecture. In feistel half of the data block is used to modify the other half of data. Wheres AES works on the entire block as a single matrix for substitution and permutation during every round.
- The main key is partitioned into an set of fortyfour 32 bits of words. Four distinct words of size 128 bits are used for round key in each round.
- There are total four stages used in AES, one is for permutation and the remaining three are for substitution
  - Substitute bytes: It uses S-box to apply byte byte substitution operation on the block
  - Shift Rows Operation: It is a simple permutation operation
  - Mix Columns Operation: In this operation GF(28) method is used for subsitution.
  - Add Round Key Operation: A bitwise XOR which is performed on current block with a portion of the expanded key
- The structure of AES is very easy. in Encryption and decryption phase, cipher starts with an AddRoundKey round with nine stages, each stages consists all four rounds, followed by a tenth round of three stages. Figure 5.4 shows the structure of a full encryption round.

- The Add Round Key round makes use of the key.The cipher starts and ends with an Add Round Key stage.
- Add Round key rounds works like Vernam cipher and by itself would not be daunting where remaining three rounds are used for confusion, jumbling and nonlinearity. But important thing is that these stage provide security without using a key.
- Each stage is very easy to reverse. An inverse function is applied in decryption algorithm in each stage of substitute Byte, Shift Rows and Mix Column Round. The inverse of Add Round key rounds can be achieved by simply XORing the same round key round on block by using the result of A B B = A.
- Normally block cipher algorithms used the expended key in reverse order while performing the decryption process. But, decryption process are not as identical as the encryption. But AES works in different way that why encryption and decryption is performed with same speed.
- When all these four rounds are reversible than it is easy to check that decryption process recover the plaintext. Figure shows out the encryption and decryption process in opposite vertical directions. Where at each horizontal point state is same for encryption and decryption.
- The last round of both phase contains of only three rounds. Again, it is a importance of the particular layout of AES algorithm and it is required to build the cipher reversible.

1.7 What is HIPAA Act and GDPR ?

HIPAA [10] is an abbreviation of health insurance portability and accountability act. It was passed by USA government in 1996 to protect patient sensitive information. It guides the health care sector that which patient attributes needs

[10]http://pranav-mnit.tripod.com/aes.htm

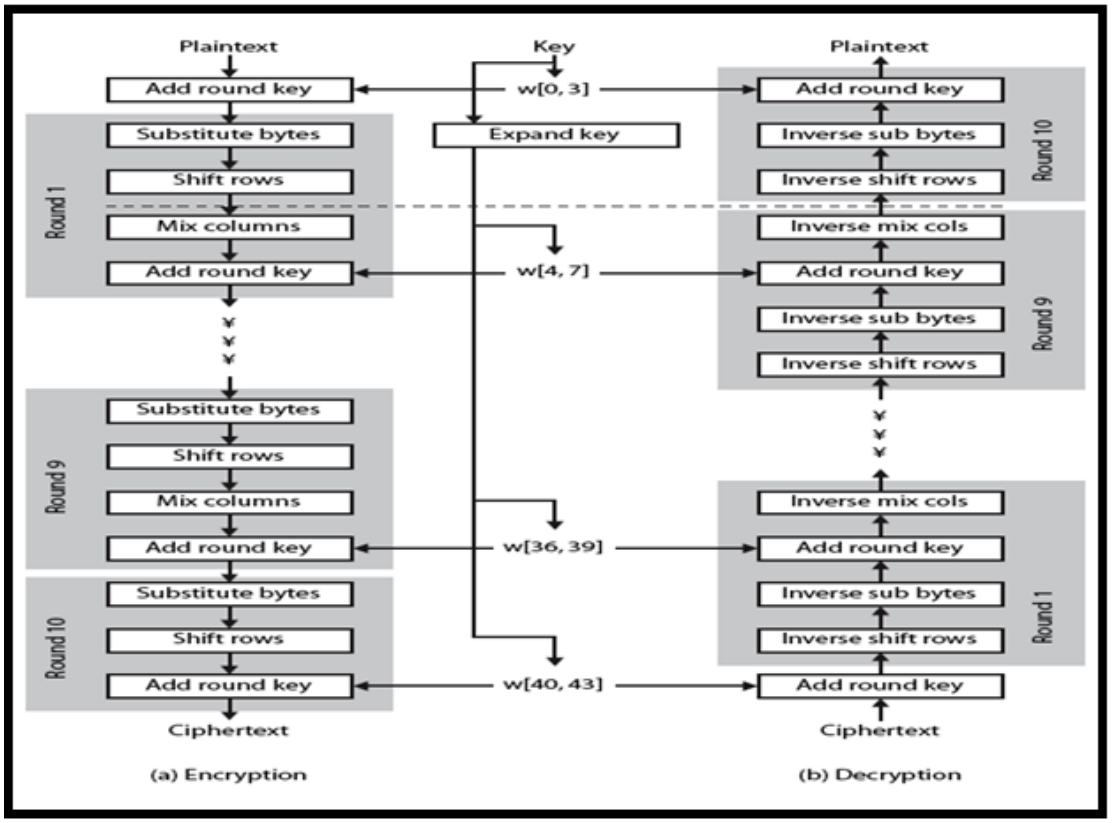

FIGURE 1.11: Architecture AES Algorithm [10]

more protection and security especially when data is in cloud environment. It provides different rules regarding data access and data protection according to sensitivity of the data. Following 18 attributes are identified by the act which needs protection[11].

- Patient First and Last Name
- Address including zip code,city,country
- All dates e.g DOB, DOA etc
- Phone No
- Fax
- Email ID
- SSNo(Social Security Number)

[11]https://www.luc.edu/its/aboutits/itspoliciesguidelines/hipaainformation/18hipaaidentifiers/

- Medical record No
- Health Card information
- Bank Account No / Credit Card Information
- Certificate or driving license
- Vehicle No
- Device identifiers and serial numbers
- Web Address
- Internet Protocol (IP) address
- Biometric
- Any type of image
- Any other characteristic that could uniquely identify the individual

Where GDPR[12] (general data protection regulations) is the European Union regulations which was accepted in 2016. After 2018 it has become compulsory for all the organization of European Union countries which stores the personal information of person must be compliance with GDPR.

1.8 Motivation Factor

When a protected health information is leaked out then it will become very dangerous for both patients and health organization. For example, if a patient credit card is stolen then he may lose his money. But when the patient sue against that organization then court fines that organization. So, two type of loses are occurred here. One patient is getting suffered and at the same time organization is also losing its reputation. This point encouraged us to suggest a secure and reliable technique for both.

[12] https://www.hipaajournal.com/what-countries-are-affected-by-the-gdpr/

1.9 Problem Statement

There is a question mark on condentiality of PHI data when it is stored in cloud environment. This information can be leaked out due to plain format storage or by using the weak encryption algorithms

1.10 Research Questions

The above problem statement raises following research questions:-

Q # 1: What types of data confidentiality techniques are available for cloud based environment?

Q # 2: What are the major drawbacks/ flaws in these techniques?

Q # 3: How multilayer based encryption techniques can effectively be used to preserve the confidentiality of healthcare data?

1.11 Research Methodology

Research methodology plays very important role to achieve the target. We have adopted the following research methodology Figure 1.12 to answer the above questions. Because this help us in finding the research gap. In step first, we have made selection of paper based on single and multilayer encryption techniques for cloud environment.

A set of 45 paper is chosen and then comparative analysis is performed on it and at last a proposed technique of multilayer encryption is suggested. The first criteria selection of paper is answering question no one and comparative analysis is helping us in finding the research gap and at third point we are able to produce new technique. This is the work flow of our methodology which is showing that who we will achieve the target.is showing that who we will achieve the target.

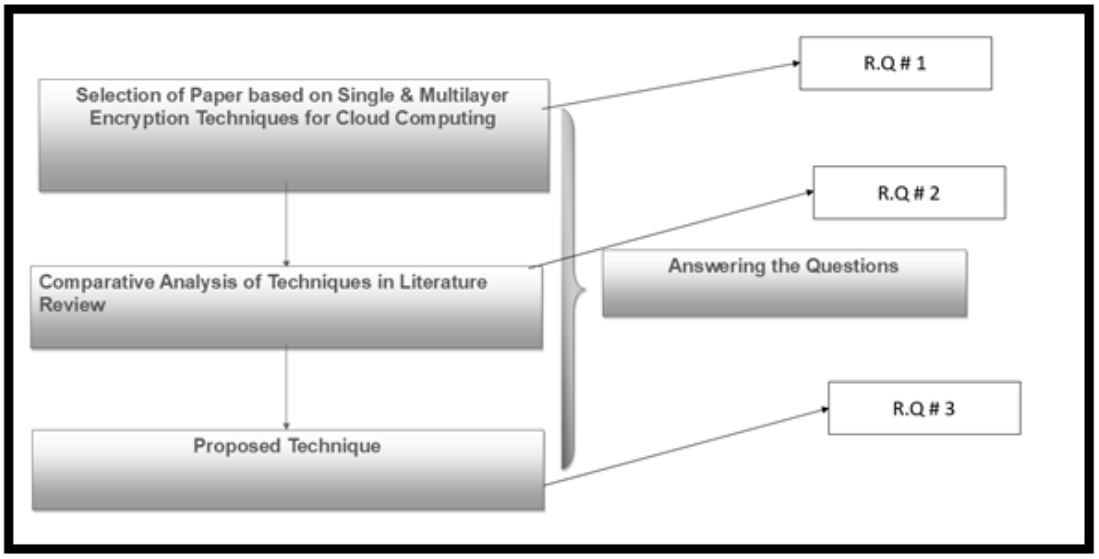

FIGURE 1.12: Research Methodology Diagram

1.12 Purpose of Study

The main objective of this thesis is to provide a comprehensive scheme which will provide confidentiality, integrity to patients data by keeping in view of HIPAA and GDPR compliance. This will be gained by encrypting and decrypting the data in multilayered form and data is available at cloud environment on the basis of 24/7.Algorithms which we will use for encryption are industry standard algorithms recommended by NIST[13] .

