A SECURED HYBRID CRYPTOGRAPHIC SCHEME & TWO-FACTOR AUTHENTICATION PROTOCOL FOR CLOUD-BASED TELECARE MEDICAL INFORMATION SYSTEM

Thesis submitted to the SASTRA Deemed to be University
in partial fulfillment of the requirements
for the award of the degree of

B. Tech Computer Science and Engineering

Submitted by

NALLAMILLI SIVA RAMA REDDY
(Reg. No.: 120003200)
TIPPARAJU VENKATA LAKSHMI SASANK
(Reg. No.: 120003332)

May 2020

SCHOOL OF COMPUTING

THANJAVUR, TAMIL NADU, INDIA-613 401

SASTRA

ENGINEERING · MANAGEMENT · LAW · SCIENCES · HUMANITIES · EDUCATION

DEEMED TO BE UNIVERSITY

(U/S 3 OF THE UGC ACT, 1956)

THINK MERIT | THINK TRANSPARENCY | THINK SASTRA

SCHOOL OF COMPUTING

THANJAVUR, TAMIL NADU, INDIA-613 401

Bonafide Certificate

This is to certify that the thesis titled “ **A Secured Hybrid Cryptographic Scheme & Two-Factor Authentication Protocol for Cloud-Based Telecare Medical Information System** ” submitted in partial fulfillment of the requirements for the award of the degree of B. Tech. Computer Science and Engineering to the SASTRA Deemed to be University, is a bona-fide record of the work done by **Mr. NALLAMILLI SIVA RAMA REDDY** (Reg. No. 120003200) **Mr. TIPPARAJU VENKATA LAKSHMI SASANK** (Reg. No. 120003332) during the final semester of the academic year 2019-20, in the **School of Computing**, under my supervision. This thesis has not formed the basis for the award of any degree, diploma, associateship, fellowship, or other similar title to any candidate of any University.

Signature of Project Supervisor :

Name with Affiliation :

Date :

Project *Viva Voice* to be held on ________________

Examiner 1 **Examiner 2**

SASTRA

ENGINEERING · MANAGEMENT · LAW · SCIENCES · HUMANITIES · EDUCATION

DEEMED TO BE UNIVERSITY

(U/S 3 OF THE UGC ACT, 1956)

THINK MERIT | THINK TRANSPARENCY | THINK SASTRA

SCHOOL OF COMPUTING

THANJAVUR, TAMIL NADU, INDIA - 613 401

Declaration

We declare that the thesis titled “**A Secured Hybrid Cryptographic Scheme & Two-Factor Authentication Protocol for Cloud-Based Telecare Medical Information System**” submitted by us is an original work done by me under the guidance of **Dr. Dindayal Mahto, AP-III, School of Computing, SASTRA Deemed to be University** during the final semester of the academic year 2019-20, in the **School of Computing**. The work is original and wherever we have used materials from other sources, we have given due credit and cited them in the text of the thesis. This thesis has not formed the basis for the award of any degree, diploma, associate-ship, fellowship or other similar title to any candidate of any University.

Signature of the candidate(s) **:**

Name of the candidate(s) **:**

Date **:**

Acknowledgements

First and foremost, I thank the almighty for helping me to gain support in all forms to finish my project successfully. I express my sincere thanks to **Dr. S.Vaidhyasubramaniam**, Vice Chancellor and **Prof. R. Chandramouli,** Registrar, SASTRA Deemed to be University, for permitting me to do this project as a part of my curriculum.

I express our profound gratitude to **Dr. Umamakeswari A,** Dean and **Dr. Shankar Sriram** Associate Dean, School of Computing, SASTRA Deemed to be University for their complete support throughout the Project.

I am fortunate to have, **Dr. Dindayal Mahto**, AP-III School of Computing SASTRA Deemed to be University, as my project guide. His valuable assistance and supervision guided me towards the successful completion of my project.

I would like to thank all our internal panel members for feedback and their constructive criticism which helped me improve. Their support, guidance, valuable information and making the entire process a smooth one.

Lastly I thank all the technical and non-technical staffs of Computer Science department and my parents and friends for their constant support throughout the completion of my project report.

Contents

List of Figures

List of Tables

Nomenclature

Abbreviations

TMIS	Telecare Medical Information System
ECC	Elliptic Curve Cryptography
ECDH	Elliptic-curve Diffie–Hellman
AES	Advanced Encryption Standard
GCM	Galois/Counter Mode
AAD	Additional Authenticated Data
IV	Initialization Vector
DES	Data Encryption Standard
SHA	Secure Hash Algorithm
MD5	Message-Digest algorithm 5
RSA	Rivest, Shamir, Adleman
ECB	Electronic Code Book
CBC	Cipher Block Chaining

Abstract

Lately, we know how technology plays a crucial role in numerous fields and also in the healthcare zone. Users can simply obtain healthcare functionalities through the net. It reduces any possibility of transmitting viral diseases from a patient to the doctors with low cost, and saves time remarkably. Accounting sensitivity of the health information, to obstruct the people factor attacks, the healthcare institutions need to adopt strong user authentication and security protocols while managing the account holder details. The main objective of the project "A Secured Hybrid Cryptographic Scheme & Two-Factor Authentication Strategy for Cloud-Based Telecare Medical Information System" is to provide strong user authentication and healthcare information security over the cloud.

So, we've developed an application that's employed in the agreement to all or any of the standards to prevent risks and supply utmost data security with two-factor authentication protocol (login and OTP) in the system, which is that the combination of an asymmetrical crypto algorithm (ECDH) for key exchange and agreement protocol and symmetric crypto algorithm (AES-GCM) for encryption and decryption to share data safely. When compared with previous paperwork (Kumar, Ahmad, & Kumari, 2019) the encryption completely is done with ECC. One of the primary disadvantages of ECC is that it escalates the size of the enciphered message unusually and quantum attacks loom over ECC and other is encryption, decryption process takes longer compared to symmetrical.

Conclusively the improved protocol is more effective based on computation time and memory usage. It has a well-built reliability protocol with a two-factor authentication scheme together with a symmetric encryption technique that is strong against various security attacks, satisfies avalanche effect, and is claimed to be quantum-safe.

Specific Contribution

- Interface design, Key Agreement protocol, Encryption, Decryption algorithm, and Documentation

Specific Learning

- Cryptographic Algorithms, Android Application and Firebase Cloud Storage.

Keywords: Telemedicine, Data security, Cloud, Cryptographic Algorithms, Authentication.

CHAPTER 1

INTRODUCTION

1.1 WHAT IS TELECARE MEDICAL INFORMATION SYSTEM?

Recently, we have noticed the rapid growth in technology and how it plays a crucial role in numerous fields and identified benefits associated with it. Lately, it also enters into the medical field. The innovation of technology in the health zone, popularly known as eHealth, is developing as one of the most vastly growing fields in healthcare today. One of the healthcare services is telemedicine, which provides easier communication between doctors and patients in remote areas. Telecare Medical Information System using in almost all advanced countries to provide treatment to patients remotely. The existing method requires doctors or patients to visit each other to get or provide treatment. But TMIS does not require any manual visits for treatment as the hospital will register patient and embed the sensor in patient body and that sensor monitor patient health condition and report to patient mobile and patient mobile will report to concern hospital. Hospital people will analyze that data and send require a prescription to patient mobile upon abnormal conditions detected. All medical data of patients will be store at cloud servers and this data can be accessed.

1.1.1 The Impact of Technology in Health Care

With the help of mobiles, patients can easily acquire healthcare services online. It's become more effortless to keep up, supervise, and track several medical phases like medicine intake, remedy for the disorder. Additionally, it also gets to eliminate any possibility of transmitting infectious diseases from a patient to the healthcare providers. It also reduces costs and saves patients time remarkably. Healthcare professionals must possess a sturdy and authentic network security solution on account of its sensitivity to healthcare information in cloud storage.

1.2 CRYPTOGRAPHY BASICS

Cryptography is a research area of the strategy of working algorithms for safeguarding information. It is a course of action permutes file into a secure scribbled format. Using these algorithms, we can deploy a cryptosystem that is competent in the event of information security. Confidentiality, integrity, and availability (CIA) is a triad model that’s framed to assist the policies and principles for data security enclosed within an organization.

1.2.1 The Basic Principles of Cryptography

- Encryption is utilized for information privacy to comprehend confidentiality. It is the method of encoding information. It is process of transforming the primary data (plaintext) into an alternate form called ciphertext, so that only certain authorized people can decode the ciphertext back and access the primary data.

- Authentication is another important principle of cryptography. It’s the strategy of justify the individuality of a process or user.
- Integrity ensures the accuracy and completeness of knowledge. It signifies to safeguard the data from being customized or misused by an unauthorized party.

