A Framework for Cloud-Based EHR Security Using Hybrid Cryptographic Methods of AES and ECC

MSc Research Project

MSc Cybersecurity

Vansh Arora

Student ID: 21144222

School of Computing

National College of Ireland

Supervisor: Dr. Rohit Verma

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Vansh Arora
Student ID:	21144222
Programme:	MSc Cyber security **Year:** 2022 - 2023
Module:	MSc Research Project
Supervisor:	Dr. Rohit Verma
Submission Due Date:	25/04/2023
Project Title:	A Framework for Cloud-Based EHR Security Using Hybrid Cryptographic Methods of AES and ECC
Word Count:	**8448** **Page Count:** 20

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:

Date: 25/04/2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

A Framework for Cloud-Based EHR Security Using Hybrid Cryptographic Methods of AES and ECC

Vansh Arora

x21144222

Abstract

The establishment of electronic health records (EHRs) for patient monitoring is a notion that has gained widespread acceptance in the healthcare sector. Patients can contact their individual doctors and seek their advice for disease diagnosis using this useful web app. This enables them to maintain a digital and electronic record of their medical records. Yet, due to the possibility of several patients trying to access them, the volume of the data uploaded to the EHR is enormous. Due to the system model's vulnerability in this situation, the data that has been obtained may be subject to various attacks and breaches, which could even result in the loss of power for data stored on the relevant EHR on the cloud. In addition to this; since the working of cloud gives access to users for retrieval of data irrespective of their location, the entire system becomes more prone to exposures and breaches. Therefore, in order to protect the data being sent over the EHR, I propose the implementation of hybrid encryption techniques in this study. Elliptic Curve Cryptography (ECC) and the Advanced Encryption Standard (AES) are utilised in a hybrid cryptographic technique (HCT) for this purpose. Asymmetric encryption is not practical for encrypting massive amounts of data because it is slower and less effective than symmetric encryption. By utilising both symmetric and asymmetric encryption, hybrid encryption can overcome these constraints. The informational communication is expected to be secured on the cloud using the HCT thus described.

Keywords: AES, cryptography, ECC, encryption, EHR

1 Introduction

With massive evolution in technological domains, wireless communication has observed to be significantly integrated with healthcare. This technology has made it possible to store huge amounts of data in remote places using cloud computing [1]. The idea behind this; is the ability to control, supervise, and distribute resources to specific consumers. Implementing electronic health records is one service that the cloud offers (EHR). The primary reason EHRs are used is to enable remote patient health information sharing and access by medical professionals for interpretation. Such system helps to monitor patient physiology, medical images of the patient and further tends to record them electronically. The healthcare systems thus built using this concept tends to exchange and transmit data over cloud networks so that it can be remotely accessed by users as per their convenience. However, due to patient's data privacy, their stored data must remain private and all the challenges with respect to cloud database must be eliminated to develop and store patient information. Dealing with massive amounts of data in real time may also cause delays in the delivery of EHR services. Since, patient data is just not sensitive to his personal information; but rather might also affect the diagnosis conducted by the physician; protecting this data becomes mandatory. So, the level of security of the data stored in the cloud is entirely dependent on the security approach used by the cloud service provider. Due to the presence of various attackers and hackers present on the cloud, over which the user has no control, data may be at risk. As a result, protecting the data uploaded to EHRs has drawn the attention of numerous research experts. Hence for a divulged form of transmission and information exchange; implementation of encryption techniques becomes a

compulsion. Yet, both symmetric and asymmetric cryptography, which both includes the production of keys based on the respective key size, can be used to secure, and protect the entire process of data on the cloud through encryption. However, due to the complexity of the procedures involved and the ability to balance longer key lengths, performance evaluation of asymmetric algorithms tends to be stronger [2]. Besides the already existing cryptographic ideas, other methods like AES, DSA, RSA, blowfish, and ECC have also been taken into account. ECC-based encryption algorithms have a tendency to take up less processing time than AES and RSA, despite the fact that Authors K Gupta et.al 2011 [3] implement the theory of the AES algorithm. The computational cost associated in the process becomes suited for healthcare data because the generation of key sizes in ECC is small.
The proposed study additionally suggests implementing AES algorithm in addition to ECC. This improvement is made to facilitate effective key management, allowing for the safe upload of patient data to the cloud.