Based on this methodology we have found the research gap that multilayer encryption is more suitable for health care sector as well as for other related organizations.

1.13 Significance of The Thesis

Following list is showing the significance of the thesis

- This study will increase the confidentiality level of the patient data and IT based healthcare sector.

[13] https://www.nist.gov/

- The proposed technique will provide better security by using multilayer encryption
- The algorithms combination will be selected to ensure the better security and performance as well.

Table 1.2: Significance of Thesis

The problem of	Data confidentiality, Privacy
Affects	Hospitals, Patient, Cloud Computing Environment, Health Insurance and related organizations
The impact of which is	A patient may be led to death, heavily loss for health related Organization, Personal privacy will disturb, personal information will be lost
A successful solution will provide	Data confidentiality ,Patient data must be safe, secure and available 24/7

1.14 Conclusion

Following are key points of the above chapter.

- What is cloud computing and its little history?
- Cloud computing service model for health care sector.
- What is cryptography and a glimpse on its history?
- How the algorithms which will be used in experimental setup will work.
- A few points about HIPAA and GDPR

- Motivation factor of the thesis and problem statement.
- How is research methodology adopted?
- What will be the significance of this thesis?

1.15 Thesis Organization

This thesis is organized as follows

- Chapter 2 is about literature review in which we have described the different suggested techniques and made a comparative analysis on these techniques.
- Chapter 3 is regarding Experimental setup for proposed scheme in which we have described how we will take dataset ,how encryption is performed in RDBMS and how our methodology will work.
- Chapter 4 is presenting about the hardware and software requirements for experimental setup, how practically experimental is performed and it results are discussed.
- Chapter 5 is about conclusions and Future work.

Chapter 2

Literature Review

To provide a solid solution of the problem statement discussed in chapter 1 we need to answer the following questions during our literature review.

Q No 1: Is multilayer techniques adopted for encryption and decryption?

Q No 2: What are the approaches adopted in the literature?

Q No 3: What are the strength of the techniques adopted by different users?

Q No 4: What are the drawbacks / Weakness in current techniques?

This section provides a comprehensive literature review of the research conduct in this area and provides critical reviews of all the proposed approaches. We have divided this chapter into two sections. Section 2.1 shows the techniques of research methodology Section 2.2 shows the related work. Section 2.3 shows the critical reviews of the literature review and 2.4 shows the conclusions of the literature.

2.1 Related Work

In [11] author has defined the multilayer approach for e-health service according to ISO 17799 document. He has divided the information in three categories i.e. Top secret, highly confidential and proprietor information. They have introduced the

symmetric encryption algorithms 3DES and hash value function. Authors have used the key size of 193 bit long for layer1 and 129 bit to 192 bit for layer2 and 112 to 128 for layer3 and 80 to 111 bit for layer 4. But their work is focused on only one algorithm which is 3DES. Only single algorithm is used for encryption and decryption.

In [12] this paper authors have introduced the cipher text policy attribute based encryption (CP-ABE). The key for encryption consists of policies and they say that if key has hacked then only those records will be decrypted whose key is hacked but the remaining will remain protected.

In [13] authors discussed the Elliptic curve cryptography technique and they introduced a third party key generation techniques. Data owner send request to third party for key and encryption of the document online. Third party will encrypt and send key to data owner and the owner will upload the date at cloud server and keep the key for future use.

In [14] this paper author introduced medical data encryption technique by using AES with SOAP/XML and SHA-1. He has encrypted the data with AES algorithm by using the SOAP/XML.

In [15] authors have projected a new method for big data analysis in healthcare sector to preserve the security and privacy. They have used bilinear pairing protocol for big data analysis. They have also used the authenticated key management system. Time complexity is depended upon the key size. Computational complexity is measured with bilinear paring system.

In [16] authors have just compare the DES,AES,3DES, CAMELLIA, Height, and RECTANGLE algorithm with different key size and block size of data and compare the results. They have also proposed a new S-box should be prepared for eHealth systems. That will increase the speed and throughput.

In [17] a flaw is found in [18] for USB MSD (Mass storage Device) implementation. Then a new ERP is introduces for smart healthcare system which is more secure than [17].

In [19] authors used a techniques in which EPR and logo of the data has been generated by bilinear interpolation and then magic rectangle encrypted the data by using LSB algorithm which is called steganography.

In [20] authors have well thought-out a new healthcare model for cloud data storage. They have applied the RBE (Role Based Encryption) model. First, they have described the PCEHR (Personal Control Electronic Health Record) model which has been introduced by Australian government. Then this PCEHR is implanted in RBE for data security. They design the PHR structure and the attribute based encryption on it. They claimed that their approach will provide a flexible control on data storage.

In [21] first authors have discussed the threat sculpt and authentication model for Iot-based devices in cloud environment. They have tried to investigate the current challenges of security and requirement for IoT based data linkage in cloud. Their main focus in research is the authentication mechanism. They have given a virtual concept of new technique. In their paper they have made a comparative study on computational and communication cost. Merits and demerits of existing authentication techniques are also remain under consideration but not specification solution is suggested.

In [22] authors suggested a hybrid technique. They have applied the linear network coding method by using the ElGamal algorithm for the security of healthcare data. For the exchange of key ElGamal re-encryption method is used. Then a comparison based on reliability factor achieved from LNC is compared with other schemes. But single encryption is done on patient data.

In [23] this paper EGC (Elliptic Galois Cryptography) protocol is introduced which provides high data protection security. Authors main focused on IoT data transmission between cloud and IoT. With the novel ECC over Galois field, the proposed EGC protocol provided better security.

In [24] Surveys the modern schemes on secure and privacy-preserving medical data sharing of the past decade with a focus on block chain-based approaches. They

classified them into permission less block chain-based approaches and permission block chain-based approaches and analyze their advantages and disadvantages. They also discussed potential research topics on block chain-based medical data sharing.

In [25], they have presented the ECC technique for the protection of patient data in WBAN. They applied the symmetric cipher algorithm DES and Feistal for encryption and decryption on patient sensitive. They used the ECC for the management the keys for distribution, alteration and storage.

In [26] authors encrypted the patients data by using Advanced Encryption Standard Algorithm (AES). Then this hidden data is protected behind image by using by Least Significant Bit Algorithm. This protected data is now sent to the desired receiver. At receiver end Inverse technique is applied on encrypted data for decryption. They claimed that their technique provides better security with combination of cryptography and steganography.

In [27] authors introduced the digital auditing and water marking techniques. They said that insider are more dangerous for patient data in cloud environment. They applied the low quality water marking on low interested data and high watermarked image.

In [28] authors approach is based on columned based encryption and decryption. A new scheme is developed with the name IFHDS. This scheme is masked the personal and sensitive data. Theme of this framework is that it partitioned that sensitive data according to requirement and performs encryption on it and stored it in cloud. Authors claimed that if attack occur then only a little portion of the data will be open not the all. They performed different experiment on sensitive data and claimed the best technique. But only single type encryption is done on sensitive data.

In [29] They offered a novel technique by using clustering algorithm for data which is partitioned vertically. They examined the throughput of algorithm by using

different experiment. After that they presented a local version of protocol by using homomorphic encryption.

In [30] authors suggested an idea named MIDEA model. Encryption process is assigned to cloud server. They claimed that this will increase the scalability and decrease computational cost and data. After that MAC encryption text will be attached with the stored data for better protection.

In [31] authors described the efficiency of AES algorithm for data protection. In their research they modified the AES algorithm for the enhancement of the security. They used one time padding technique. They implemented the polybius square matrix and also increased the no of rounds for data protection

In [32] authors encrypted the message by using authentication MAC. They used AES128 and block chain mode for message encryption. They introduced a new technique with name ultra-low power AES algorithm with 8 bits. They claimed that this approach used low power consumption with higher resources efficiency.

In [33] introduced a techniques named attribute based encryption with the name HealthShare. Their focused was on sharing of patient data which is being stored at different clouds between different organizations. They developed a new protocol which was based on attribute based encryption and revocable key policy. They said that encrypted patient data cloud be shared to different organization based on patients willingness and data owner.

In [34] developed a new protocol for protection of data storage at cloud. Their theory is based on two main points. At first they described the Siemens Healthcare system with name Melior. Second, they have discussed the challenged of migrating the Patient Health system at cloud and what basic security requirement are required to move at cloud.

In [35] writers explained the small plain text data encryption technique with single algorithms which are currently available in market. They said that if you want to secure the big healthcare sector data then you need to adopt some new approaches which will be based on big distributed process and storage in cloud environment.

In [36] Author has warned the healthcare sector about the insider and outsiders attack. He said that insiders attacks ratio is very high rather than outsiders. He further says that 52% healthcare hospitals believe that they are at high risk due to insiders. Because insider can alter the patient record easily and they can easily sell the data for any type of ravage. He can also blackmail the patient for some money.