1.2.2 Types of Cryptography

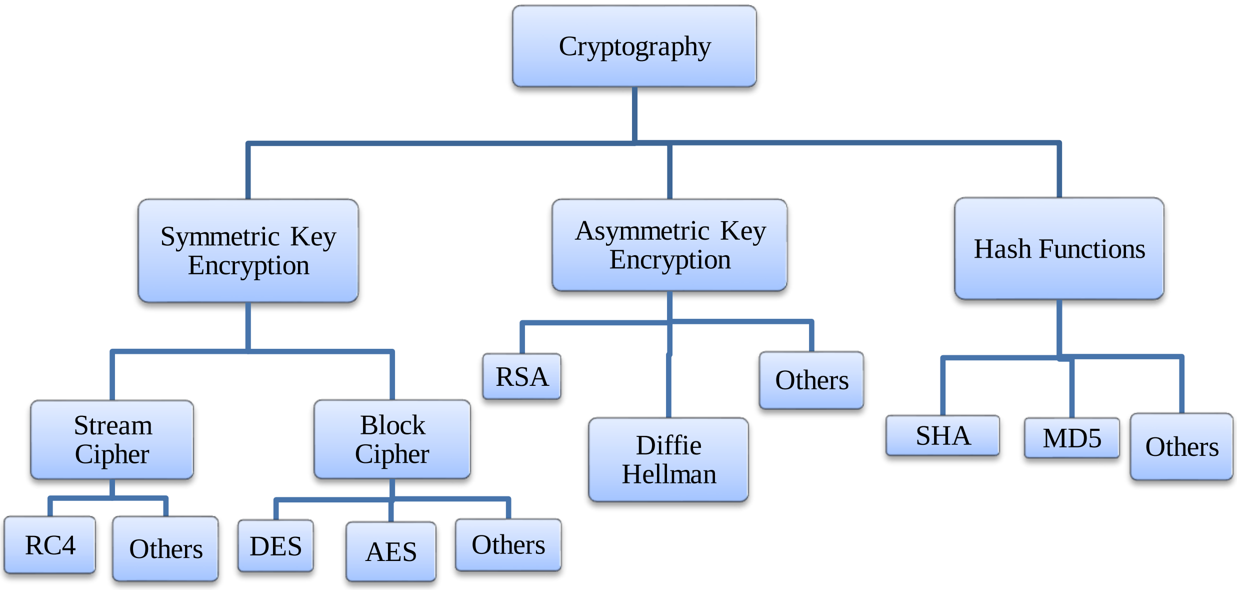


Figure 1.1 Layered Cryptographic Methods

1. **Secret Key Cryptography** also exclaimed as symmetric-key cryptography that handles one key for both encoding and decoding. Administration of keys among the parties is the greatest drawback with this system. This algorithm makes use of 1 key for both encryption and decryption a variety of the algorithms are DES, AES

2. **Public Key Cryptography** is also remarked as asymmetric-key cryptography. It handles 2 keys for encipher and decipher procedure in which connection can occur between receiver and sender in an exceedingly secured channel. During this process, each user incorporates a public key and a non-public key (private). The private key is hidden and is not revealed to other users while the public key is open to all sources of users you would like to connect. If a party desires to convey information to another, then he encodes the data with other party’s’ public key and sends it in an exceedingly

secure path. Meanwhile the other end user can decode the ciphered info together with his non-public key to access original data variety of the algorithms are RSA, ECC

3. **Hash Functions.** It does not handle any key either public or private. It uses hash functions that encode the incoming part of the text into a fixed hash value that is mathematically calculated. These functions are accustomed to check the integrity of the info provided by user and also ensure the text in communication channel has no interruptions by attackers. A variety of the algorithms are SHA, MD5

1.3 SOFTWARE SPECIFICATION

Windows (7 or Later)
Developing Language: Java Standard edition 8 or above
Storage: Firebase Database
Tools: Android Studio or Eclipse and Android SDK Tool

1.4 MOTIVATION

About 27 million patients were affected because of a security breach and IT incidents caused by attackers in the medical industries in 2019. To forestall the human factor attacks the medical management has to gain reliable account holder authentication and security protocols when acquiring the account holder’s data within the cloud storage with the assistance of an IT zone

CHAPTER 2

OBJECTIVES

2.1 PROBLEM STATEMENT

TMIS application provides a patient to access his health information through chips embedded in the body and stored in the cloud server. The healthcare professionals who are authorized by admin will access the patient data to provide proper treatment like medicine intake. We all know how crucial the patient information is and even a small change in data leads to fatal damage to him/her respectively.

Basic architecture of application is given below Figure 2.1 and different phases are explained

2.1.1 Admin Phase

In this phase, the admin registers the patient at the hospital and will store patient details. Each patient provided with login credentials as an authorized user. The admin can manage doctors and patients by adding or removing them from authorization

2.1.2 Patient Information Transmit Phase

In this phase, the patient sensor will read patient body data and send it to the mobile and mobile send to the hospital. Here we don't have sensors so we will write values in the application

2.1.3 Treatment Phase

In this phase, the doctor authenticates with the cloud by using his credentials given by admin and allows to access patient data for providing treatment

2.1.4 Checkup Phase

In this phase, the patient authenticates himself with the cloud. After verified, the patient can view his records and doctor prescription

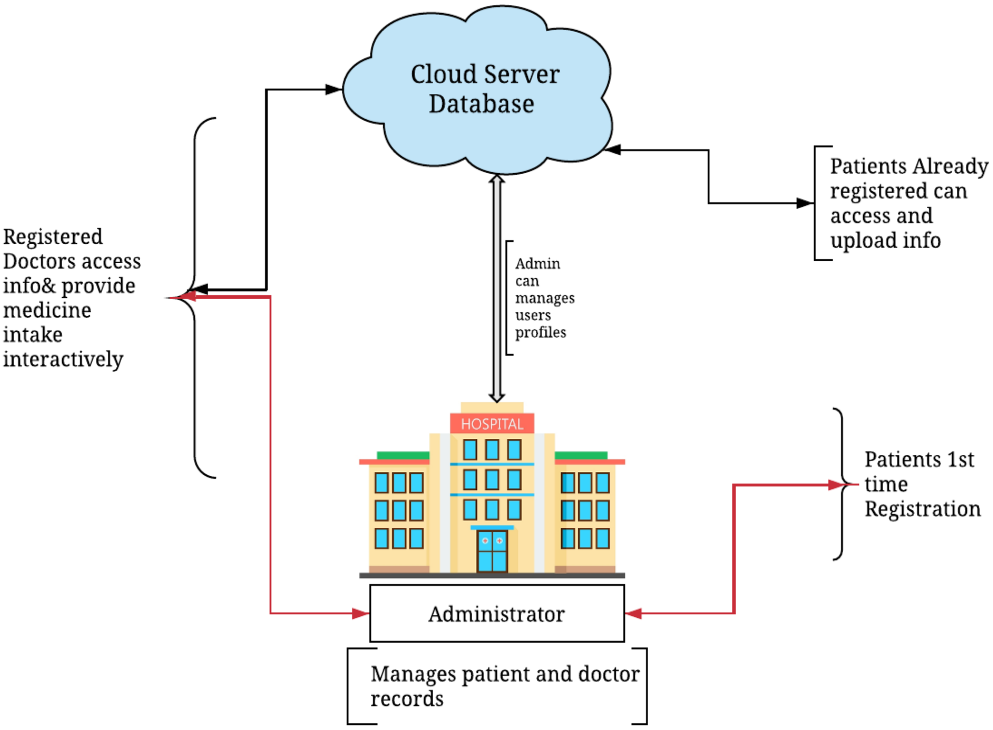

Cloud Server Database
Registered Doctors access info& provide medicine intake interactively
Admin can manages users profiles
Patients Already registered can access and upload info
HOSPITAL
Patients 1st time Registration
Administrator
Manages patient and doctor records

Figure 2.1 Architecture of TMIS model

Assumptions and Importance of Confidentiality, Authentication, Integrity in TMIS

- If a third party accessed the data storage and able to manage the health information then it may cost the patient's life since attackers can modify or misuse the data in the black market

Providing strong authentication along with authorization and (data authenticity) integrity is one of main objective required for healthcare services.

- The attackers may also try to breach the data whenever a user tries to upload it into a cloud server. He may attack the communication channel in the middle to get classified information regarding the user
  Providing strong encoding and decoding security protocols for the users to share data in a secured communication channel.

So we have to provide strong user authentication so that third party or unauthorized people cannot access the specified information and the best encryption security protocols to forestall the attackers in the middle of communication. This results in healthcare professionals to provide an efficient remedy for the respective disorders to users.

CHAPTER 3

LITERATURE SURVEY

This section will have all the details of the research work done in Hybrid Encryption techniques

Recently they have proven that by using a hybrid encryption algorithm we can improve the security of the message, by combining encryption techniques the confidentiality of the information and security increases with less complexity (Patel & Panchal, 2014). His work gave us an idea to combine various encryption techniques rather than using a single encryption technique. He compared the RSA algorithm with the combination of RSA and Diffie Hellman algorithm in terms of complexity and time. By looking at the encryption and decryption time comparison tables he provided for RSA vs RSA and Diffie Hellman, we can say that hybrid encryption time is less and more convenient. It also makes it more difficult for the intruder to find the plain text from the ciphertext in a secured communication channel. He used the RSA algorithm for providing security of message (encryption and decryption) and Diffie Hellman algorithm to generate a secret key for the sender and receiver for the communication. He also added XOR operation to increase the secured complexity of the message [5].

One more protocol proposes the hybrid encryption technique by using AES and ElGamal and also provides a good comparison between all three algorithms (AES, ElGamal, Hybrid AES, and ElGamal), the comparison has been made to support these parameters: Encryption Time, Decryption Time, and Throughput by taking various sizes of information (Rani & Kaur, 2017). These results show that Hybrid AES and ElGamal is more suitable than employing a single algorithm [6].

Focuses on the Hybrid ECC-AES approach for improved cloud storage security since ECC provides fast generating keys and the AES algorithm is extremely time-efficient, requires less computation and memory space (kajal & Gulshan, 2018). He used the AES algorithm for higher security. In combination, it gives a complex system for the eavesdropper. It also provided comparison results between AES and hybrid AES-ECC algorithms by considering the encryption and decryption factors by various key sizes like 64,128,192,256 bits where AES algorithm takes the biggest encryption and decryption time than Hybrid AES-ECC algorithm on all the various key sizes [3]

(Sharma & Chopra, 2016), Provided the analysis of AES encryption with ECC, he used AES algorithm for encryption and decryption and ECC for key generation and also provided the analysis of AES encryption with ECC supported various parameters like storage requirement, avalanche effect, correlation, encryption time and decryption and therefore the obtained results illustrate that the hybrid approach is healthier than other algorithms [8].