1.1 Background

Storing data on the cloud is one of the models and concepts of data computing that allows multiple services to users irrespective of their physical location. This is done so that the services can be accessed at any point of time with unlimited data storage and network and is therefore widely accepted by people. Its attractive features have strongly developed a reliance on cloud; that has eventually led to an ever-increasing dependence of service usage by individuals. The dependence has however led to massive drive of voluminous data on cloud; thereby raising multiple security and privacy issues. Challenging activities of such services; majorly includes data breach and attacks that are done on the cloud by various attackers. Hence, this triggers to restricting certain amount of data to clients and users so that only specific data can be accessed by them through an authorization process. This amount of data can further be categorised by depending on the characteristic of the cloud thus adopted. Following are the types of cloud characteristics:

- Network access: this feature enables the user to access services from any network irrespective of his geographical location
- Services on demand: this feature provides multiple services to the user as per his requirements
- Pooling: this feature enables multiple service providers to pool their resources and make it accessible to users

In addition to services on clouds, multiple devices can also result into data breach. This can be done when the attackers reuse the respective APIs of the networking data, thereby causing data loss. Therefore, in such a scenario application and concepts of cryptography must be employed to secure and monitor the data being uploaded on cloud. The working implementation of such encryption and decryption techniques is done with the help of multiple keys being generated on both the sides of the communicating channel. There are primarily two keys of encryption which are performed on the data:

- Asymmetric Key Encryption
- Symmetric Key Encryption

The implementation of an Asymmetric Key Encryption (AKE) follows the concept of public key cryptography wherein there are two keys which are to be generated. A public key and a private key. On the other hand, the implementation of Symmetric Key Encryption (SKE) follows the concept of private key cryptography wherein only one key is generated. However, both the encryption keys are used for storing and securing data that further blocks the activity of hackers. The keys so generated are transferred through a medium and differs in key sizes that ensures the security being maintained in user data. Table 1 below describes multiple techniques that are used to encrypt the data:

Table 1: Abbreviations of Cryptographic Techniques

Abbreviation	**Explanation**
AES	Advanced Encryption Standard
ECC	Elliptic Curve Cryptography
RSA	Rivest-Shamir-Adleman
DES	Data Encryption Standard
PHECC	Polynomial-based hashing elliptic curve cryptography
NIST	National Institute of Standards and Technology
EAP-CHAP	Extensible Authentication Protocol—Challenge Handshake Authentication Protocol
GDLP	Generalized Discrete Logarithm Problem
API	Application Programming Interface
CISP	Cryptographic Service Provider

Asymmetric Key Cryptography (AKC) is a theory that is put into practise in conventional ECCs, where two unique keys are generated between the communicating parties. These keys are referred to as private and public keys. The generated keys are distributed to the users during implementation via a communication channel. Although its encryption implementation is identical to those of RSA and Diffie-Hellman, ECC is chosen over the two due to its use and production of smaller keys.

The key size produced by ECC, RSA, and DH is compared in the Table 2

Table 2: Key size Comparison with various algorithms combination

Elliptic-Curve Cryptography (bits)	**RSA and DH (bits)**	**Key Size Comparison**
160	1024	1:6
224	2048	1:9
256	3072	1:12
384	7680	1:20
521	15360	1:29

Nonetheless, there is a significant agreement involved because the implementation process in ECC and DH is extremely comparable [4]. This key agreement is started by creating private keys (a, b), and it is kept between the two parties in confidence. The following step involves multiplying the private keys (a, b) to create the public keys (a, b). Next, using the appropriate

domain specifications, this produced public key is communicated with. As public keys are generated by point multiplication, the entire encryption executional protocol is safeguarded and becomes even less susceptible to Man in the Middle Attacks (MITMs).

1.2 Research Problem

The workflow of an electronic health record (EHR) follows by a patient initially uploading his health records on the web app. The health record includes his personal information such as that of his pulse rate, heart rate, blood pressure etc. So, protecting this patient information becomes a requirement to prevent the loss of patient files. Apart from storage of a single patient's data records; sensitive information of various other patients is also present and stored on the cloud. In addition to this; since multiple owners and users are associated with cloud implementation; the privacy and accessibility of patient information becomes very crucial. Hence, patient data must be encrypted before uploading it on cloud and its access must be restricted to only its specific owner. Due to this restriction of data storage over cloud; attacks such as third-party impersonation and eavesdropping are more likely to occur. Such attacks being made on patient data might result into a loss of user trust since his data is exposed to risk. In such a scenario, aggregating patient data on EHR with methods of encryption serves to overcome this research problem and thereby eliminates the lack of interoperability between storage infrastructures and stakeholders.