In [37] authors said the by using the Internet data transfer has become very popular and easy. Internet is a source by which data can be transmitted fast and very accurately to the destination. But, the attackers may misuse it. They said that cryptography and Steganography techniques are very helpful for this. In this papers they have used the Least Significant Bit (LSB) algorithm on patient image based data e.g. x-ray, MRI etc. for encryption. They have used some machines learning techniques for their comparisons.

In [38] Authors have developed a new methodology which can be used for hiding the information in shape of image. They have compressed the file which needs encryption. Then on compressed file they have applied the AES algorithm and after that they applied steganography techniques by using LSB algorithms.

In [39] authors converted the doctors diagnosis and reports in scanned images then they applied the steganography and cryptography.

In [40] authors have simplified the Feistel algorithm without S-Box. Then they have applied the encryption and decryption on sensitive patient data. They have compared the results with old DES algorithms. They have acknowledged that their techniques have poor avalanche effect because of S-Box removal.

In [41] authors have used the ECC and SNAP protocol to secure the patient data for WBAN. They said that each sensor has a biometric device which authenticate the patient then he can share the sectors information.

In [42] authors have developed a role based access control system named (CPRBAC) for cloud based data protection. They have also developed an auditing technique which is used to monitor actively and report any illegal activity on system. But

their work is not used any cryptographic techniques which provide integrity and confidentiality.

In [43] author has introduced a patient centric e-system. By using this selective portions of data can be shared at cloud. They have utilized the broadcast attribute based encryption on patient files. They have also used public key encryption with public key encryption search techniques but they have not defined the algorithm.

In [44] authors have mixed the block chain technique with signature based technique to protect the storage of patient data. Signature based techniques verifies that data is from original send and block chain provide integrity. But they have stored all the data in on chain blocks which has great impact on network performance.

In [45] authors have secured the PHR with attribute based encryption in semi trusted cloud environment. They said that public domain is for doctors and researchers and personal domain is for family and friends. They have split the ABE techniques separately for public and private cloud. This creates a huge burden on patient that how he will manage the keys and authorized the users.

In [46] authors have developed an algorithm and combine multiphase and multiple encryption techniques. They have used AES 256, RSA, DES, Blowfish algorithms for random multiphase encryption process. At end they compared the time complexity and security of data on data size.

In [47] authors have implemented the ECC algorithm for encryption with multiple times. They observed that multiple time usage of ECC algorithm has increased the time complexity. According to them there is a tradeoff between security and time.

In [48] authors have implemented the multiple encryptions on secure electronic transition. They said that this multiple encryption process provides better security. They have applied their strategy on ATM transactions.

In [49] authors have compared the homomorphic algorithms. They have just described how the encryption and decryption keys would work for cloud.

In [50] authors said that IDM (identity management) is main problem in cloud environment. They proposed an IDM method which will not trust on third parties. They have applied the RSA distribution key and attribute based encryption method for sensitive data security.

In [51] different encryption algorithms have been referred for data security in cloud. Authors have compared the security level of different standards algorithm.

In [52] different challenges of cloud environment are highlighted. Authors have provided different suggestion to different cloud providers for data security.

In [53] authors provided a novel approach for the improvement of data security. They suggested how an organization cloud use specific encryption techniques named location based encryption.

In [54] data security concerned is discussed. ECC is importance also discussed.

In [55] different security challenges of cloud computing is reviewed. Different techniques of data security discussed which created reliability.

2.2 Literature Review Analysis

We have performed an analysis an experiment on the basis of literature review and compared the results of different authors on the basis of above questions and then find a research gap See Table 2.1. However, there was some concept of multilayer based encryption is introduced by different authors on protected information but we have found that nobody has utilized this approach of built-in RDBMS (Microsoft SQL server & support Cryptography algorithms) specially management of the keys regarding symmetric and asymmetric. We will prefer to use the symmetric key because here in our module we do not want to share the keys with patient as well. This will provide increase the security level.

TABLE 2.1: Literature Review Analysis

Paper	**Multilayer Approaches**	**Security Goal Achieved**	**Strengths**	**Weaknesses**
[11]	Yes	Data confidentiality	3DES and Hash Algorithm	How key shared, standards of HIPAA and GDPR defined attributes not consider
[12]	No	Data confidentiality	Attributes based multilayer algorithm but one for each	How keys shared, standards of HIPAA and GDPR defined attributes not consider, RDBMS built-in work
[13]	No	Data confidentiality	ECC algorithm	Single Encryption method used, not follow any standards.
[14]	No	Data confidentiality	AES algorithm	Single Encryption method used, not follow any standards like HIPAA, GDPR
[15]	Yes	Data confidentiality	Bilinear Pair and Authentication key	Key management issues and HIPAA, GDPR compliance
[16]	No	Data confidentiality	Survey on DES, AES, 3DES algorithms	No implementation
[17][18]	No	Data confidentiality	USB protection for healthcare data, Both almost same work.	Single layer encryption

[19]	Yes	Data confidentiality	EPR and LSB	Image based encryption not follow any standards like HIPAA, GDPR
[20]	No	Data confidentiality	Role based encryption	not follow any standards like HIPAA, GDPR
[21]	Yes	Data confidentiality	IoT based devices	Single encryption
[22]	No	Data confidentiality	Elgmal algorithm	Single encryption
[23]	No	Data confidentiality	ECC using glaious field	Single encryption
[24]	No	Data confidentiality	Block chain	not follow any standards like HIPAA, GDPR
[25]	Yes	Data confidentiality	DES, Feistal and for key management WBAN	not follow any standards like HIPAA, GDPR
[26]	Yes	Data confidentiality	AES and LSB algorithm	Placed as image based encryption
[27]	Yes	Data confidentiality	Watermark on data and digital auditing took	not follow any standards like HIPAA, GDPR
[28]	No	Data confidentiality	Data partition and apply single encryption on data	No Multilayer encryption and not according compliance

[29]	No	Data confidentiality	Partition the data vertical and apply encryption	Single encryption
[30]	No	Data confidentiality	MIDEA model for encryption and MAC based encryption	
[31]	Yes	Data confidentiality	AES based encryption and hide data behind round rectangle	Image base encryption & if data is stored in RDBMS then how apply
[32]	Yes	Data confidentiality	AES128 bit & Block chain	Implementation on RDBMS and not follow any standards like HIPAA, GDPR
[33]	Yes	Data confidentiality	Attribute based encryption & revocable key	Implementation on RDBMS and not follow any standards like HIPAA, GDPR
[34]	No	Data confidentiality	Survey	
[35]	No	Data confidentiality	Single Encryption	
[36]	No	Data confidentiality	Insider attackers are more dangerous instead of outsiders	

[37]	Yes	Data confidentiality	Steganography using LSB and converted in image	Not possible on PHI attributes
[38]	Yes	Data confidentiality	AES with some variation and then LSB	Convert into image based data
[39]	No	Data confidentiality	Steganography	Single Encryption
[40]	Yes	Data confidentiality	Feistal Algorithm with S-box modification and DES	Apply old techniques

2.3 Findings from Analysis

From this critical analysis it has been figured out that all the techniques are applied on sensitive data for its protection in different ways. Some authors have combined the different cryptographic algorithm for the better results. A few have used the old techniques of encryption and decryption. Some has considered HIPAA standards partially. Another group has used the different machine learning algorithm and stored the data at cloud in shape of images. However, we have revealed that researched techniques has not combined the HIPAA act & GDPR on PHI attributes with multilayer encryption. Sharing of keys is also between encryption and decryption is big issue. Becuase for sharing the keys we have to involve third party or we have to pay against each key. That's why solution will become costly.

From our research, we have revealed that more consideration is required at HIPAA & GDPR attributes to secure the sensitive data of patient. Therefore, we have proposed a new techniques in which we have taken a patient data attributes according HIPAA and GDPR compliance and apply multilayer encryption on it and then we will compare the results with other techniques for the cadre of confidentiality and performance. Surely, this approach will increase the confidentiality, integrity level of the patient as well as the IT health based sector. It will also open a new concept of protection on health care sector.

2.4 Summary

In total we have reviewed 45 research papers out of which 8 are shown here. In our literature we have found 8-10 techniques are based on single cryptographic algorithms where 5-6 authors have worked on imaged based data, and converted the data in shapes of images and 2 authors has worked on role based encryption, another theory we have found is related to block chain techniques. Two techniques is related to wireless body area network. Some authors more consideration is related to IOT based data. One author focused on insider attacks and saying insiders are more dangerous rather than external. So result is that we have found the nobody has combined the multilayer encryption techniques by keeping in view of the acts of HIPAA and GDPR to protect the patient PHI attributes in such way. We thought this can be useful for the healthcare sector by which patient information will become more protected and confidentiality level will be more enhanced.

Chapter 3

Experimental Setup for Proposed Scheme

In this chapter, we have analyzed the experimental set up of the proposed techniques. This scheme focuses on encryption and decryption methods that how we protect the protected /sensitive information of the patients. We have developed a scheme which will encrypt the PHI data according to multilayer algorithm. The encrypted data will be then uploaded at any trusted cloud based server which will be accessible by the patient for his future prospective. We have developed the above scheme by using client/server architecture that needs to be transmitted over the network.

We have divided this chapter into different sections. Section 3.1 describes how we get the dataset, Section 3.2 describes about how the data will be encrypted, Section 3.3 describes the methodology architecture , 3.4 describes that encryption facilities are available in SQL server database for encryption ad Section 3.5 is about conclusion.