Some well-known cryptographic techniques are discussed and proved the importance of every algorithm with comparisons, results had shown that AES is that the best algorithm of symmetric encryption technology, AES is safer than the Blowfish algorithm but Blowfish gives more throughput compared to other algorithms (Shaikh & Kaul, 2014). So hybrid AES and Blowfish algorithm is powerful against vulnerabilities.ECC provides the very best strength-per-bit compared to the other algorithm with smaller key size ends up in faster communications, low power consumption, and low memory and it also provides high speed, efficient and scalable implementation of protocols for authentication and key agreement.ECC with Diffie Hellman called ECDHA solves the key exchange problem. Another feature of ECC is that the digital signature called the ECDSA algorithm. These prove that one or more cryptographic algorithms will be used per the necessity and finding out the simplest algorithms for our problem [7].

(Bommala, Kiran, Pujitha, & Reddy, 2019) They used a hybrid AES -ECC algorithm for the cloud environment used AES-192 algorithm for encryption and decryption of files and ECC with Diffie Hellman to get the key.ECC is employed to secure communication from external risks. Comparison supported file encryption size, encryption time, decryption time, and correlation proved that AES -ECC is extremely safe, secure, and difficult to interrupt [1]

Earlier we have worked on a thesis (Kumar, Ahmad, & Kumari, 2019) in which the ECC encryption technique is used. ECC mechanism works well in generating secret keys but increases the size of the encrypted message, more complex and difficult to implement. These drawbacks of the ECC mechanism made us a step forward and look to hybrid cryptography. So we chose ECDH for generation and exchange of secret keys and AES-GCM for encryption and decryption [4].

CHAPTER 4

METHODOLOGY

4.1 PROPOSED METHOD

After researching through various papers and books, we have classified the advantages and disadvantages of symmetric and asymmetric algorithms. So that we can propose an hybrid algorithm which comprises of both techniques in developing a cryptosystem which is strong against various kinds of attacks and best efficient solution in terms of computation time and memory usage.

4.1.1. Objectives to overcome from Previous Model

- To provide a robust authentication protocol to limit access for unauthorized users and third parties may be done employing a two-factor authentication protocol. Two-Factor authentication protocol comprises authorized login credentials and OTP as a one-time password that is a token sent to the registered mobile number of the user
- To provide a robust and safe connection for information transmit via secured channels, we will use the most effective cryptographic algorithm supported client requirements based on computation time, expenses, and memory capacity that are suitable for organizational goals in their environment.

4.1.2 Important Characteristics of Symmetric and Asymmetric Techniques

Advantages of Symmetric Encryption and Asymmetric Encryption with respective to each other

- Symmetric encryption is very swift and more effective for enciphering huge amounts of data compared to asymmetric encryption. Since asymmetric process recommended to utilize more number of CPU cycles than symmetric process.
- Symmetric encryption, more specifically AES is quantum-resistant till now whereas asymmetric techniques are not strong against quantum computing
- The symmetric algorithms are having trouble in key transmission compared to public-key encryption techniques. Because the secret key in the symmetric encryption process should be transmitted in a secure channel for encryption and decryption between two end-users. The attackers try to breach and acquire the knowledge of an ephemeral key in the middle of the transaction. But in asymmetric encryption, there is no prerequisite for key distribution. Using the Diffie Hellman method, both users can calculate the shared ephemeral key.
- Compared to Symmetric key generation, the asymmetric algorithm can generate keys very fast like ECC.
- As in Table 4.1, we can see that AES 256 bit key size gives the same level of security bit(256) compared with ECC 512 bit key

Table 4.1 Security Level vs. key size recommended by (Elaine, 2006) NIST [2].

Security Bit Level	AES Key Size	ECC Key Size	RSA Key Size
112	NA	224	2048
128	128	256	3072
192	192	384	7680
256	256	512	15360

Since each of symmetric and asymmetric cryptographic algorithms has its advantages and disadvantages, we suggest a modern secured data transfer using both the techniques in the coming days. A hybrid cryptosystem comprises key derivation protocol using asymmetric techniques and the complete encryption and decryption process with the help of symmetric algorithms. We can use hash functions for message authenticity.

4.1.3 Enhancements

Based on advantages and disadvantages of both symmetric and asymmetric algorithms, we propose an algorithm which is combination of for key agreement protocol to derive a secured secret key on their own and using that secret key AES-GCM encryption and decryption is done to provide maximum security with less complexity and time consumption and more efficiently. Thus the proposed hybrid cryptosystem is strong against all security attacks and quantum resistant and also follows all the principles of cryptography triad model (Confidentiality, Integrity, and Availability).

4.2 KEY AGREEMENT PROTOCOL

4.2.1 Elliptic Curve Cryptography Basics

It is a public-key cryptosystem that uses two keys for processing. It is supported by the elliptic curve theory which can be utilized to rapidly fabricate tiny and more potential keys over a finite group. Due to the massive accumulation of prime numbers, most of the asymmetric cryptosystems took longer for the key spawning process. But with the aid of elliptic curves and their mathematical calculations over fields, spawning of keys through the components and properties of the elliptic curve equation has become easier and productive

Definition: According to the Weierstrass equation, an elliptical curve as in Figure 4.1 can be defined as a collection of points over a prime field Z_P

$$Y^2 = (X^3 + a^* X + b)^* \{mod\, p\} \quad where \quad (4^* a^3 + 27^* b^2)\ ^*\{mod\, p\} \neq 0 \quad \text{(Non-singular curve)} \qquad (4.1)$$

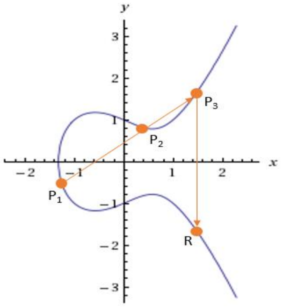


Figure 4.1 Elliptic Curve

Arithmetic Operation on ECC

- Adding Two Points on curve: If $P_1 (x_3, y_3)$ & $P_2 (x_4, y_4)$ are two points on the curve then $P_1 + P_2 = P_3 (X_r , Y_r)$ is the resultant point.
  Where $X_r = \{ \lambda^{*} \lambda - x_3 - x_4 \}^{*} \{mod\ p\}$, $Y_r = \{ \lambda^{*} (x_3 - x_r) - y_3 \}^{*} \{mod\ p\}$
  $$\lambda = \{ (y_4 - y_3) / (x_4 - x_3) \}^{*} \{mod\ p\} \qquad (4.2)$$
- Doubling point: *If* $P_1=P_2$ *then* $P+P=2P$ is known as point doubling $R=2P$
  $$Where \quad X_r = \{ \lambda^{*} \lambda - 2^{*} x_3 \}^{*} \{mod\ p\}$$
  $$Y_r = \{ \lambda^{*} (x_3 - x_r) - y_3 \}^{*} \{mod\ p\}$$
  $$\lambda = \{ (3^{*} x_3{}^{*} x_3 + a) / 2^{*} y_3 \}^{*} \{mod\ p\} \qquad (4.3)$$
- Point at Infinity: remarked to be the ideal point on the curve denoted by O
  If conditions are met $x_3 = x_4$ & $y_3 = y_4 =$ *or* $x_3 = x_4$ & $y_3 = - y_4$ then the points are said to be intersected at infinity
- Negation: Point by adding it to itself will produce outcome of ideal point
  $$P + (-Q) = O \qquad (4.4)$$
- Elliptic curve point multiplication is that the process of successive augmentation of point along an elliptic curve to itself continuously. It's employed in elliptic curve cryptography (ECC) as a way of fabricating trapdoor function (one-way function)
  N*P= P+P+P+P+P.... N times, where N is scalar. (4.5)

Table 4.2 Elliptic Curve Parameter Description

Parameter	Description
p	Prime number defining the Field F.
a, b	Coefficients in the equation of Elliptic curve
G	A base point or generator point of Elliptic curve
N	Order of G in E(F_p)
h	Co-factor

4.2.2 Elliptic Curve Diffie–Hellman Key Agreement Protocol

It is a key agreement protocol which uses elliptic curve arithmetic operation like point multiplication and addition as shown in Figure 4.2

How does it Works?

Let us take two parties 'D_a' and 'D_b'. Both of them should agree on elliptic curve parameters (p, a, b, G, N, h) Table 4.2 shows the elliptic curve parameters description is defined on Weierstrass equation, an algebraic curve with non-singular points.

For key agreement process, 'D_a' will get the 'D_b's public key and compute the shared secret key using his own private key; Similarly 'D_b' will get the 'D_a' public key to accumulate the secret key using his private key.