1.3 Motivation

Securing patient data on cloud-based health care systems is considered to be as the utmost priority of research scholars which can thus be executed in multiple ways. In order to protect transfer of data over cloud, encryption techniques and strategies are used. However, a significant challenge with respect to adoption of these techniques is that the algorithms possess large key lengths and size which thereby tends to occupy a larger memory space. This in turn leads to usage of high computational power in order to secure and monitor the data. Therefore, this has been considered to be as a major problem in encrypting data over cloud and has thereby motivated the authors of the proposed study to contribute their work in this domain. For the above-mentioned reasons, the author suggests the implementation of AES and ECC algorithms to store and retrieve patient data from the health care app. As and when an input is given to the server system, a private key is generated using the AES encryption. Since AES follows the concept of symmetric cryptography; the same key is again used for the purpose of decryption. Hence it can be said that, if this single key is accessed by a third party; the entire patient data becomes exposed to attacks and might lead to data loss which could easily be read by someone else. Although AES is considered to be as one of the commonly used and secured cryptographic algorithms; it still has the probability of information exposure. Hence, the authors propose to develop a hybrid cryptographic technique; that utilizes the concepts of AES as well as ECC; so that two keys are generated and further used for the encryption and decryption process. Since ECC follows the concepts of asymmetric cryptography; getting access to both the keys generated becomes a challenging task. In addition to generation of secret key and public key through ECC; the size of the keys thus generated is comparatively small. Thereby making it difficult for the attacker to get access to sensitive data thus produced.

1.4 Research Objectives

The proposed study seeks to resolve the concerns by creating a hybrid cryptographic technique that might secure the EHR system installed on the cloud, taking into account the research problems listed as above. The healthcare data is encrypted for this reason, and the implementation is further broken down into two stages:

- To secure communications on the EHR, use AES encryption
- To generate keys, use ECC encryption.

The report's stated objectives are as follows to serve this purpose:

- To add novelty to the current system
- To improve the system model's overall efficiency

1.5 Research Questions

In the past ten years, the world has seen a significant amount of technological and digital transformation. This has been enhanced by cloud computing. The ability to secure data on the cloud is swiftly emerging as the next great thing in technology, shattering all preconceptions of what is conceivable and creating countless possibilities for meeting technical demands. One such field that has been conquered is healthcare, where patient monitoring is totally done remotely via a website that has been set up on the cloud. These web applications are linked to the cloud, where patient data is handled by specialists and is prepared for extended storage after being examined by several doctors. Nevertheless, cloud based EHRs, or healthcare systems typically struggle to handle enormous amounts of data. Monitoring and regulating patient data among doctors in such a situation is prone to become a tiresome process. This could also cause a lag or delay in the EHR service. The exchange of patient data between online apps and sensor-cloud, as well as between the cloud and hospitals or specific doctors, may be delayed if just the cloud is used. There can be no compromise on speed or efficiency since the healthcare sector demands real-time operations. Sending such massive volumes of data back and forth does not seem like a good idea in this case due to latency concerns and security reasons. As a result, a hybrid cryptographic technique is needed rather than a single encryption algorithm that would be in responsibility of performing cryptography and real-time activities. Hence, this narrates the fundamental research question of the proposed report:

RQ: Which hybrid cryptographic technique (HCT) is most appropriate for monitoring real-time EHR on cloud activities?

1.6 Organization of the Thesis

The proposed study's Chapter 1 Introduction explains how hybrid cryptography may secure electronic health records in real time. It also states the objectives of the research study along with research questions thus related. Chapter 2 Related Works briefs on similar works being proposed by multiple authors from the same filed. The chapter also provides a comparative analysis of the same and mentions the contributions of the suggested research. Chapter 3 Methodologies Used summarizes the implement of the thesis; such as implementation of ECC and AES. The chapter also explains the proposed workflow of the framework. Chapter 4

Implementation Details highlights the implementation details of the same along with architecture of the system. Chapter 5 Results illustrates the results, and Chapter 6 Discussion discusses them, thus obtained followed by Conclusions and Future scope mentioned in Chapter 7. The thesis finally comes to an end by references.

2 Related Works

The notion of monitoring patient data in real time is facilitated using a cloud network which is secured through cryptography. This concept is traditionally referred to as an e-health care system that tends to collect sensitive information of the patient using his unique ID. The collected information is then stored on a database which can be accessed by multiple individuals based on their levels in the health monitoring database. This transfer and exchange of information between the two communicating parties is enabled through encryption and cryptographic techniques. However, the algorithms and strategies used to secure the data differ from author to author; but the concept of securing the medium remains the same. To managing and securing the patient data gets challenging when the data share occurs between various parties such as insurance organizations and other health centres. By adopting the concepts of encryption and cryptographic techniques; a patient monitoring system deployed on cloud can thus be stored and secured in real time.