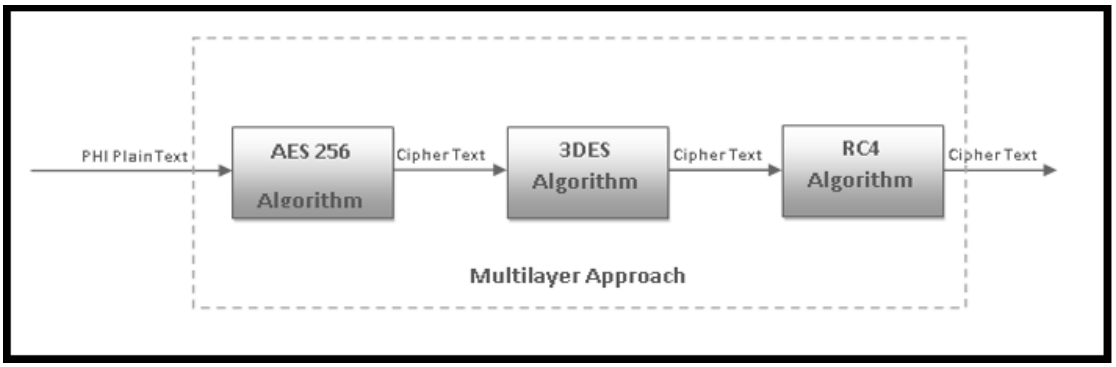

FIGURE 3.1: Multilayer Protection Technique

3.1 Data Set Selection

For the development of the scheme and analysis of the target we have select a dummy dataset (for patient safety) of approximately 500 patients and we have used the below diagram for encryption of PHI each attribute

3.2 Multilayer Encryption of PHI Attributes

Figure 3.1 shows that an attribute is selected from PHI data in the shape of plain text. This attribute is passed to one algorithm e.g. AES256 with a key and then output of this algorithm which will be cipher text that will be passed to 3DES algorithm with a different key and so no. This is the concept of multilayer encryption which will protect the data and increase the confidentiality level.

3.3 Methodology Architecture

Figure 3.2 presents that a healthcare system exist with a database management system. All the PHI related data is stored in the database. We will take dummy test data from database and apply the encryption algorithms which are available in RDBMS and apply these standards algorithms on PHI attributes and save the data in cloud environment. At start when patients will be register a MR No with randomly generated complex password will be assigned to patient for information

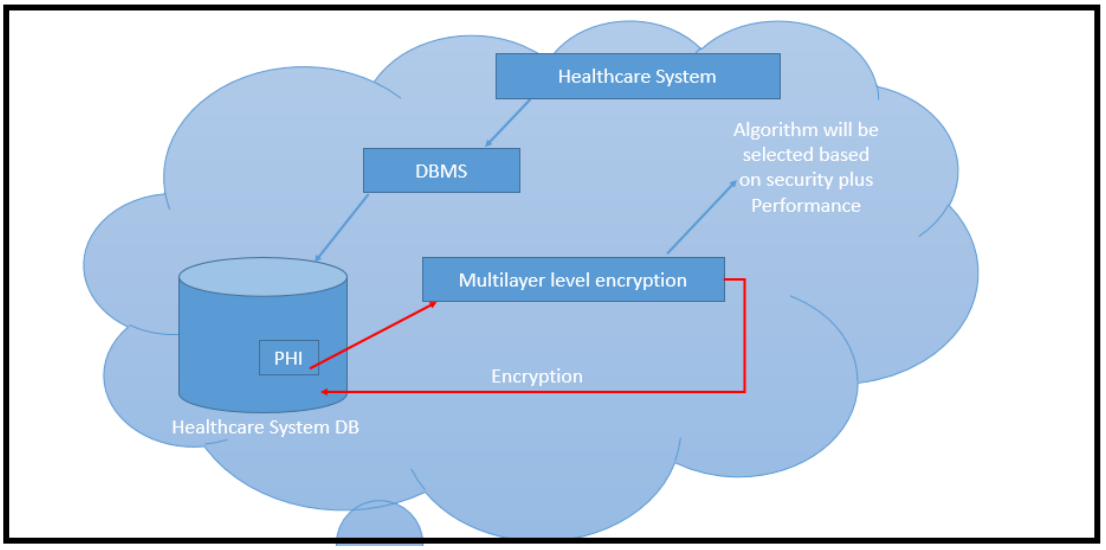

FIGURE 3.2: Architecture diagram of methodology

Receipt #: 1-2020-01-20390 **Date:** 28/01/2020 **Visit:** 8
MR No: 1-2018-23524 **Name:** MUSHTAQ AHMAD S/O MUHAMMAD MASKIN **Category:** Free
CNIC: 3740616044471()
Contact No: 03005049139 **Clinic:** GLAUCOMA CLINIC (G-8) **Age:** 65 Yrs

Payment Mode : Cash
Reg Fee : 0
Consultaion : 200
Discount : 200
Payable Amount : 0

Next Follow-up: ____/____/_____

For Web Access use MR No as Username and Password = Xt19&6P@

https://wwwl.alshifaeye.org/PatientModule/login

FIGURE 3.3: Login Slip for Patient

access See Figure 3.3. At website patient will input MR No as username and password and click Login. If a username is valid and password is accurate then doctors prescription will be displayed to him after decryption.

We have applied symmetric encryption algorithm AES with different key combinations and 3DES on the data because key is stored in RDBMS and protect by Microsoft SQL server and it is password protected. So for encryption and decryption there is no need to provide the key to patient for encryption and decryption process.

3.4 Encryption & Decryption Process in RDBMS (Microsoft SQL Server)

SQL server has provided 3DES, and different variant of AES for encryption and decryption by using a certificate asymmetric or symmetric key. SQL server maintains the certificates of key internally. This secures certificates and keys provide a hierarchy of encryption and decryption. This characteristic of SQL is called Secret Storage.

Key features of encryption processes supported by SQL server is speed. Symmetric encryption methods are very fast and work with large volumes of data. Another feature is multiple symmetric keys can be open at one time and encryption and decryption can be performed through this way.

3.4.1 How an Encryption is Performed in SQL Server?

The Figure 3.4 will show the overall encryption process of SQL Server on column of a table.

The basic purpose of the database master key is the protection of private keys and certificates which are stored in the database. It is based on symmetric technique. This key is protect by a password at the time of creation.

3.4.1.1 Creation of Master Key

In encryption process first of all a Master key is required with password. After that a certificate will be generated on the basis of Master key.

3.4.1.2 Creation of Certificate

In this RDBMS a digitally singed certificate is required that will be used to protected the Database Master Key.

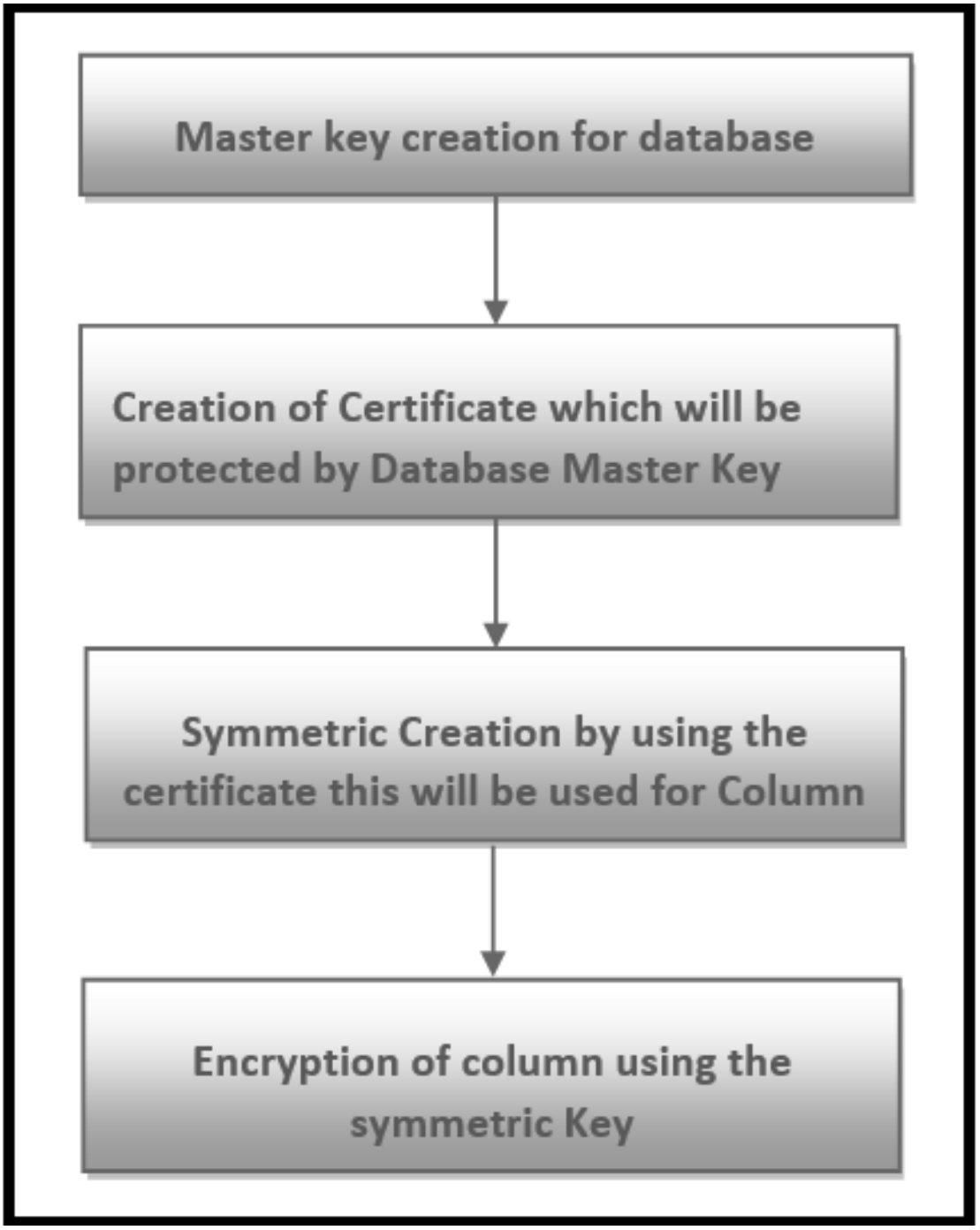

FIGURE 3.4: Overall Encryption Process

3.4.1.3 Symmetric Key

In next step, a symmetric key is required which is used for the encryption and decryption. This key is based on encryption algorithms which are built in sql server e.g. AES128, AES192 and AES256. For the encryption of the symmetric key SQL server use the digital certificate which we have already created above.