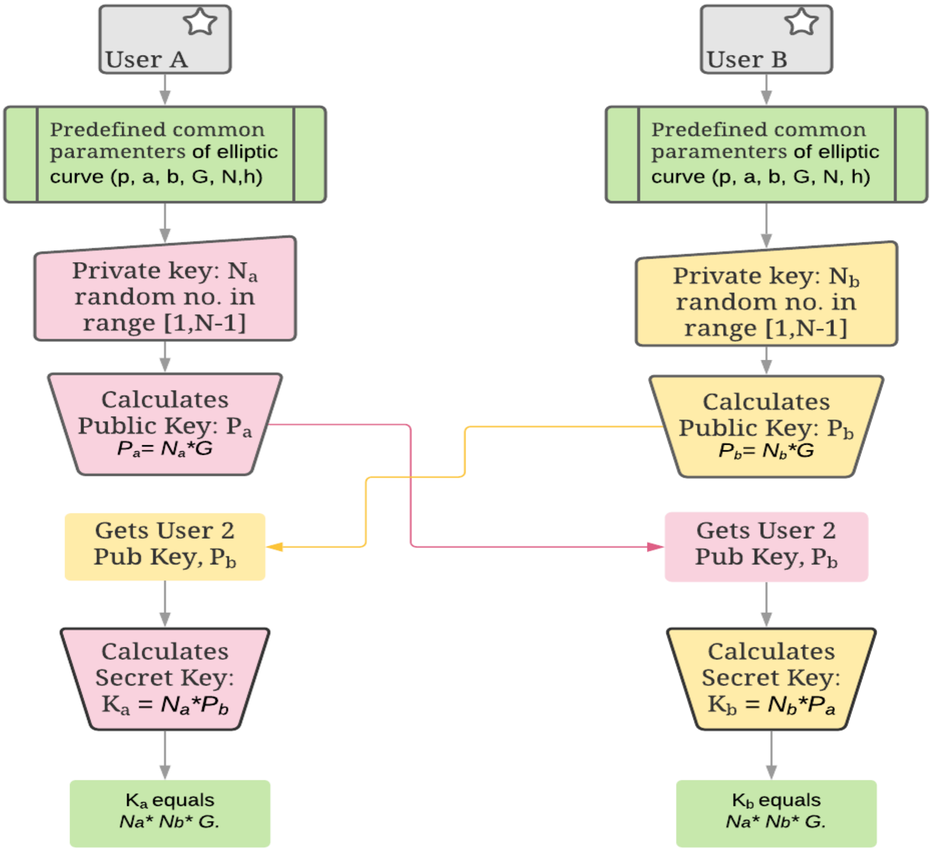

User A
User B
Predefined common paramenters of elliptic curve (p, a, b, G, N,h)
Predefined common paramenters of elliptic curve (p, a, b, G, N, h)
Private key: N_a random no. in range [1,N-1]
Private key: N_b random no. in range [1,N-1]
Calculates Public Key: P_a $P_a= N_a*G$
Calculates Public Key: P_b $P_b= N_b*G$
Gets User 2 Pub Key, P_b
Gets User 2 Pub Key, P_b
Calculates Secret Key: $K_a = N_a*P_b$
Calculates Secret Key: $K_b = N_b*P_a$
K_a equals $Na* Nb* G.$
K_b equals $Na* Nb* G.$

Figure 4.2 ECDH Key Agreement Protocol

4.3 ENCRYPTION ALGORITHM

4.3.1 AES Basics

It is a subset of Rijndael and one of the best symmetric block cipher algorithms. It processes message encryption with a fixed block size of 128bits and there are three types of keys of size 256/192/128 bits each take 14/12/10 rounds to convert plaintext into ciphertext respectively. AES operates on 16 bytes array (4*4) known as the state matrix.

Table 4.3 AES parameters

Key size (bit)	Rounds	No. of Sub keys (32bit each)	Block size (bit)
128	10	44	128
192	12	52	128
256	14	64	128

Algorithm for AES in brief steps are

1) AES desires a definite fixed bit round key of 128bits block for every round and an additional 1key for the entire method. These Round keys are extracted from the given key using the AES key schedule algorithm.
2) First round key addition: Using bitwise XOR, each byte of primary state array is fused with a byte of the round key respectively
3) Based on key size, each round consists of these particular steps, it maybe 9 or 11 or 13 rounds
    a. Substitute bytes transformation, a non-linear replacement step where each byte in a 16 input byte array is substituted with another byte forming completely a new one according to a lookup table (S-box)
    b. Shift rows transformation, a transposition step where we shift rows circularly in a pattern. Where the second row is shifted one position gets replaced with successive element, the third row is shifted two positions and the last is shifted three positions to the left circularly to form a complete shift row state matrix.
    c. Mix columns transformation, is a linear mixing arithmetic operation that runs on the columns of the state array i.e. each 4 bytes of state matrix is now changed using a special arithmetic principles. It takes 4 bytes of each column as functional input and fabricates a new four bytes that replaces the original column
    d. Add round key transformation the same as initial add round key using bitwise xor.
4) Final round (14th, 12th or 10th round respectively)
    a. Substitute Bytes
    b. Row shifting
    c. Round Key Add Transformation

Since AES is a block cipher encryption, it has distinct modes of an operation as shown in Table 4.4 whose main purpose is to mask patterns in the ciphertext. Each of its operations in AES is utilized in particular scenarios accordingly. Among them, GCM is the best because it provides privacy, data authenticity with high throughput, and high efficiency.

Table 4.4 Modes of Operation advantages and disadvantages (Smekal, Hajny, & Martinasek, 2018)

Mode	Advantage	Disadvantage
Electronic Code Block (ECB)	High –speed; parallelization; easy	No integrity check; equal plaintext block lead equal cipher text block
Cipher Block Chaining (CBC)	Error multiplication properties; chaining; widespread; parallelization (only decryption)	Dependence; slow (can't be parallel in encryption); decryption implementation is needed
Counter Mode (CTR)	Parallelization; stream cipher; message length can be arbitrary; decryption implementation is not needed	No error multiplication properties
Galois\Counter Mode (GCM)	Confidentiality; integrity; high-speed; parallelization	Complexity; computing power

4.3.2 AES-GCM Algorithm

Galois/Counter Mode (GCM) is authenticated encryption algorithms provide robust authentication mechanism with associated data than any other (non-cryptographic) checksum or error-detecting code. Specifically, these algorithms can detect unauthorized, intentional, and also accidental modifications of the information.

How does it Works?

Let's consider IV is an initialization vector (nonce) and Ek be the ephemeral key used for AES encryption. GCM works almost similar to counter mode as shown in Figure 4.3 Every block is enumerated successively. Each numbered block is fused with IV and enciphered with a cipher Ek; which are usually AES blocks. The results of this encryption are then XORed with the original text to supply the ciphered message. Contrary to counter modes, GCM encryption is mostly a stream cipher. A unique IV must be employed for every stream

The ciphertext blocks are considered as the constant multiplicative factors of an expression. Using mathematical operations over a finite field, these can be analyzed at a key-dependent point H. An authentication tag is constructed with the assistance of the outcome from the key-dependent point. This auth tag is utilized to verify the authenticity of the data (Integrity). The final block comprises of the ciphertext, auth tag, and the IV.

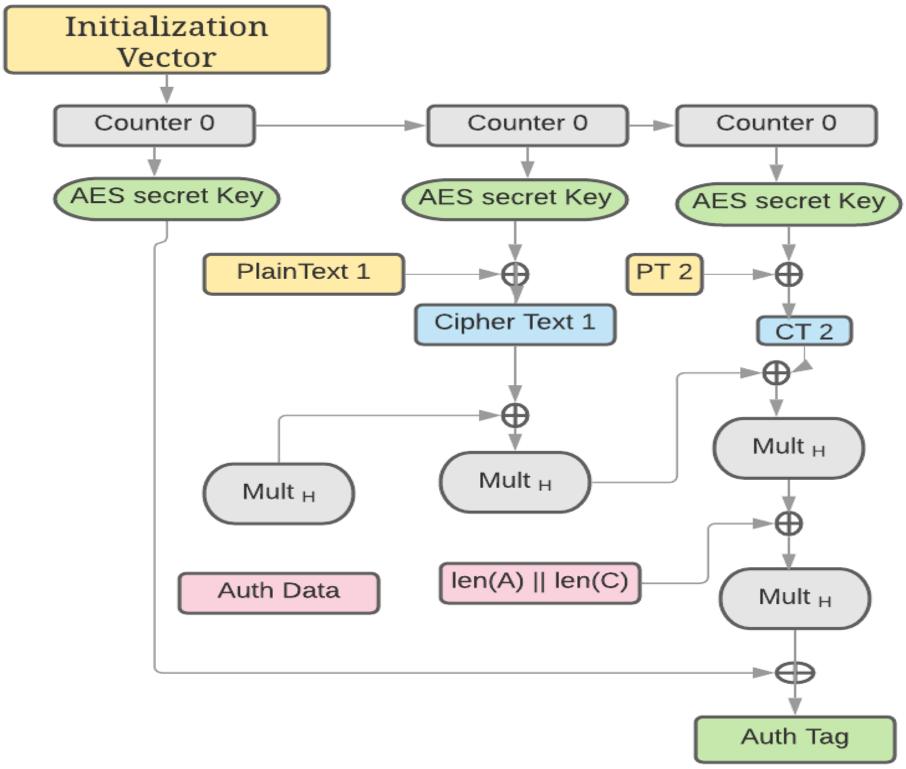


Figure 4.3 AES-GCM Encryption Method

GCM is a mode of operation of the AES algorithm which gives strong reliability of confidentially and authentication (up to about 64 gigabytes per encryption key) using a universal hash function which is described over a Galois binary field.

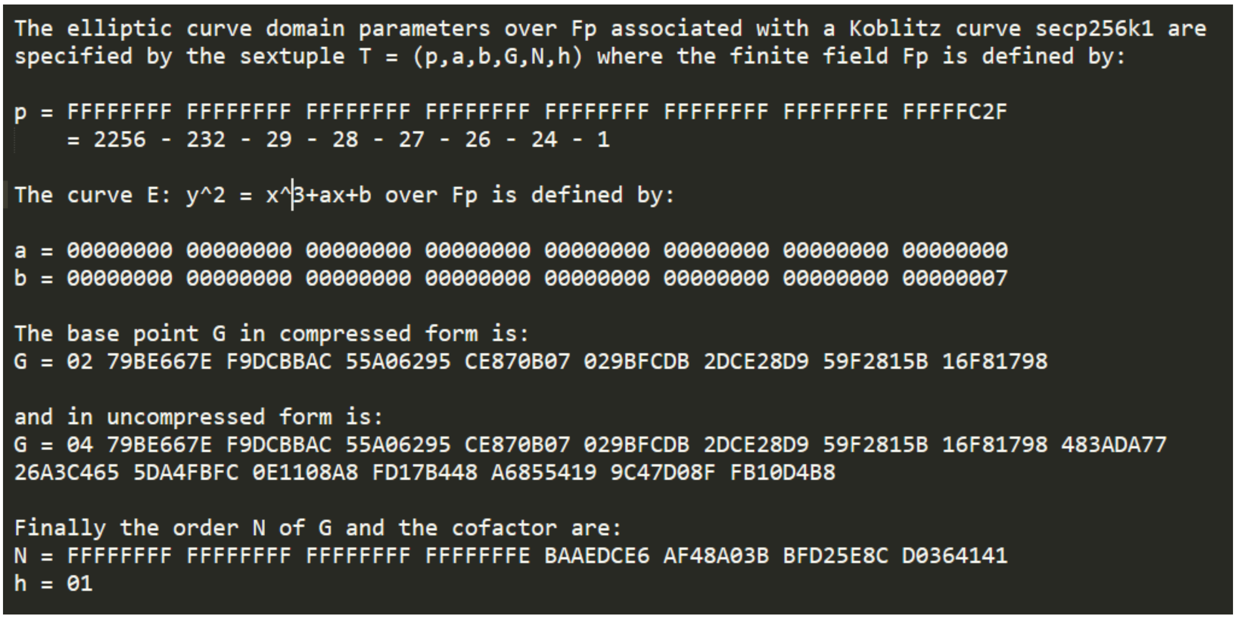
4.4 INTEGRATED ALGORITHM

The following Figure 4.4 shows the parameters we used for Elliptic curve from secp256k1, a koblitz curve which is more popularly used in Bitcoin's asymmetric cryptography and is defined in "Standard for Efficient Cryptography (SEC)".