Multiple research works have been published in the domain of encrypting healthcare data with the usage of AES, RSA, and DES algorithms [5][6][7]. Authors Bansal et al. 2015 in [8] created a working model in which they combined Blowfish and the RSA method. The implementation utilised Field Programmable Gate Arrays to build a distinct type of cryptography (FPGA). Unfortunately, the system remained less efficient in terms of cost and performance because it was unable to produce higher degrees of security. The system's inability to handle key sizes larger than bits was the main issue with the suggested approach. Authors Kartit Z et al. 2016 [9] used the concepts of AES and RSA encryption algorithms in order to secure the data that was being stored on cloud. This enabled to resolve the issues as faced in the previous work mentioned in [8]. AES was used as the basis for symmetric key encryption wherein the key sizes of 128 bits, 196 bits and 256 bits were used to perform cryptography on the data being provided. On the other hand; the scenarios where the key size exceeds 256 bits and resulted in the generation of 1024 bits; the implementation of RSA method was adopted for cryptography. Hence, in this way the author proposed the implementation of two algorithms thus combined as AES and RSA. However; the execution of each algorithm was dependant based on key sizes thus generated. Even though, two distinct keys were developed, employed, and shared by the two communication parties during the decryption process; the system was prone to attacks.

In contrast to the previous two works, Oladeji P. Akomolafe 2017 in [10] presented a work in which he created a novel framework of HCT that merged the operational implementations of the AES, Blake2b, and Schnorr Signature algorithms. Using the three algorithms helped a web app that was set up in the cloud to establish contact between two parties to have enough degrees of security. When a user uploaded his or her particular data to the cloud, a good level of encryption was constructed and established that allowed user authentication on the client side. Nonetheless, numerous audio, video, and image file formats were also uploaded and shared. On the other hand, authors Navdeep Singh et.al 2015 in [11] proposed a framework for

encrypting data being delivered on the cloud. They also suggested a normal and standard encryption approach. It was suggested that the data be implemented utilising algorithm pairings and the development of the AES and RSA algorithms. The corresponding data was encrypted and decrypted using both techniques. Yet, the proposed methodology was successful in preventing DoS assaults on the cloud server and offered high levels of security accuracy. Authors M. K. Sarkar et.al 2016 [12] presented a remarkably similar piece of work in which they deployed a secure model on the cloud using the encryption methods AES and RSA and an HCT. Yet one thing that set the two apart was how they generated various key sizes.

Elliptic Curve Cryptography and Diffie- Hellman ideas were used to execute cryptography in a research project being carried out by authors C. K. et al. 2017 in [13]. Combining these two different cryptographic methods improved the system model in terms of the precision and security levels attained. The use of ECC made it possible to compute the binary fields of a polynomial equation using an elliptical curve graph. The proposed method did have several drawbacks, though, such as the integrity not being balanced because of numerous attacks on the data deployed through the cloud.

However, Kanna et al. 2019 in [14] offered a similar technique to address the security vulnerabilities present in the work mentioned above in order to overcome the drawbacks of the aforementioned system. To increase security and protect the system from different attacks, ECC was used as the only encryption mechanism during construction. The key size was constructed using a large number of bits.

As opposed to the works previously stated, author Bhatt Agarwal et al. 2019 in [15] recommended the deployment of an HCT that entailed the distribution of equal data over the cloud in order to prevent data overload and the system's service delay problems. The alternative data distribution strategy was used in the algorithm's implementation, which improved the model's security while also requiring less time to compute and distributing the workload equally across the cloud.

In a research work proposed by author Vipul et al. 2006 in [18] ABE based encryption method was suggested that could efficiently manage keys being generated on both the ends of the communicating parties. Since the involvement of keys had the generation of only private key; ABE served the purpose of encrypting and protecting the user data with utmost security. However, for the process of decryption; another key was assigned which was known to the respective user and sent to him through a mail ID. This assigned secret key was used for decrypting and the data would further be accessed using ABE as the proposed encryption method. Since ABE exhibited this feature; scenarios of data exposure and collision were prevented.

2.1 Comparative Analysis

Research Author	Title	GIST	Challenges
N Kryvinska et.al, 2021 [16]	Cloud-based secure smartcard healthcare monitoring and tracking system	Patient parameters such as blood pressure, oxygen levels and pulse were calculated	No observations of synchronisation between smart cards and cloud servers

Yang et.al, 2018 [17]	A novel hybrid cloud for medical resource sharing among autonomous healthcare providers	Response time is measured in milliseconds and bandwidth in kb/sec	Usage of smart cards to only fulfil the authentication process
Kausar et.al, 2021 [19]	Iris based cancellable biometric cryptosystem for secure healthcare smart card	Performance measures of false acceptance and rejection rates are calculated	Performance measures of false acceptance and rejection rates are calculated
Li et.al, 2018 [20]	Cloud assisted mutual authentication and privacy preservation protocol for telecare medical information systems. Computer Methods Programs Biomed	Real time data upload of patients such as check-up phase, data upload, report updates, blood pressure levels are done in real time	Usage of symmetric key encryption
Al Saggaf et.al, 2019 [21]	Renewable and anonymous biometrics-based remote user authentication scheme using smart card for telecare medicine information system	Computational complexity is calculated in real time using milliseconds as the parameter and include login and registration phases	Since hashing function is used for information transfer a specific implementation of an encryption algorithm is eliminated
Kumari et.al, 2020 [22]	ECC based secure and efficient mutual authentication protocol using smart card	Response time is calculated in seconds	Deployed system does not support upload of data in various phases
P Luthra et.al, 2018 [23]	Secure file storage in cloud computing using Hybrid Cryptography Algorithm	Using steganography, key generation and sharing are monitored	Sliced data are encrypted using the RSA algorithm
Batra et.al, 2018 [24]	Secure File Storage in Cloud Computing using Hybrid Encryption Algorithm	Model merging with various techniques enhance data indexing and information retrieval	Data is distributed over a variety of multimedia files
Sai Akhil et.al, 2020 [25]	Data slicing and hybrid cryptography	The system model's integrity and confidentiality are achieved, and a process of AES encryption employed for keys with	Using steganography, key generation and sharing are monitored