3.4.1.4 Creation of Certificate

Now, to alter the store the encrypted data we need to alter the schema of the table and field type will be required in varbinary with max column length.

Here, we have described the general form of encryption that how an encryption is performed in RDBMS (SQL server) and practically implementation is described in Experimental chapter.

3.5 Conclusion

In this chapter we have described these main points

- How we will arrange a dataset for the proposed scheme?
- How mulitilayer encryption will be performed on PHI attributes?
- what will be our methodology?
- How encryption and decryption is performed in RDBMS
- What is the concept of master key?
- What is the purpose of certificate?
- How symmetric key works in RDBMS?
- How certificate and keys will be created?

Chapter 4

Experimental Analysis of Proposed Scheme

This chapter describes in detail the practically how an encryption is done on one table field and the results obtained from this scheme. Chapter 4 is divided into different section. Section 4.1 describes about dataset information. Section 4.2 describes the experimental setup. Section 4.3 provides encryption process. Section 4.4 describes the decryption process and last section 4.5 is about the results analysis.

4.1 Dataset Selection

We have prepared a dummy dataset of 500 patients for test purpose. Sample of the dataset is show below Figure 4.1. Some of the attributes has been taken from by keeping in view the GDPR and HIPAA e.g. MR No (Medical Record No), name, relative name, gender, address, date of birth, Date of registration, NIC, mobile no and Account no/Credit card info. Both these acts defined these attributes need extra care specially when the data is in cloud environment. To enhance the confidentiality level we have taken special consideration on these PHI attributes for encryption and decryption.

Patient_no	first_name	last_name	relative_name	sex	address	date_of_birth	date_of_registration	visit_date_time	NIC	Phone_No
1-2018-10154	REHMAN	BI	M IBRAHIM	1	GILGIT	01/01/1973	08/02/2018	08/02/2018	7110347468740	3469557182
1-2018-10157	MUHAMMAD	NASEER	MUHAMMAD BASEER	0	BANNU	01/01/1970	08/02/2018	08/02/2018	1110154036677	3369115007
1-2018-10159	GHULAB	JAN	ABDUL GHAFOOR	1	POONCH	01/01/1956	08/02/2018	08/02/2018	8230327053772	
1-2018-1016	MUHAMMAD	YOUSAF	MUHAMMAD KHAN	0	KOTLI	01/01/1957	04/01/2018	04/01/2018	8120253533745	3445216411
1-2018-1016	MUHAMMAD	YOUSAF	MUHAMMAD KHAN	0	KOTLI	01/01/1957	04/01/2018	04/01/2018	8120253533745	3445216411
1-2018-10162	GHULAM	NABI	MUHAMMAD AJAB KHAN	0	ABBOTABAD	01/01/1958	08/02/2018	08/02/2018	3429459488	3429459488
1-2018-1017	MALIK	ADNAN	MALIK PERVAIZ AKHTAR	0	RAWALPINDI	01/01/1981	04/01/2018	04/01/2018	3740517480127	3485613623
1-2018-10172	ABU	BAKAR	YASIR ALI	0	RWP	08/01/2018	08/02/2018	08/02/2018	1654564564565	3035197907
1-2018-1018	DUA	ZAINAB	M JUNAID	0	RAWALPINDI	01/01/2016	04/01/2018	04/01/2018	3740198364911	3425697212
1-2018-1018	DUA	ZAINAB	M JUNAID	0	RAWALPINDI	01/01/2016	04/01/2018	04/01/2018	3740198364911	3425697212
1-2018-10187	M	MAJID	JHANZAIB	0	RWP	01/01/2014	08/02/2018	08/02/2018	4548978978987	3324888716
1-2018-1019	TAYYABA	NASIR	NASIR MEHMOOD	1	RAWALPINDI	01/01/2001	04/01/2018	04/01/2018	3720118671240	
1-2018-10191	RASHID	SOHAIL	M BASHIR	0	RWP	01/01/1989	08/02/2018	08/02/2018	1215648789789	3325576558
1-2018-102	MUHAMMAD	LIAQUAT	DOST MUHAMMAD	0	MURREE	01/01/1950	01/01/2018	01/01/2018	3740468232941	3445363872
1-2018-1020	KHURSHIDA	BIBI	IMTIAZ AHMED ABBASI	1	RAWALPINDI	01/01/1951	04/01/2018	04/01/2018	3740403786010	3165006762

FIGURE 4.1: Sample of Dummy Dataset

4.2 Hardware and Software Configuration Setup

Following hardware and software is used for the implementation.

4.2.1 Hardware Requirements

Following hardware is used to build the framework.

- Processor Intel Core i7-6500U Processor
- 8 GB RAM
- 500 GB Hard disk

4.2.2 Operating System and Development Software

Following software is used to build the framework.

- Windows 10 or above
- Visual Studio 12 or 15
- SQL Server 2014 or above
- Framework 4.5

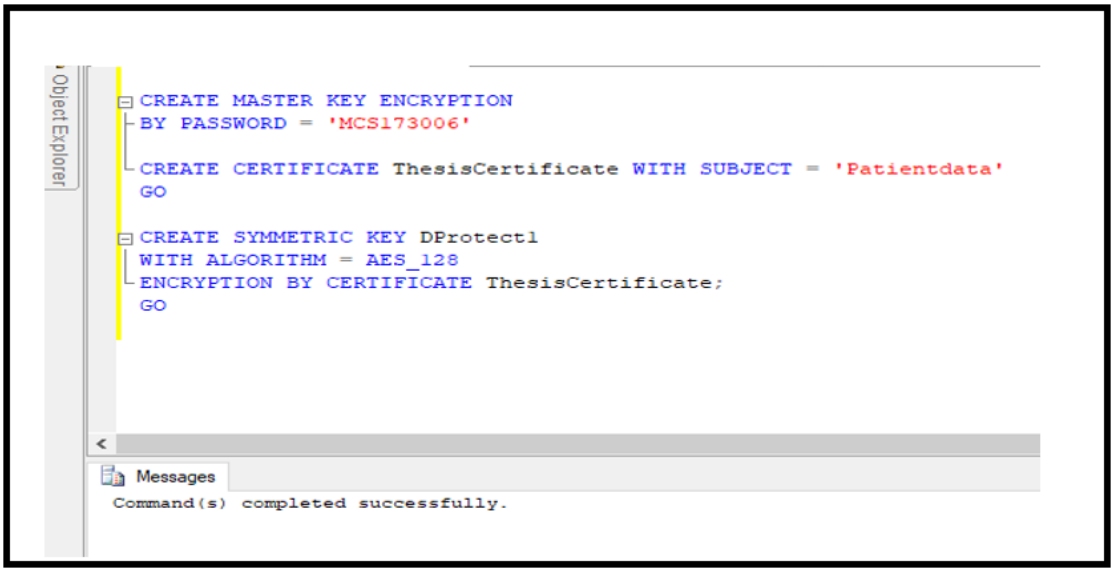

FIGURE 4.2: Keys and Certificate Creation

4.3 Data Encryption Phase

In this phase patient sensitive data which needs to be uploaded on clouds is prepared and Encryption process is applied on it. Steps of encryption of sample is shown step by step with the Figures 4.2.

Step 1: CREATE MASTER KEY ENCRYPTION BY PASSWORD = MCS173006

Step 2: CREATE CERTIFICATE ThesisCertificate WITH SUBJECT = 'Patientdata'

GO

Step 3: CREATE SYMMETRIC KEY DProtect1 WITH ALGORITHM = AES_128 ENCRYPTION BY CERTIFICATE ThesisCertificate;

GO

Step 4: ALTER TABLE patient_registration ADD Sencryptedmrno varbinary(MAX)NULL,
Sencryptedfname varbinary(MAX)NULL,
Sencryptedlname varbinary(MAX)NULL,
Sencryptedrlname varbinary(MAX)NULL,

Sencryptedgender varbinary(MAX)NULL,

Sencryptedaddress varbinary(MAX)NULL,

Sencrypteddob varbinary(MAX)NULL,

Sencrypteddoreg varbinary(MAX)NULL,

Sencryptednic varbinary(MAX)NULL,

Sencryptedmobile varbinary(MAX)NULL,

Sencryptedregamount varbinary(MAX)NULL,

Sencryptedconsamount varbinary(MAX)NULL,

Sencryptedtotamount varbinary(MAX)NULL,

Sencryptedrelwithrelative varbinary(MAX)NULL

go

Step 5: OPEN SYMMETRIC KEY DProtect1

DECRYPTION BY CERTIFICATE ThesisCertificate;