Properties of secp256k1:

- Since the variable ‘a’ value is zero, the ‘a*x’ term in the elliptic curve equation is always zero, and becomes $y^2 = x^3 + 7$.
- It has characteristic p, and defined over the prime field Z_p.

Figure 4.5 shows the entire process of Integrated Cryptosystem. Instead of AAD we can also use hash functions like MD5, SHA for message authentication. But with authenticated AES-GCM encryption which has both GCM tag and AAD tag gives confidentiality and data authentication, also known as integrity is most efficient against most of security attacks.



```
The elliptic curve domain parameters over Fp associated with a Koblitz curve secp256k1 are
specified by the sextuple T = (p,a,b,G,N,h) where the finite field Fp is defined by:

p = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F
    = 2256 - 232 - 29 - 28 - 27 - 26 - 24 - 1

The curve E: y^2 = x^3+ax+b over Fp is defined by:

a = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
b = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000007

The base point G in compressed form is:
G = 02 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798

and in uncompressed form is:
G = 04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77
26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8

Finally the order N of G and the cofactor are:
N = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141
h = 01
```

Figure 4.4 Elliptic Curve Parameters used for application

Integrated algorithm will take the following steps

1) Text files are taken as input.
2) **Elliptic Curve Parameters**
   Define elliptic curve parameters for each user and create a secured communication channel to cloud.
3) **Elliptic Curve Diffie–Hellman Key Agreement Protocol**
   Perform ECDH Key exchange protocol and Calculate compressed secret key of size 256 bits.
4) **AES-GCM Algorithm**
5) AES-GCM algorithm is applied for encrypting the computer file, employing a secret key, and also the GCM tag and is uploaded to the cloud. Generate a random nonce of 12bytes for each communication cycle, so the identical nonce cannot reuse for the encryption process. GCM tag is of 16 bytes where 12 bytes are (nonce) IV tag and

remaining 4 bytes for a counter. Use the AAD tag for authenticated encryption so that message authentication is done

6) Original message can be accessed from client side by decryption with secret key and GCM tag. AAD tag is verified here for authentication of message i.e. data integrity
7) In the end, analysis is finished on the idea of various parameters like Avalanche effect, encryption time, decryption time, storage.

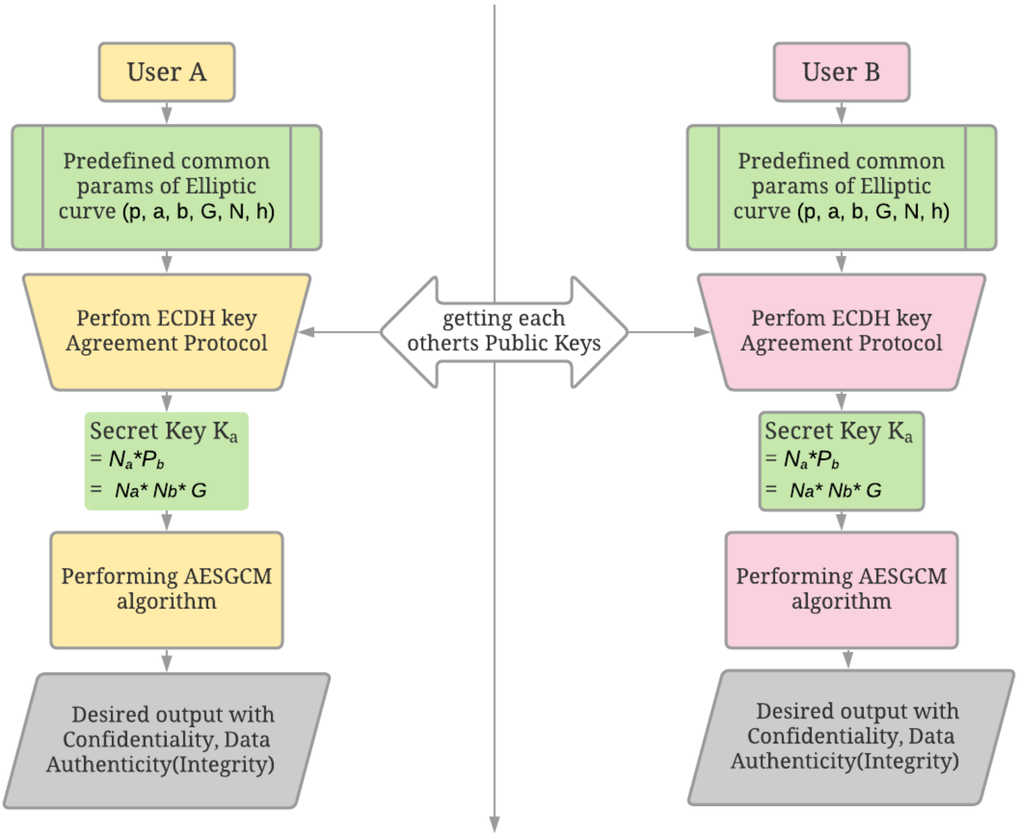

User A
User B
Predefined common params of Elliptic curve (p, a, b, G, N, h)
Predefined common params of Elliptic curve (p, a, b, G, N, h)
Perfom ECDH key Agreement Protocol
getting each otherts Public Keys
Perfom ECDH key Agreement Protocol
Secret Key K_a = N_a*P_b = Na* Nb* G
Secret Key K_a = N_a*P_b = Na* Nb* G
Performing AESGCM algorithm
Performing AESGCM algorithm
Desired output with Confidentiality, Data Authenticity(Integrity)
Desired output with Confidentiality, Data Authenticity(Integrity)

Figure 4.5 Combined Protocols (Refer 4.2.2 for ECDH and 4.3.2 for AESGCM)

4.4.1 Flow Chart and Class Diagram for Proposed Solution

First patients visit hospital and register themselves with help of admin. Authenticated doctors are given access to the cloud by admin to get health details to provide effective medicine intake in a safe communication path interactively with patients. Admin can add and remove the users accordingly and their records in cloud but unable to read health information due to encryption. They are provided with login details and can access them as shown in flowchart below Figure 4.6