		different key sizes in bytes	
Soman & Natarajan, 2017 [26]	An enhanced hybrid data security algorithm for cloud	Authentication of the system model is done using ECDSA and SHA256 algorithm	Using steganography, key generation and sharing are monitored
Bose et.al, 2020 [30]	Smart automated health machine using IoT to improve telemedicine and telehealth	Included patient information such as ECG, heart rate and blood pressure	Lacked synchronisation between system integration and cloud
Sanjuan et.al, 2020 [31]	A cryptographic smart card approach	Response time is calculated in milliseconds	Implementation of RSA did not result into generation of optimised results

2.2 Contributions

Following are the contributions of the study:

- To improve the overall security of patient health care in the cloud, by introducing a hybrid technique that would combine the concepts of AES and ECC
- Provide a time stamping mechanism that converts plain text to cypher text utilising symmetric and symmetric cryptography
- Minimize the time required for key generation, execution, encryption, and decryption in order to optimise the model and overcome the limits of the current system

3 Methodologies Used

With advancements in cloud services being made; the storage capacity for user data has exponentially increased and elevated the entire process of encryption and decryption. This not only improves data retrieval, but also eliminates the need of a third party. However, it is worthy to note here that; no cloud services can securely be stored without the implementation and adaption of encryption techniques. For this purpose, the patient data on the cloud must be stored in a secured manner so that it can be remotely accessed without any time delay. This can however be achieved by exhibiting cryptographic strategies such as symmetric and asymmetric key encryptions.

Both the above-mentioned forms of key generation follow the concepts of cryptography wherein the original data is altered and sent over a communicating channel and further recovered using a key. This facilitates the data to be secured and verifies user authentication. The key which is used in this process can either be labelled as a secret key or a public key. If the encryption process follows the concept of a secret key; the process is referred to as

symmetric encryption wherein the key remains secret to both the parties involved. One of the commonly used symmetric key encryption algorithm is referred to as Advanced Encryption Standard (AES). As per NIST [32]; the implementation of AES is considered to be as the easiest way to secure patient data on cloud with utmost security Omotosho, A et.al, 2015 [27]. In addition to securing the data; AES also increases the processing speed of the algorithm by reducing the overall key size as specified by the user Chenthara et.al, 2019 [28]. Hence the usage of AES can prove to be effective in maintaining patient data on cloud and thereby satisfy the pre-requisites of encryption and decryption mechanism to secure the data.

On the other hand; if the encryption process follows the concept of a public key; the process is referred to as asymmetric encryption wherein the key remains public to both the parties thus involved. The usage of a public key involves multiple keys (public key and private key) that are sent over a communicating channel to complete the process of encryption and decryption. One of the commonly used asymmetric key encryption algorithm is referred to as Elliptic Curve Cryptography (ECC) Abbas, A., & Khan et.al, 2014 [29]. An ECC uses the methodology of dividing working modules of a patient monitoring system into individual chunks; wherein each user like that of a patient, doctor, hospital staff etc. can individually access the monitoring system deployed on cloud with utmost security. The encrypted files present on the cloud can therefore by decrypted using a specific key shared to them through Gmail. Each user in this concept has access to his profile, where he can obtain the private key and decrypt the files, depending on his level in the database. This ensures that only a legit individual can get access to patient data and thereby eliminates the probability of data exposure and collision.

Hence for the purpose of implementation of the proposed thesis; ECC and AES are chosen as encryption algorithms since it has provided better computational complexity in comparison to other linear algorithms.