Step 6: OPEN SYMMETRIC KEY DProtect1

DECRYPTION BY CERTIFICATE ThesisCertificate;

set statistics time on

UPDATE patient_registration

set Sencryptedmrno=EncryptByKey(Key_GUID('DProtect1'), mrno),

Sencryptedfname =EncryptByKey(Key_GUID('DProtect1'), FirstName),

Sencryptedlname=EncryptByKey(Key_GUID('DProtect1'), lastname),

Sencryptedrlname =EncryptByKey(Key_GUID('DProtect1'), relativename),

Sencryptedgender=EncryptByKey(Key_GUID('DProtect1'), gender),

Sencryptedaddress =EncryptByKey(Key_GUID('DProtect1'),address),

Sencrypteddob=EncryptByKey(Key_GUID('DProtect1'), dateofbirth) ,

Sencrypteddoreg =EncryptByKey(Key_GUID('DProtect1'), dateofregistration),

Sencryptednic=EncryptByKey(Key_GUID('DProtect1'), nic),

Sencryptedmobile=EncryptByKey(Key_GUID('DProtect1'), mobileno) ,

Sencryptedregamount=EncryptByKey(Key_GUID('DProtect1'), regamount)

Sencryptedconsamount=EncryptByKey(Key_GUID('DProtect1'),consultamount),

Sencryptedtotamount=EncryptByKey(Key_GUID('DProtect1'), otalamount)

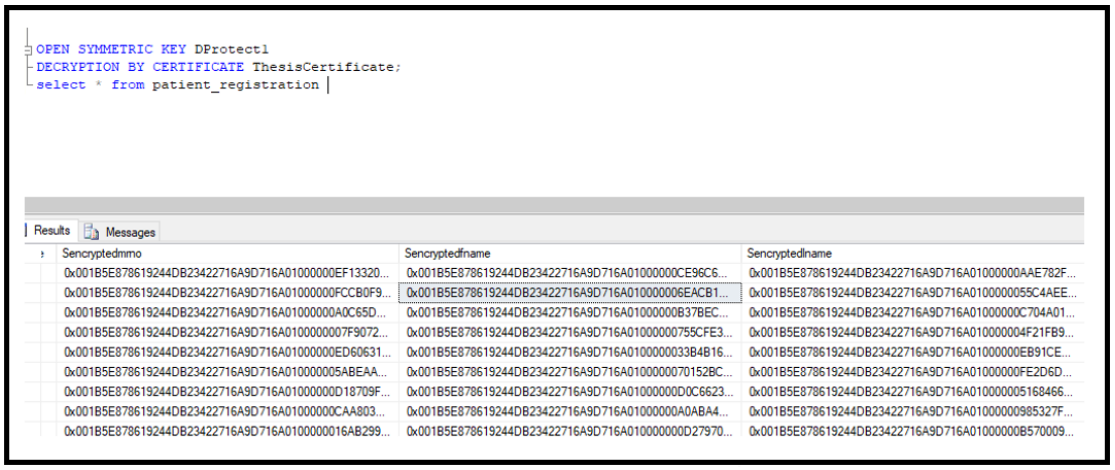

FIGURE 4.3: Encrypted form of Single data Encryption

Sencryptedrelwithrelative =EncryptByKey(Key_GUID('DProtect1'), relwithrelative)

Step 7: : Now the data will be saved in the database table in this format shown in Figure 4.3

4.4 Data Decryption Phase

Patient will visit the URL which is printed on registration slip. Patient will use the MR no as username, password and click on login. The below history of patient will be displayed in Figure 4.4 and Figure 4.5.

4.5 Result Analysis

In this section obtained results are compared with single and combined methods. Following graphs depicted in the Figure 4.6,Figure 4.7 and Figure 4.8 show the results of elapsed time, CPU time and Data storage capacity of different encrypted algorithms. **Elapsed Time** Figure 4.7 provide us the following elapsed time on 500 records with single encryption algorithms.

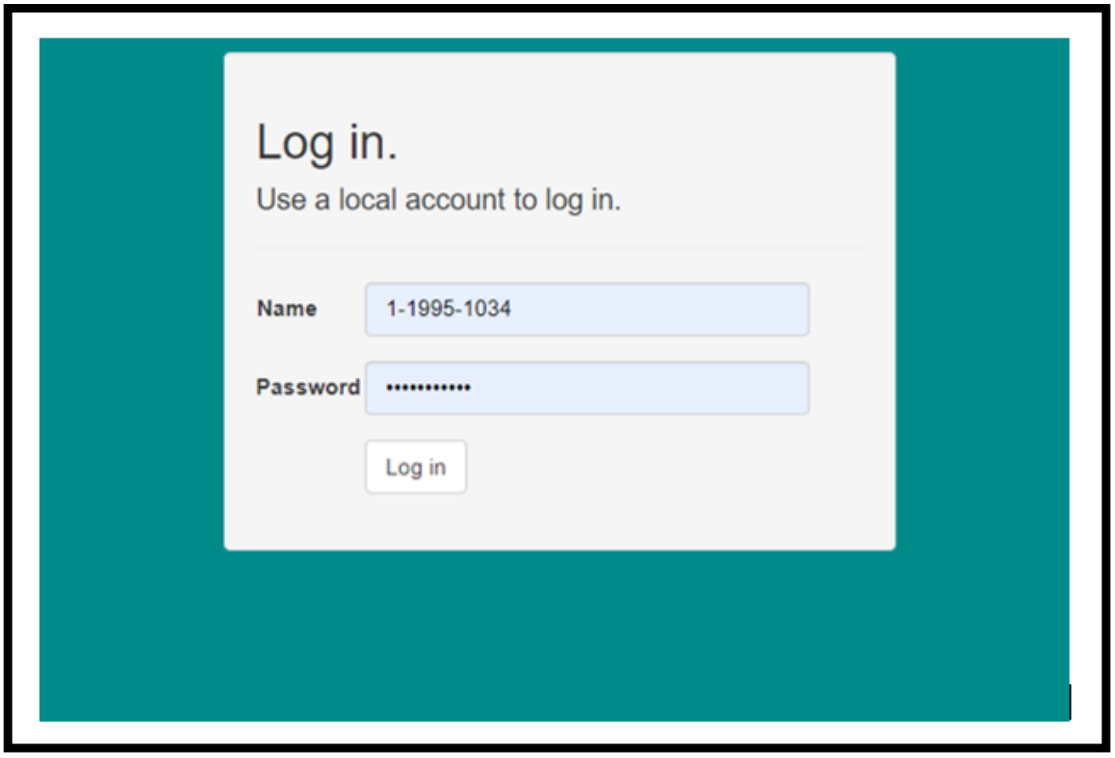

FIGURE 4.4: Login Screen for Patient Login

FIGURE 4.5: Medical Record Detail of a Patient

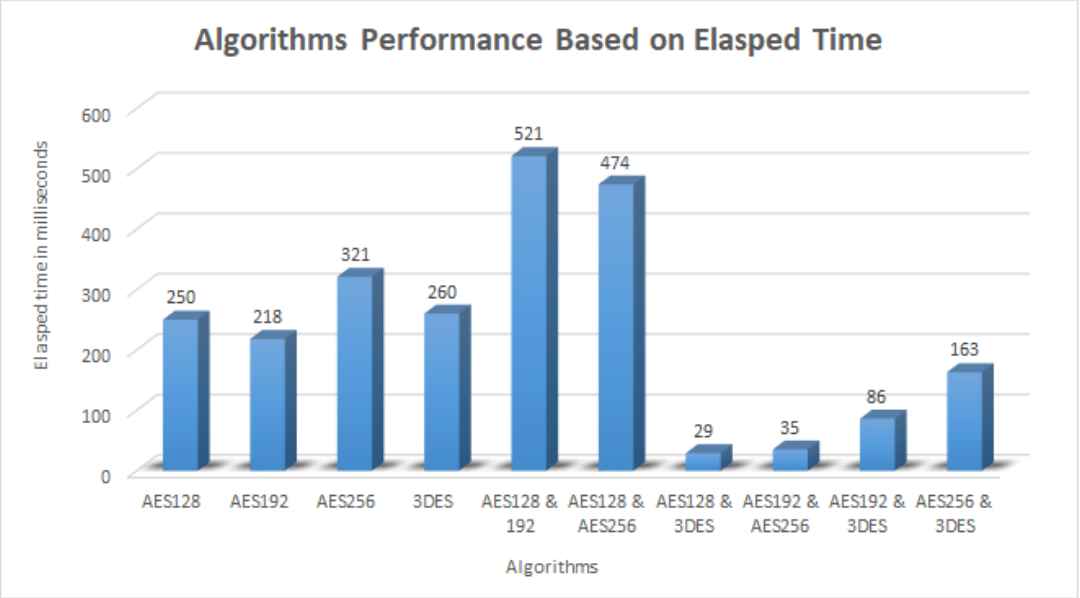

FIGURE 4.6: Graphical view of elapsed time of single and multilayer encryption Algorithms