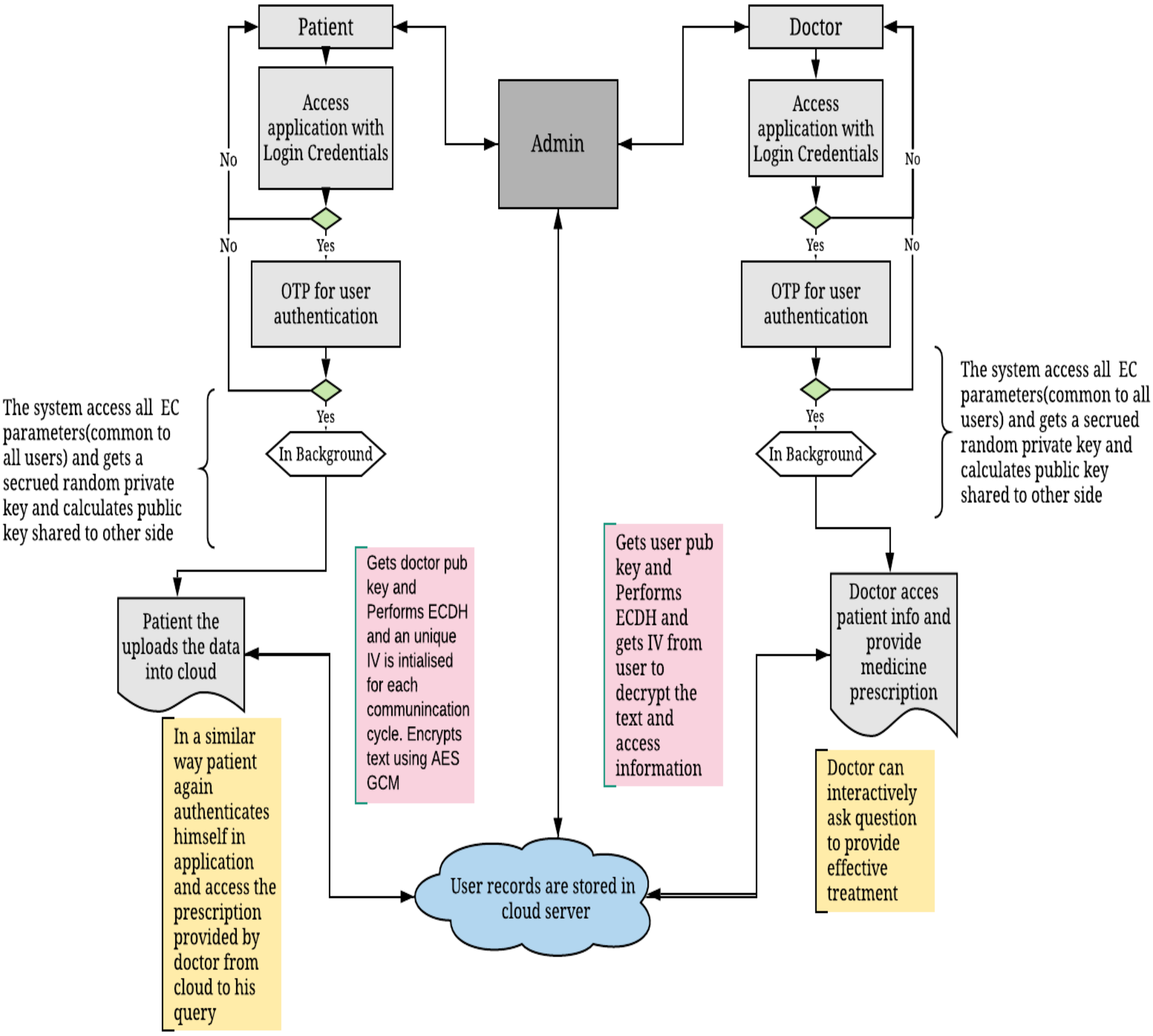

Patient
Access application with Login Credentials
No
No
Yes
OTP for user authentication
Yes
In Background
The system access all EC parameters(common to all users) and gets a secrued random private key and calculates public key shared to other side
Patient the uploads the data into cloud
In a similar way patient again authenticates himself in application and access the prescription provided by doctor from cloud to his query
Gets doctor pub key and Performs ECDH and an unique IV is intialised for each communincation cycle. Encrypts text using AES GCM
Admin
User records are stored in cloud server
Gets user pub key and Performs ECDH and gets IV from user to decrypt the text and access information
Doctor
Access application with Login Credentials
No
Yes
No
OTP for user authentication
Yes
In Background
The system access all EC parameters(common to all users) and gets a secrued random private key and calculates public key shared to other side
Doctor acces patient info and provide medicine prescription
Doctor can interactively ask question to provide effective treatment

Figure 4.6 Flowchart of the process

We have compiled the factors and functionalities of every phase and therefore the restrictions imposed on them. We represented the consistent view of the application in a very similar way of sophistication diagram which analyses the visualizing and documenting different aspects of a system and also helps in developing a runnable code for the software application as in Figure 4.7

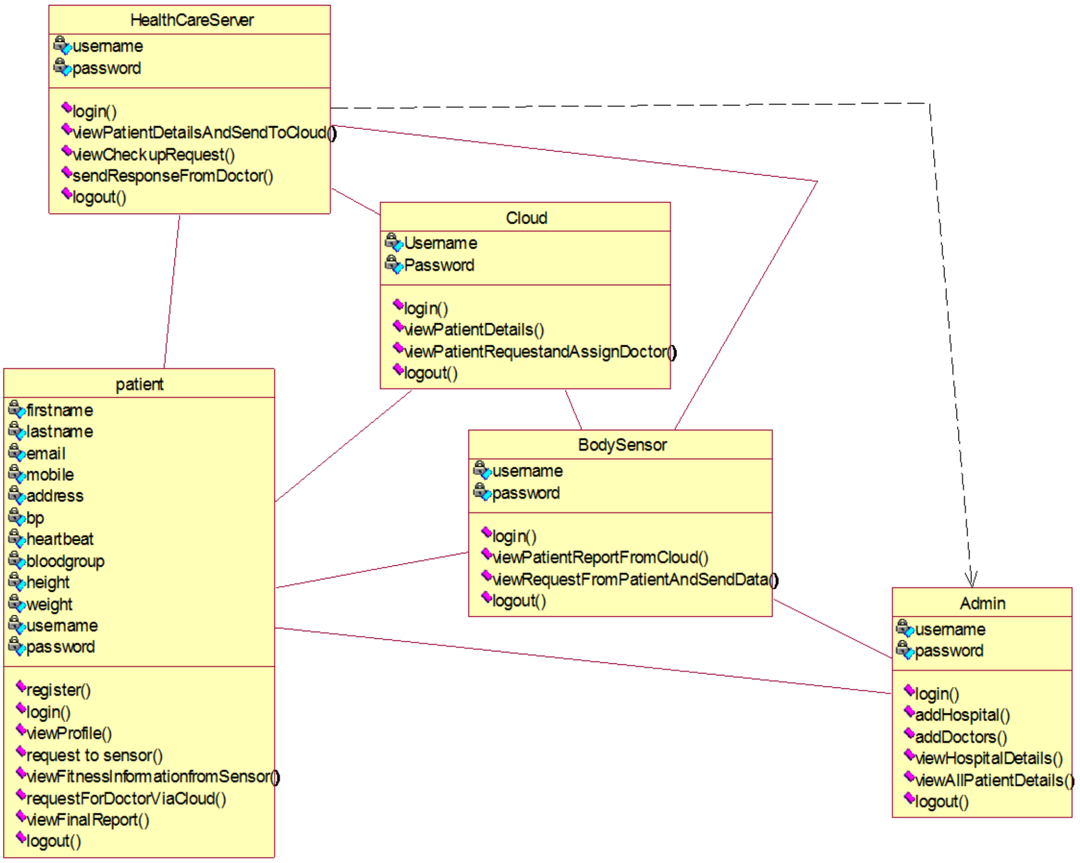


Figure 4.7 Class diagram

CHAPTER 5

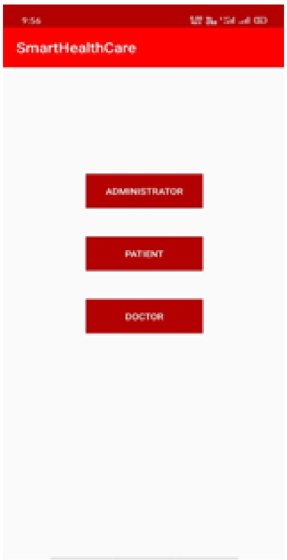
RESULTS AND DISCUSSIONS

5.1 RESULTS

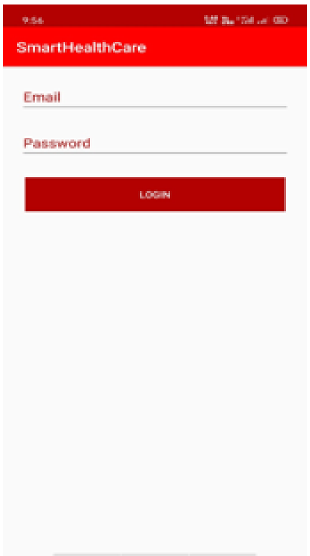
We have successfully developed a basic model of telecare medical information system application in mobile platform using android studio SDK tools. Here the admin can manage users and the patients can login with authorized credentials and next page to OTP screen where a token is send to registered mobile for user authentication. He can upload his details and health information; since we have used integrated security protocol (ECDH+AES-GCM) the information is send to the cloud in a secured communication channel and can be accessed by only authorized people like doctors who can be successfully verified with two-factor authentication protocol

5.1.1 Snaps of Proposed Scheme

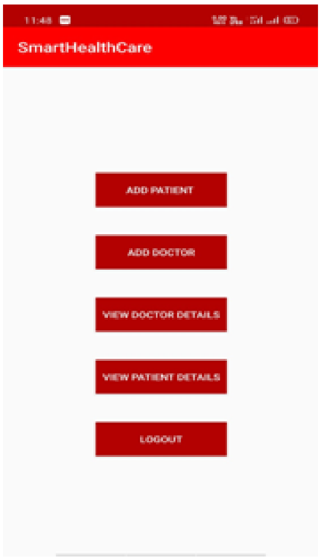
Here we have some of the application snapshots from mobile device which we have developed and interfaces of each activity are proceeded as shown in Figure 5.1a
And data base which we used is Google’s Firebase as shown in Figure 5.1b



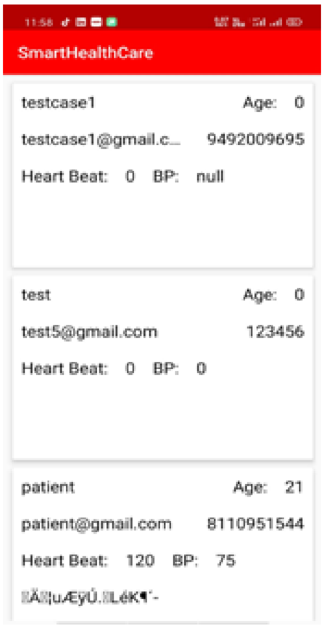
Home Page



Login Page



Admin Home Page

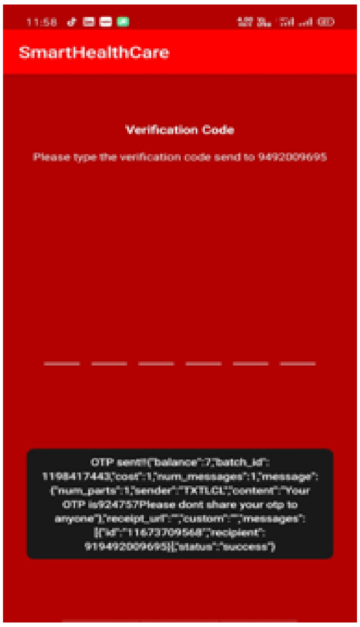


testcase1 Age: 0
testcase1@gmail.c... 9492009695
Heart Beat: 0 BP: null

test Age: 0
test5@gmail.com 123456
Heart Beat: 0 BP: 0

patient Age: 21
patient@gmail.com 8110951544
Heart Beat: 120 BP: 75
ÄluÆyÚ.LéK¶'-