3.1 Elliptical Curve Cryptography

Elliptic Curve Cryptography, abbreviated as ECC is a type of asymmetric encryption algorithm that falls under the category of cryptography. The concept is built under the notion of an elliptical curve that is spread over a finite field. The primary usage of ECC is to secure the data from attacks. Since the implementation uses two pairs of keys, breaching the stored data becomes a significant challenge for the attacker and hence is considered to be as one of the most commonly used algorithms that provide security to data. In addition to this, it also reduces the computational complexities involved in a system model by reducing the original key size of the equations thus involved. Hence it is expected to perform better than the RSA algorithm with a 512 bit of key size. Such a form of encoding, done on the curves using mathematical and algebraic structures makes it challenging for an attacker to break the security and perform its own computations. In addition to this; the execution of an ECC algorithm is intricate and difficult to implement since it involves the usage of two keys (public key and private key). Therefore, hacking in such a two-dimensional field becomes difficult. ECC also tends to be reducing the original key size and thereby getting it accessed by only limited and authorised people thus involved in the healthcare system. Hence the proposed study tends to implement the ECC as a form of asymmetric cryptographic technique to perform patient data encryption on cloud. The explanation of the same is illustrated in figure 3.1.

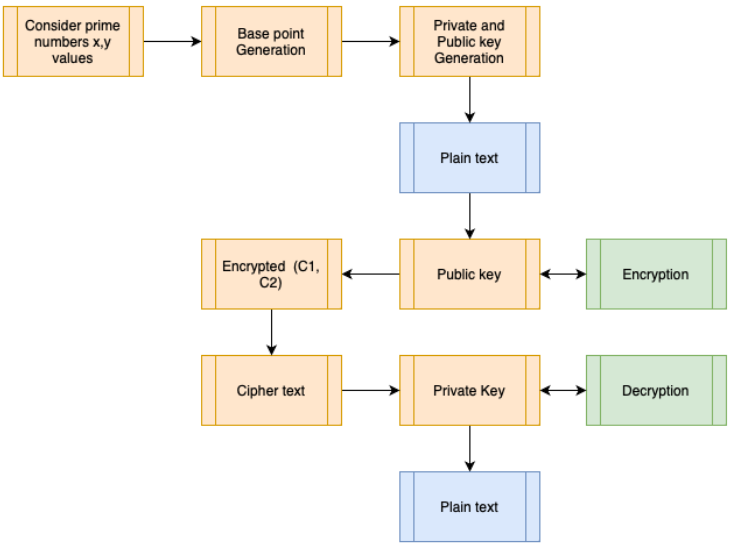

Figure 3.1: Diagrammatic Representation of ECC

3.2 Advanced Encryption Standard

Advanced Encryption Standard abbreviated as AES is a form of symmetric encryption cryptography wherein the algorithm uses only one key to encrypt and decrypt the data and thereby convert original text to cipher texts. To achieve this, it makes use of block ciphers and thereby secures the data through performance operations such as storing patient data on cloud, performing statistical analysis, upload of patient data on health care etc. Hence, it is considered to be a strategic algorithm that enhances data storage and retrieval on cloud by using one pair of keys. The block ciphers used by AES can be varied in three different key lengths and sizes as 128-, 192- and 256-bit sizes. Depending on the length and the size of the keys, the process of data encryption is performed in rounds.

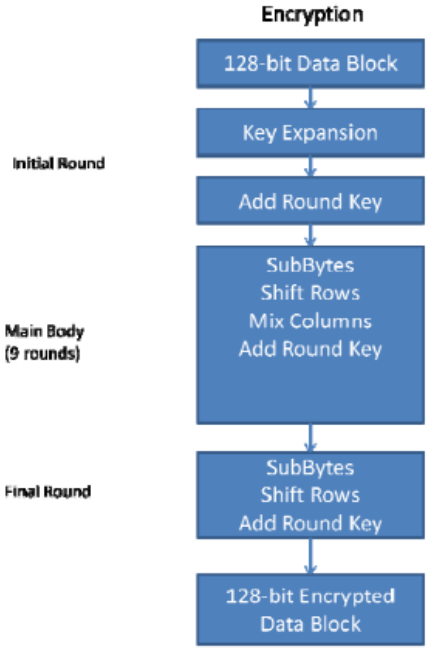

Figure 3.2: Diagrammatic Representation of AES

For instance, the numbers of rounds required in the above-mentioned key sizes are as follows:

- AES-128 would require 10 rounds of encryption performance
- AES-192 would require 12 rounds of encryption performance
- AES-256 would require 14 rounds of encryption performance

During the performance of the above functions; 10, 12 and 14 rounds are iteratively executed in loops until the final transformation of original text to cipher text is achieved. This process enhances the overall security of patient data on cloud and makes it easy during data retrieval. However, the transformations required in AES-128, AES-192 and AES-256 are pre-determined and therefore follows certain steps to perform conversions on block ciphers. The executed steps are mentioned in Figure 3.2 which represents the diagrammatic illustration of the same process. Through the steps, it can be concluded that the implementation of an AES algorithm is very feasible and easy to implement. In addition to this, its computational execution is less expensive in comparison to RSA, DSA, and ABE. Hence, for the above-mentioned reasons; the authors of the proposed study use the implementation of AES to secure patient data on cloud.