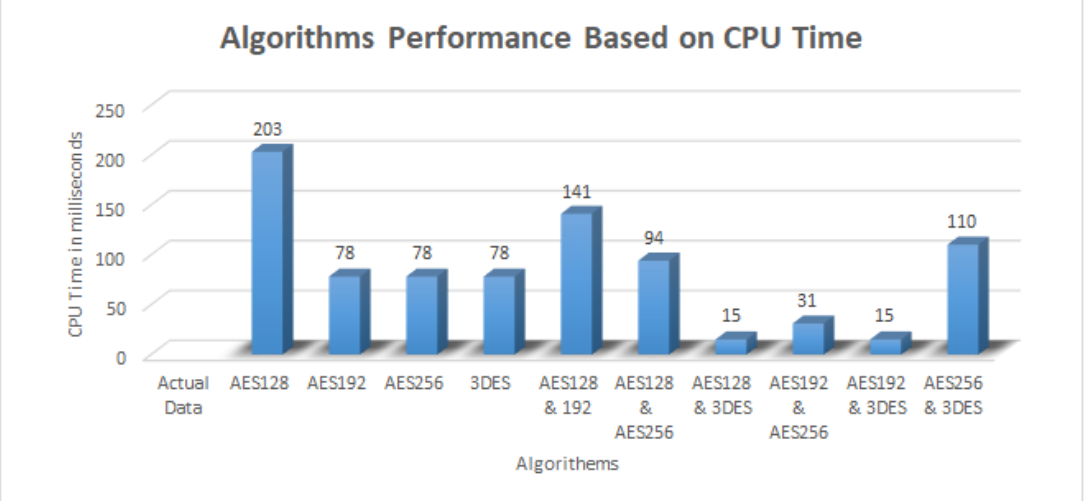

FIGURE 4.7: Graphical view of CPU Time of single and multilayer encryption Algorithms

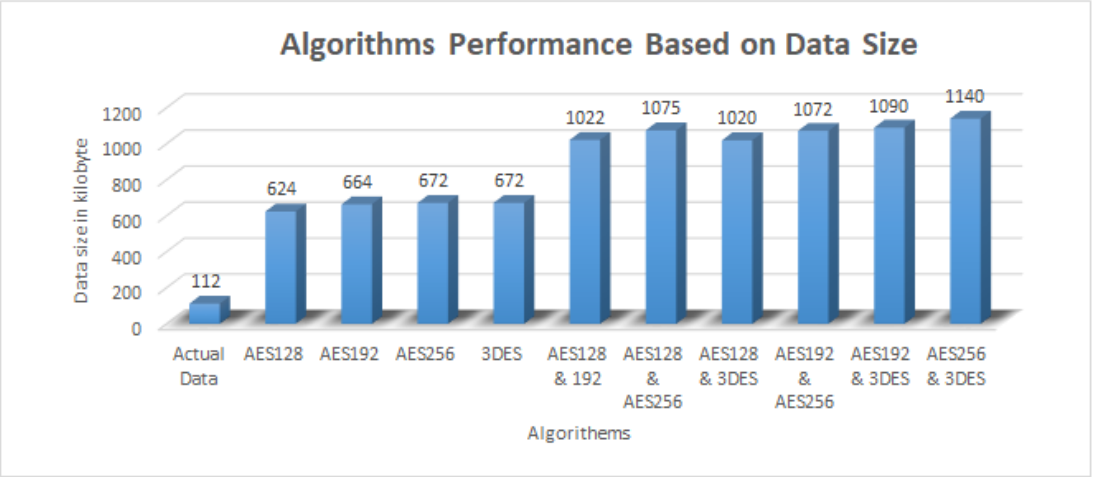

FIGURE 4.8: Graphical view of Database Table Size in KB After Encrypted data is stored in the RDBMS

- If the single encryption algorithem AES with 128 bit key size is applied than total elapsed time will be 250 milliseconds
- If the AES with 192 bit key size is applied than total elapsed time will be 21 milliseconds
- If the AES with 218 bit key size is applied than total elapsed time will be 321 milliseconds
- If the 3DES alone is applied than total elapsed time will be 260 milliseconds

Results of multiple combination of algorithms with same dataset is also shown in this figure

- If a combination of AES128 and 192 is used than elapsed time will be 521 milliseconds
- If a combination of AES128 and 256 is used than elapsed time will be 474 milliseconds
- If a combination of AES128 and 3DES is used than elapsed time will be 29 milliseconds

- If a combination of AES192 and AES256 is used than elapsed time will be 35 milliseconds
- If a combination of AES192 and 3DES is used than elapsed time will be 86 milliseconds
- If a combination of AES256 and 3DES is used than elapsed time will be 163 milliseconds

CPU Time Figure 4.8 provide us the following CPU time in milliseconds for 500 records with single encryption algorithms.

- AES128 takes CPU time of 203ms
- AES192 takes CPU time is 78ms
- AES256 takes 72ms
- 3DES takes 78ms

Results of CPU time for multiple combination of algorithms with same dataset is also shown in this figure

- AES128 and 192 takes 141ms
- AES128 and AES256 takes 94ms
- AES192 and AES256 takes 31ms
- AES192 and 3DES consumes 15ms
- AES256 and 3DES takes 110ms

Although the CPU time with AES256 and 3DES requires more CPU time but the elapsed time of AES256 and 3DES is providing a better scheme for multilayer approaches because encryption will only perform data is uploaded. For the best confidentiality level AES256 with 3DES is good.

TABLE 4.1: Comparison of Different algorithm Single and Combine 3DES and AES256

	Multilayer AES256 & 3DES	**Multilayer AES192 & 3DES**	**Multilayer AES128 & 3DES**	**3DES**	**AES256**
Confidentiality level [56]	High	Medium	Medium	Low	Low
Encryption & Decryption Speed [56]	Medium	Medium	Fast	Fast	Fast
No of Keys Uses [56]	Two Keys	Two keys	Two keys	Single key	Single Key
Possibility of Attack [56]	Very hard	Hard	Hard	Difficult	Difficult
Number of Rounds [56]	60	48	12	48	12
Key Length in Byte [56]	Varies	128, 192	256	128, 192	256

In Table 4.1 we have made a comparison of different algorithms with single and multiple layer. Confidentiality level is divided into three parts:

- Low
- Medium
- High

It is just like person who has a vehicle and when he parks his vehicle at some public location and use one single lock for safty. Then, his mind remains thinking that his vehicle may be stolen. That is showing his confidentiality level. Now in second scenario, Suppose he has another lock attached with that but its is less secure then he is more satisfied with first one level but a fear always remain under his mind that the car may be stolen. In third scenario, he has applied the two locks on his vehicle and both are very strong. Then his confidentiality level will become very high because of the methods which he has applied on it. Same is the case with patients and health organizations, if both have applied weak algorithm than patients and organization are always at risk. Consequences is that patient data might be loss. But if the data which is saved at cloud is encrypted with multiple algorithms then level of confidentiality will be very high. Second Row of the Table 4.1 is showing about the speed of the different algorithm. AES256 and 3DES speed is medium, AES192 and 3DES is also medium but the speed AES256 and 3DES singly is better than multilayer algorithms. The only a little bit disadvantage of 3DES algorithm is speed. Thats why when it is used with some other algorithm it also slow down the process. The reason behind is that 48 no of rounds in 3DES. Third row of Table 4.1 represent the key combination. Because of the key combination it is also increasing the confidence level because data is encrypted with multiple keys. In result, the multilayered approach has low in speed because of its layered encryption but high in approach of confidentiality.

4.6 Conclusion

In this chapter we have described these main points

- How we have taken the dataset for the experiments?
- How the encryption decryption will be performed on data?
- How experiment is performed on data?
- Analysis of Result and results of experiment is discussed.

Chapter 5

Conclusions and Future Work

5.1 Conclusions

Patient sensitive data protection is very challenging task because of security concern. From the comprehensive review of literature we have studied currently which techniques have been introduced. Finding new technique was also very challenging. We have found that multilayer encryption techniques can also be helpful for the protection of patient data. This approach Multilayer Encryption Model for Healthcare Data in Cloud Environment is implemented on patient data and effects are analyzed. Following advantages are achieved from suggested techniques are

- Data is secured by using multilayer techniques
- Additionally, Key management issue is resolved by using built-in method
- Confidentiality level is increase on cloud computing
- Patients gain confidence
- Cost effective
- Confidence level will enhanced on cloud computing

- Multilayered technique is also suitable for the other sectors where security of data is more concerned.
- Open new ways for the researchers to enhance confidentiality level.

5.2 Future Work

Following targets are set for future innovations:-

- Selection of encryption algorithm on random bases
- More industries standards algorithm will be added
- Encryption speed increase
- Implementation of multilayer algorithm on patient image based data

Bibliography

[1] Son, Ha Xuan, Minh Hoang Nguyen, and Hong Khanh Vo., "Toward an privacy protection based on access control model in hybrid cloud for healthcare systems.", *10th International Conference on EUropean Transnational Education (ICEUTE 2019)*, 2019.

[2] S. M and Altowaijri, "An architecture to improve the security of cloud computing in the healthcare sector," in *Smart Infrastructure and Applications*. Springer, pp.249–266,2020.

[3] "https://tutorialspoint.com/cloud-computing/cloud-computing-overview.htm/"

[4] "https://timesofcloud.com/cloud-tutorial/characteristics-of-cloud-computing-as-per-nist/"

[5] F. Gao, S. Thiebes, and A. Sunyaev, "Rethinking the meaning of cloud computing for health care: A taxonomic perspective and future research directions," *Journal of medical Internet research*, vol. 20, no. 7, p. e10041, 2018.

[6] Z. Yan, R. H. Deng, and V. Varadharajan, "Cryptography and data security in cloud computing," 2017.

[7] T. M. Damico, "A brief history of cryptography," *Inquiries Journal*, vol. 1, no. 11, 2009.

[8] "https://www.garykessler.net/library/crypto.html/ "

[9] Babatunde, A. O., A. J. Taiwo, and E. G. Dada., "Information Security in Health Care Centre Using Cryptography and Steganography.," *arXiv preprint arXiv:1803.05593*,2018.