Patient Details

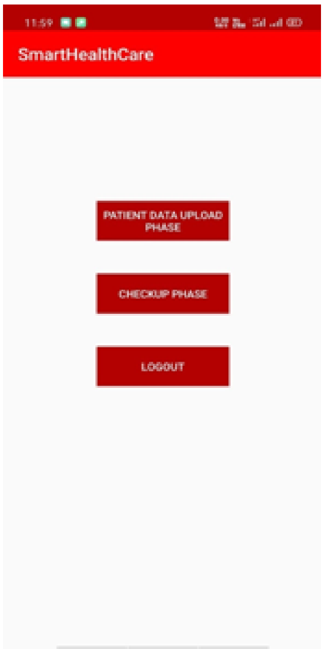


Verification Code

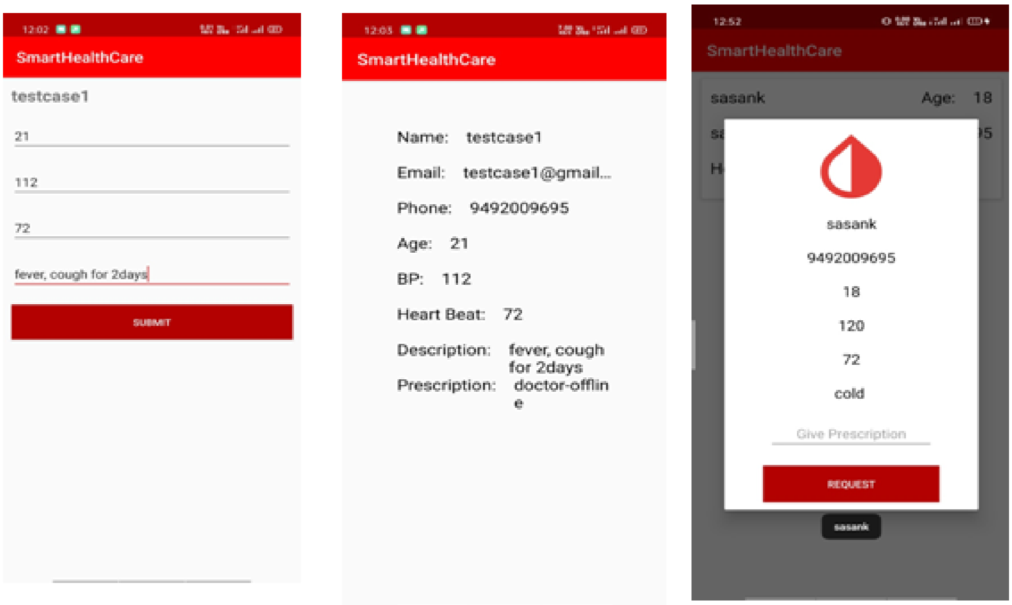
Please type the verification code send to 9492009695

```
OTP sent!!{"balance":7,"batch_id":
1198417443,"cost":1,"num_messages":1,"message":
{"num_parts":1,"sender":"TXTLCL","content":"Your
OTP is924757Please dont share your otp to
anyone"},"receipt_url":"","custom":"","messages":
[{"id":"11673709568","recipient":
919492009695}],"status":"success"}
```

After Patient Login
OTP verification



Patient’s Home Page



testcase1

21

112

72

fever, cough for 2days

Name: testcase1

Email: testcase1@gmail...

Phone: 9492009695

Age: 21

BP: 112

Heart Beat: 72

Description: fever, cough for 2days

Prescription: doctor-offline

sasank Age: 18

sasank

9492009695

18

120

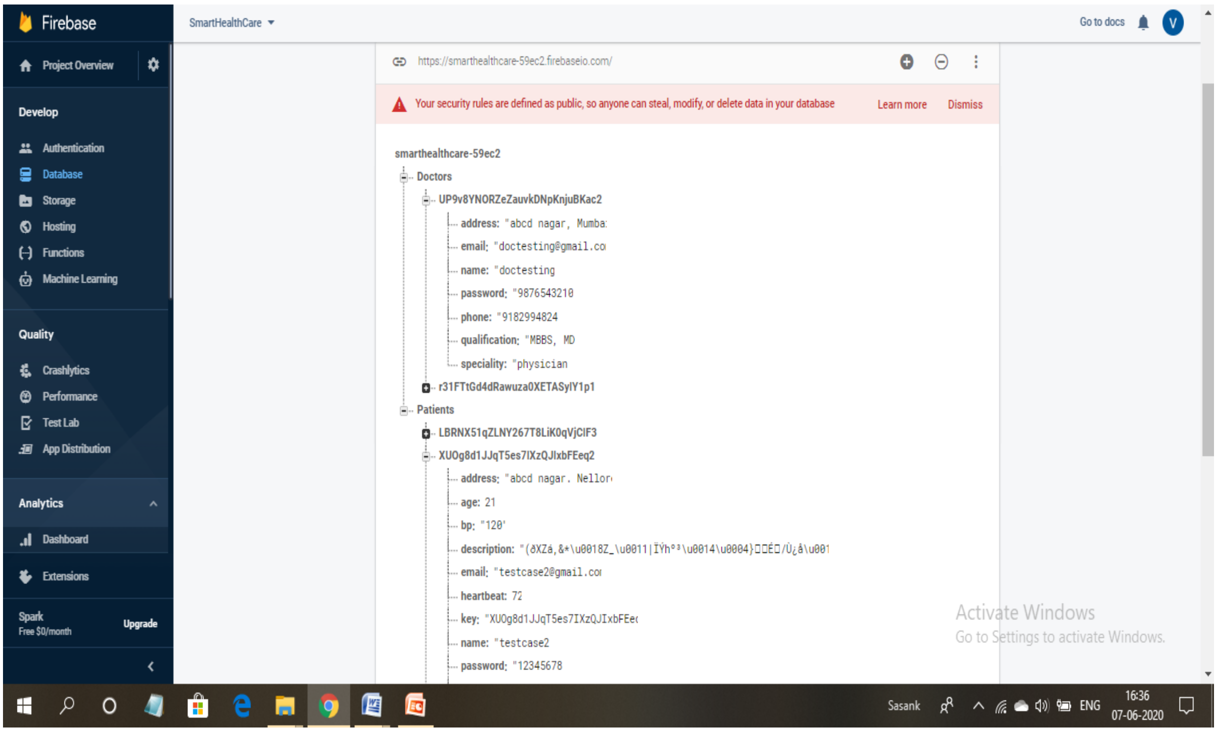
72

cold

Give Prescription

Patient Description Patient Check up page Doctor Prescription page

Figure 5.1a Some of the Application Screenshots.



https://smarthealthcare-59ec2.firebaseio.com/

Your security rules are defined as public, so anyone can steal, modify, or delete data in your database

```
smarthealthcare-59ec2
  Doctors
    UP9v8YNORZeZauvkDNpKnjuBKac2
      address: "abcd nagar, Mumba:
      email: "doctesting@gmail.co
      name: "doctesting
      password: "9876543210
      phone: "9182994824
      qualification: "MBBS, MD
      speciality: "physician
    r31FTtGd4dRawuza0XETASyIY1p1
  Patients
    LBRNX51qZLNY267T8LiK0qVjCIF3
    XUOg8d1JJqT5es7IXzQJlxbFEeq2
      address: "abcd nagar. Nellor
      age: 21
      bp: "120'
      description: "(ðXZá,&*\u0018Z_\u0011|ÏŸh°³\u0014\u0004}□□É□/Ù¿å\u001
      email: "testcase2@gmail.co
      heartbeat: 72
      key: "XUOg8d1JJqT5es7IXzQJIxbFEe
      name: "testcase2
      password: "12345678
```

Figure 5.1b Firebase Database

5.1.2 Avalanche Effect

Avalanche's effect is the preferable property in cryptographic techniques, mostly in symmetric encryption. It describes even the slightest change in an exceedingly single little bit of input or key, the output is modified significantly in additional than half the bits in cipher text are changed

Here are examples of our algorithm which shows avalanche's effect.

- *Example1:* The letter h is capitalized and you can see the variance in outputs
  Message: hye
  Encrypted message: 05536D1D38136A40EF6BE8FD23FE5298A9994B
  Message: Hye
  Encrypted message: 272E6D7E5E920DA8A77C99C480F4AA5E47E2B1
- *Example 2:* changing key for every session, same message got different output
  Message: hye
  Encrypted message: 888213AAB9299655D4266ECEE47045FA4C9878
  Message: hye
  Encrypted message: 919E18991D35C8F91BB6964CFC1E9CD83E1E
- *Example 3:* A single bit 0 is flipped and output changes
  Plain text: 000
  Encrypted message: 54F2F22DB67014BC1E2D0BE4605F3B5C295FC2
  Plain Text: 001
  Encrypted message: 34D1F37B9600AF88151249A4DBD6F6447E99F5

5.1.3 Performance in Terms of Encryption and Decryption time

Table 5.1 Performance in terms of Computation time and Memory Usage of ECDH_AES-GCM of key 256 bits

File Size (bytes)	Encrypted File Size (bytes)	Encryption Time (milliseconds)	Decryption Time (milliseconds)	Algorithm Time (milliseconds)
16	64	126	1	959
31	94	125	3	956
2522	5092	129	5	961
6771	13704	135	6	974
9513	19210	147	11	971

Hybrid concepts have emerging mostly with combination of symmetric key and asymmetric ones. Most of examples from symmetric algorithms DES, AES, Blowfish encryptions techniques with asymmetric RSA, Diffie Hellman, ECC Since symmetric algorithms are better than other techniques when compared to encryption and decryption time or memory or security level, these are used for encryption process and due to key distribution defect in single key system, key exchange or fabrication is done with the help of public key cryptosystem to get more secured cryptosystem with less complexity and memory allocation. Hence these hybrid algorithms come in handy nowadays.

RSA-AES is one of them, Encrypting data with AES-256 and the secret key is shared by encoding with help of RSA-2048 encryption using other end public key thus producing a new hybrid system. So we are comparing our protocol with these RSA-AES and our previous work EC- ElGamal.