3.3 Proposed Framework

The primary aim of the research methodology is to develop a patient health care system wherein the patient and doctor could communicate with each other over cloud using MS Azure. This communication between both the parties thus involved, comprises of sharing of patient information such as his disease and necessary parameters. The information also includes sugar levels, blood pressure, oxygen saturation etc. The doctor and the patient can login on the portal using their credentials which were initially used during their registration process. The overall implementation of the research is executed on two ends and thereby can be accessed by two separate individuals thus involved. In the proposed thesis; the two communicating parties are the doctor and the patient. They can thus individually login using their ID and passwords.

Apart from the exchange of information between the communicating parties; securing, storing, and retrieving the shared information on cloud is mandatory. For this reason, the authors have implemented the conceptual theories of cryptography that makes use of symmetric and asymmetric encryption techniques. The upload of data that takes place on the doctor’s end is where the process of encryption takes place. On the other hand; the download of data on the patient's end is where the process of decryption takes place. For the purpose of encryption, we have used AES algorithm and the AES algorithm key will be encrypted using the ECC public key whereas for the purpose of decryption, the AES encrypted key will be decrypted by the ECC private key in order to decrypt the AES encrypted file. It is worthy to note here that once the keys are generated; they are communicated using a secure channel through Gmail ID of the registered user.

In addition to the execution of the thesis; it is simultaneously important to assess and evaluate the system model so that the levels of security could be maintained. This ensures that the time and phase complexities are eventually balances and thereby generated in conjunction so that the model can accomplish higher levels of security. For this to occur; the length and sizes of the keys thus generated must match with the system model so that parsing of keys could be performed. The workflow of the same can be depicted from the schematic diagram illustrated below Figure 3.3.

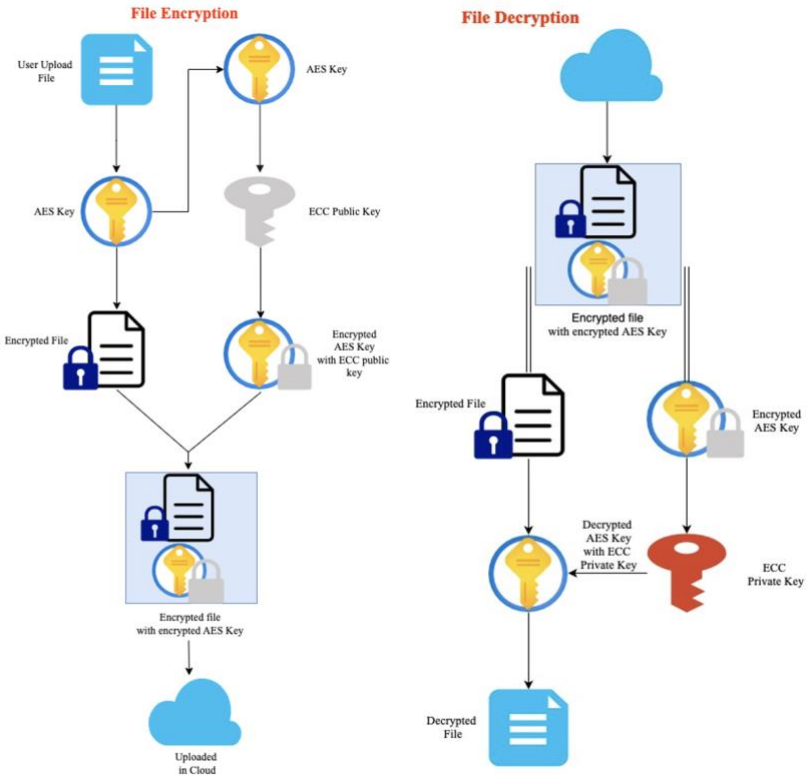

Figure 3.3: Schematic Representation

The entire process of the suggested architecture is depicted in the figure above. The implementation of the thesis thus proposed can be broken down into three different data security techniques.

- The first one is encrypted the file with AES after that the development of keys. This is the key that both users of the communication channel possess and can be used in the future to share respective files. However, this key is created via the Elliptic Curve Cryptography (ECC). Once they are generated, the keys are sent to the proper recipient
- The second stage involves sharing of the above key thus generated on both ends of the communicating channel. For the purpose of authentication, the user's user ID and password are supplied by email to the verified user. The user can acquire these common credentials by logging into his email, acquiring his login ID and password, and then entering the web server with those credentials
- Finally, AES is used to decrypt the data on the users end and thereby get access to the files thus shared by downloading them

The above framework as proposed is referred to as the hybrid-based encryption model since it combines the methodologies of AES as well as ECC to encrypt and decrypt the data. The ECC encryption algorithm is used on the doctor's end to upload patient data. Using ECC, a key is generated and transferred to the patient on his mail. In this scenario, the ECC algorithm is responsible to generate keys so that patient authentication can be performed. In addition to this; since the authentication of the patient is done through his mail ID; it becomes difficult for any hacker to get access to this generated key. Hence using this approach; a secured form of communication is established between the doctor and the patient wherein they can upload and download respective files as and when needed. The usage of this hybrid model also tends to

improve the overall security of the system and thereby keeps the data protected from attacks. The dashboard for patient and doctor can however be accessed individually through their credentials and log in ID's.