[10] J. K. Oherrin, N. Fost, and K. A. Kudsk, "Health insurance portability accountability act (hipaa) regulations: effect on medical record research," *Annals of surgery*, vol. 239, no. 6, p. 772, 2004.

[11] R. Sulaiman, D. Sharma, W. Ma, and D. Tran, "A new security model using multilayer approach for e-health services," *Journal of Computer Science*, vol. 7, no. 11, pp. 1691–1703, 2011.

[12] K. Sudheep and S. Joseph, "Review on securing medical big data in healthcare cloud," in *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*. IEEE, 2019, pp. 212–215.

[13] V. S. V. Hema and R. Kesavan, "Ecc based secure sharing of healthcare data in the health cloud environment," *Wireless Personal Communications*, vol. 108, no. 2, pp. 1021–1035, 2019.

[14] M. M. Kiah, M. S. Nabi, B. Zaidan, and A. Zaidan, "An enhanced security solution for electronic medical records based on aes hybrid technique with soap/xml and sha-1," *Journal of medical systems*, vol. 37, no. 5, p. 9971, 2013.

[15] E. Shanmugapriya and R. Kavitha, "Medical big data analysis: preserving security and privacy with hybrid cloud technology," *Soft Computing*, vol. 23, no. 8, pp. 2585–2596, 2019.

[16] F. Shahbodin, A. Azni, T. Ali, and C. K. N. C. K. Mohd, "Lightweight cryptography techniques for mhealth cybersecurity," in *Proceedings of the 2019 Asia Pacific Information Technology Conference*, 2019, pp. 44–50.

[17] D. He, N. Kumar, J.-H. Lee, and R. S. Sherratt, "Enhanced three-factor security protocol for consumer usb mass storage devices," *IEEE Transactions on Consumer Electronics*, vol. 60, no. 1, pp. 30–37, 2014.

[18] K. Renuka, S. Kumari, and X. Li, "Design of a secure three-factor authentication scheme for smart healthcare," *Journal of medical systems*, vol. 43, no. 5, p. 133, 2019.

[19] S. A. Parah, A. Bashir, M. Manzoor, A. Gulzar, M. Firdous, N. A. Loan, and J. A. Sheikh, "Secure and reversible data hiding scheme for healthcare system using magic rectangle and a new interpolation technique," in *Healthcare Data Analytics and Management*. Elsevier, 2019, pp. 267–309.

[20] L. Zhou, V. Varadharajan, and K. Gopinath, "A secure role-based cloud storage system for encrypted patient-centric health records," *The Computer Journal*, vol. 59, no. 11, pp. 1593–1611, 2016.

[21] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. Rodrigues, "Authentication in cloud-driven iot-based big data environment: Survey and outlook," *Journal of Systems Architecture*, vol. 97, pp. 185–196, 2019.

[22] K. J. Modi and N. Kapadia, "Securing healthcare information over cloud using hybrid approach," in *Progress in advanced computing and intelligent engineering*. Springer, 2019, pp. 63–74.

[23] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan, and B. Balusamy, "Securing data in internet of things (iot) using cryptography and steganography techniques," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, pp. 73–80, 2019.

[24] H. Jin, Y. Luo, P. Li, and J. Mathew, "A review of secure and privacy-preserving medical data sharing," *IEEE Access*, vol. 7, pp. 61 656–61 669, 2019.

[25] Y. S. Lee, E. Alasaarela, and H. J. Lee, "An efficient encryption scheme using elliptic curve cryptography (ecc) with symmetric algorithm for healthcare system," *International journal of security and its applications*, vol. 8, no. 3, pp. 63–70, 2014.

[26] P. D. Nayana Banjan, "Medical data security using combination of cryptography and steganography with aes-lsb algorithm," International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), Tech. Rep.

[27] G. Garkoti, S. K. Peddoju, and R. Balasubramanian, "Detection of insider attacks in cloud based e-healthcare environment," in *2014 International Conference on Information Technology*. IEEE, 2014, pp. 195–200.

[28] Y. M. Essa, E. E.-D. Hemdan, A. El-Mahalawy, G. Attiya, and A. El-Sayed, "Ifhds: Intelligent framework for securing healthcare bigdata," *Journal of medical systems*, vol. 43, no. 5, p. 124, 2019.

[29] A. M. Elmisery and H. Fu, "Privacy preserving distributed learning clustering of healthcare data using cryptography protocols," in *2010 IEEE 34th Annual Computer Software and Applications Conference Workshops*. IEEE, 2010, pp. 140–145.

[30] A. M. Badr, Y. Zhang, A. Umar, and H. Gulfam, "Dual authentication-based encryption with a delegation system to protect medical data in cloud computing," *Electronics*, vol. 8, no. 2, p. 171, 2019.

[31] Jammu, Aashmeen, and Harjinder Singh, "Improved AES for Data Security in E-Health IEEE," *International Journal of Advanced Research in Computer Science 8.5* 2017.

[32] K.-L. Tsai, Y.-L. Huang, F.-Y. Leu, I. You, Y.-L. Huang, and C.-H. Tsai, "Aes-128 based secure low power communication for lorawan iot environments," *IEEE Access*, vol. 6, pp. 45 325–45 334, 2018.

[33] A. Michalas and N. Weingarten, "Healthshare: Using attribute-based encryption for secure data sharing between multiple clouds," in *2017 IEEE 30th International Symposium on Computer-Based Medical Systems (CBMS)*. IEEE, 2017, pp. 811–815.

[34] A. Michalas, N. Paladi, and C. Gehrmann, "Security aspects of e-health systems migration to the cloud," in *2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom).* IEEE, 2014, pp. 212–218.

[35] H. Asri, H. Mousannif, H. Al Moatassime, and T. Noel, "Big data in healthcare: Challenges and opportunities," in *2015 International Conference on Cloud Technologies and Applications (CloudTech).* IEEE, 2015, pp. 1–7.

[36] J. Oltsik, "Vormetric/ESG Insider Threat Report: Profile on HealthCare, 2014, pp. 1–7.

[37] V Mahalakshmi, S Satheeshkumar and Dr. S Sivakumar, "Performance of steganographic methods in medical imaging, *International Journal of Computational and Applied Mathematics* Vol. 12, no. 1, pp 549-556,2017.

[38] PratikshaSethi and V Kapoor, "A Secured System for Information Hiding in Image Steganography using Genetic algorithm and Cryptography, *International Journal of Computer Applications, Vol. 144, No. 9Et.al.*,2016.

[39] "Steganography and cryptography approaches combined using medical digital images," *International Journal of Engineering Research & Technology (IJERT)*, vol. 4, 2015.

[40] J. L. Pan, S. P. Li and D. Y. Zhang, A Study of two algorithms based on feistel cipher in wireless medical sensor networks (in Chinese), *Chinese J. Sens. Actuators*, vol. 23, pp. 1030-1036,2010

[41] C. Jiang, B. Li, and H. Xu, "An efficient scheme for user authentication in wireless sensor networks," IEEE, pp. 438–442, 2007.

[42] L. Chen and D. B. Hoang, "Novel data protection model in healthcare cloud," IEEE, pp. 550–555, 2011.

[43] S. Narayan and M. Gagn, and R. Safavi-Naini, Privacy preserving EHR system using attribute-based infrastructure,in Proc. ACM Workshop Cloud Comput. Secur. Workshop. New York, NY, USA: ACM, pp. 4752.,2010

[44] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," pp. 11 676–11 686, 2018.

[45] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, Scalable and secure sharing of personal health records in cloud computing using attributebased encryption, *IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1*, pp. 131143, Jan. 2013.

[46] H. Kaur, H. P. S. Gill, and D. Sarmah, "Multiphase and multiple encryption," IEEE, pp. 1–8.

[47] Kumar, Vishal, et al. "Multiple Encryption using ECC and its Time Complexity Analysis." International Journal of Computer Engineering In Research Trends 3.11, pp. 568-572, 2016.

[48] Tebaa, Maha, and Said El Hajji., "Secure cloud computing through homomorphic encryption." empharXiv preprint arXiv:1409.0829, (2014).

[49] Sarhan, Akram, and LeszekLilien, "An Approach to Identity Management in Clouds without Trusted Third Parties." empharXiv preprint arXiv:1904.00880, (2019).

[50] R. Arora, A. Parashar, and C. C. I. Transforming, "Secure user data in cloud computing using encryption algorithms," pp. 1922–1926, 2013.

[51] Padhy, Rabi Prasad, ManasRanjanPatra, and Suresh Chandra Satapathy, "Cloud computing: security issues and research challenges.", "International Journal of Computer Science and Information Technology and Security (IJCSITS) 1.2", : pp. 136-146,2011.

[52] M. S. Abolghasemi, M. M. Sefidab, and R. E. Atani, "Using location based encryption to improve the security of data access in cloud computing," IEEE, pp. 261–265, 2013.

[53] Albugmi, Ahmed, et al., "Data security in cloud computing.", 2016 Fifth International Conference on Future Generation Communication Technologies (FGCT). IEEE, 2016.

[54] V. Gampala, S. Inuganti, and S. Muppidi, "Data security in cloud computing with elliptic curve cryptography," pp. 138–141, 2012.

[55] Ahamed, Farhad, SeyedShahrestani, and AthulaGinige., "Cloud computing: security and reliability issues.", Communications of the IBIMA 2013, 2013.

[56] Babatunde, AO and Taiwo, AJ and Dada, EG, "Information Security in Health Care Centre Using Cryptography and Steganography", arXiv preprint arXiv:1803.05593, 201.