Table 5.2a Comparison of Encrypted File size in bytes

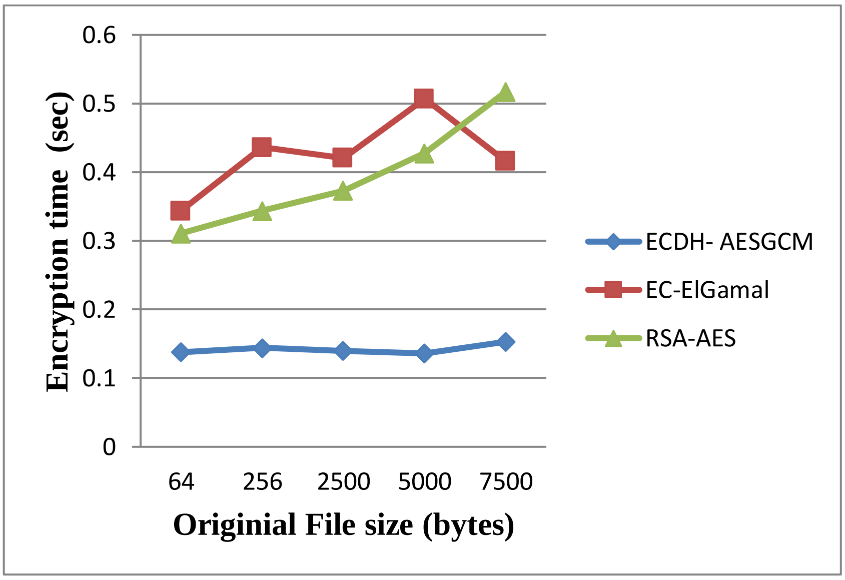
File size (In bytes)	Encrypted File size EC-ElGamal (bytes)	Encryption File size RSA-AES (bytes)	Encryption File size ECDH-AES (bytes)
64	352	809	160
256	928	1272	544
2500	7672	6667	5062
5000	15160	12678	10032
7500	22661	18688	15032

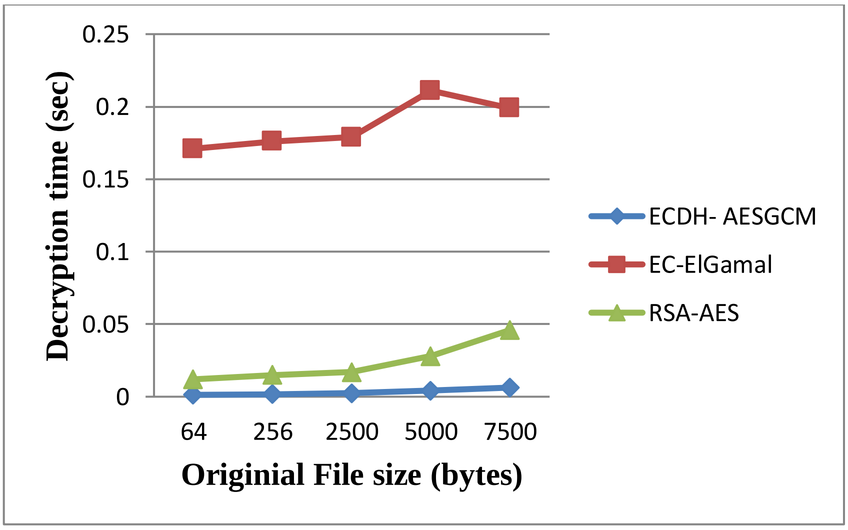
Table 5.2b comparison of Encryption time with variable text sizes

File size (In bytes)	Encryption time EC-ElGamal (sec)	Encryption time RSA-AES (sec)	Encryption time ECDH-AES (sec)
64	0.344	0.311	0.138
256	0.436	0.344	0.144
2500	0.421	0.373	0.140
5000	0.507	0.428	0.136
7500	0.416	0.517	0.153

Table 5.2c comparison of Decryption time with variable text sizes

File size (In bytes)	Decryption time EC-ElGamal (sec)	Decryption time RSA-AES (sec)	Decryption time ECDH-AES (sec)
64	0.171	0.012	0.0013
256	0.176	0.015	0.0017
2500	0.179	0.017	0.0025
5000	0.211	0.028	0.0042
7500	0.199	0.046	0.0063





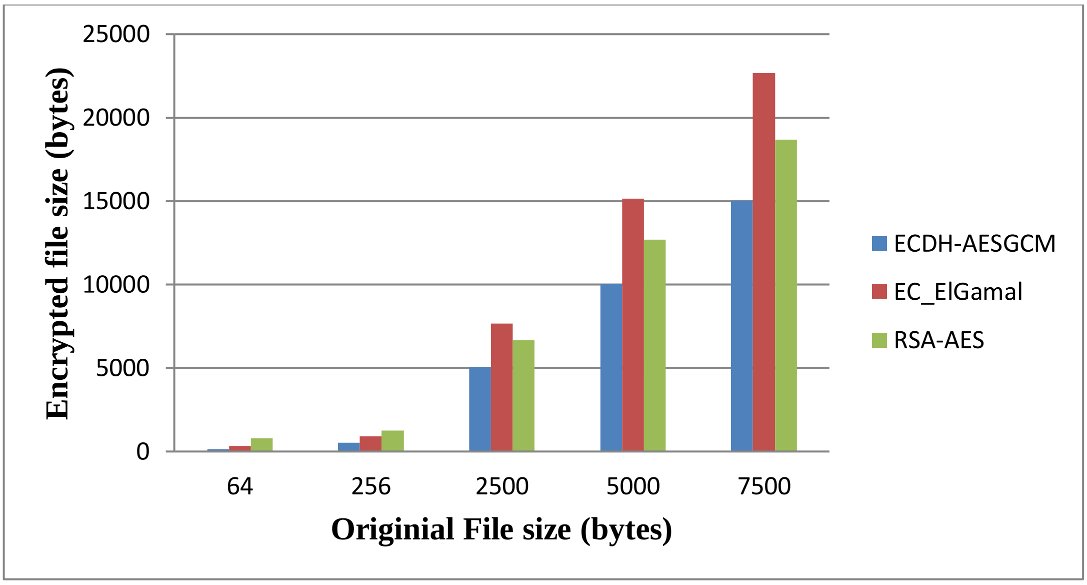


Figure 5.2 Comparative graphs of performances with ECDH+AESGCM vs. EC-ElGamal vs. RSA-AES regarding Encryption, Decryption time and Encrypted file size

Applications that need high data throughput can experience in these high-speed implementations. Thus our enhanced protocol isn't only efficient and secure, but also hardware implementations can do high speeds with low cost and low latency because the mode is pipelined.

CHAPTER 6

CONCLUSIONS AND FURTHER WORK

In this paper, we have reviewed the previous schemes proposed in various research papers. We located that message authentication fails, and a session key is impractical within the admin phase. It also fails in impersonation attack while the patient's information transmits phase, and patient anonymity, unlinkability, doctor unlinkability.

Conclusively, presented paper is the approach of a secured and effective integrated cryptosystem comprises of ECDHE key agreement protocol to calculate secret key and using that ephemeral key AES-GCM-256 encryption is finished which provides confidentiality and data authenticity (Integrity), and two-factor authentication protocol i.e. authorized user login and one-time password to the registered mobile for user authentication for cloud-assisted TMIS application.

This Integrated cryptosystem is secured against most of the security attacks even against quantum attacks and provides maximum security together with user authenticity employing a two-factor authentication method. It uses fast encryption and decryption protocol and uses it for big data files. It's simple and more efficient in terms of computation cost and memory usage compared to previous paperwork which is completed by ECC.

FUTURE ENHANCEMENT

Further, we proposed an improvised replacement protocol within the same environment. The paper shows the certainty of the proposed algorithm which supported several security attributes and functionality features. Hence, the presented protocol manages the higher security feature and attributes compare to their previous related protocols in the telecare medical information system. Additionally, we show the performance of the proposed protocol which is efficient in the cloud-based TMIS environment with less complexity

In the future, many cryptographic techniques are developing recently. Furthermore, we can add a biometric identification method for best authenticity and ECC is emerging more and more recently with more efficiency and reducing complexity. The hyper elliptic curve is one in all the emerging techniques but still in theoretical progress which has high complexity in implementation. We will see plenty of working progress within the security domain with more emerging techniques

CHAPTER 7

REFERENCES

[1] **Bommala, H., Kiran, D. S., Pujitha, M., & Reddy, R. P**. (2019). Performance of Evaluation for AES with ECC in Cloud Environment. *Int. J. Advanced Networking and Applications , 10* (5), 4019-4025.

[2] **Elaine, B.** (2006). *Suite B Cryptography*. Computer Security Resource Center, National Institute of Standards and Technology.

[3] **kajal, A., & Gulshan**. (2018). Enhanced Cloud Storage Security Using ECC-AES A Hybrid Approach. *International Journal for Research in Engineering Application & Management , 4* (5).

[4] **Kumar, V., Ahmad, M., & Kumari, A.** (2019). A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS. *Telematics and Informatics , 38*, 100-117.

[5] **Patel, G. R., & Panchal, P. K.** (2014). Hybrid Encryption Algorithm. *INTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH , 2* (2), 2064-2070.

[6] **Rani, S., & Kaur, H.** (2017). Implementation and comparison of hybrid encryption model for secure network using AES and Elgamal. *International Journal of Advanced Research in Computer Science , 8* (3), 254-258.

[7] **Shaikh, A. P., & Kaul, V. J.** (2014). Enhanced Security Algorithm using Hybrid Encryption and ECC. *IOSR Journal of Computer Engineering , 16* (3), 80-85.

[8] **Sharma, S., & Chopra, V.** (2016). Analysis of AES Encryption With ECC. *Proceedings of International Interdisciplinary Conference On Engineering Science & Management.* Goa.

[9] **Smekal, D., Hajny, J., & Martinasek, Z.** (2018). Comparative Analysis of Different Implementations of Encryption Algorithms on FPGA Network Cards. *IFAC-PapersOnLine* .