4 Implementation Details

A combined framework of ECC and AES tends to become a hybridised cryptographic approach and provides advanced encryption over cloud storage. Since the single implementation of AES encryption is slow; the hybrid method of (ECC-AES) overcomes this challenge by reducing the overall key size of the cipher text [33]. This reduced key size enables a faster mechanism of securing data and thereby leads to performance increase in the system model. The executional implementation of an ECC follows the concept of encryption and decryption using the already reduced key size. Hence, when combined with AES tends to secure the data from unauthorised access. Initially, an input is taken and encrypted from original text to cipher text through key generation and reduction of key size. The generated key is further used by the AES algorithm to decrypt the cipher text to its original text. In this manner the entire system is secured over cloud.

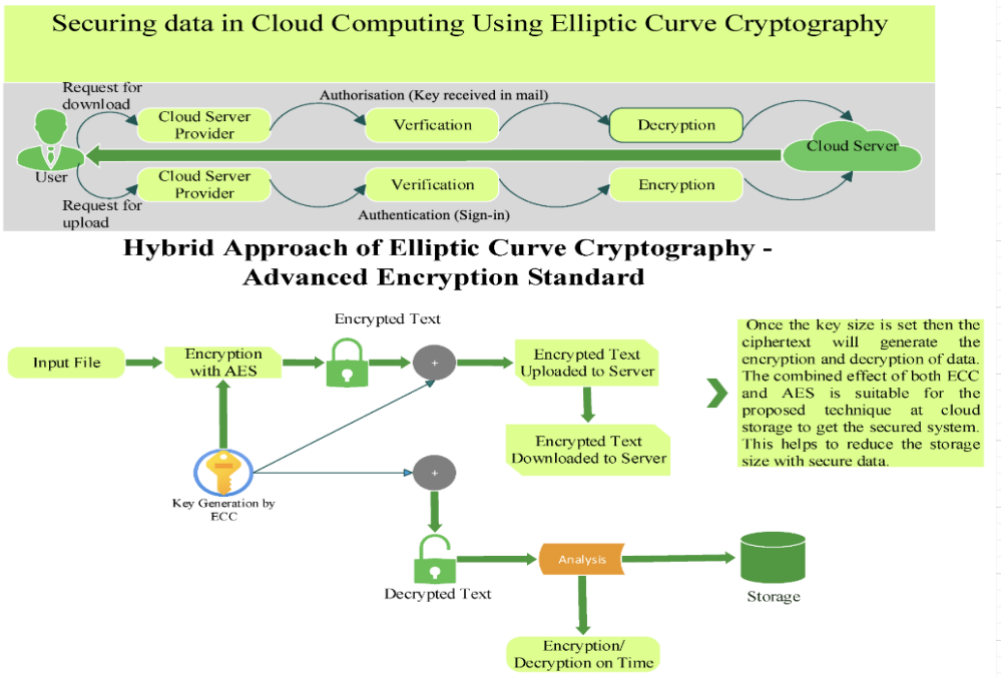

Figure 4: Block representation of AES and ECC [34]

Through the figure above, it can be observed that the combination of AES and ECC can secure information on cloud in a secured manner. The novelty thus introduced can be witnessed in the representation; wherein data transmission occurs from website server to cloud by using encryption techniques of ECC and decryption techniques of AES. In addition to this; novelty is also proposed to be introduced in terms of computational and time complexities. It is also worthy to note here that the proposed system protects the patient data from getting exposed by attackers; since the upload and download of the input file takes place through an encryption approach that involves two cryptographic algorithms.

4.1 System Architecture

The aim of the proposed research study is to secure patient data in the cloud based EHR system and file communications, such as file sharing. The EHR and respective patient information is expected to be shared between the patient and his respective doctor. An added feature in the proposed web app is that the file of the patient can also be shared between multiple doctors if the patient wishes to do so. To accomplish the aim of this study; the author of the research has put forward the concepts of encryption techniques and cryptography so that secured transfer of information exchange can occur between the patient and the doctor. Since the webserver is deployed on cloud using MS Azure, patient data is at risk to exposure and data loss. For this purpose, a hybrid cryptographic technique (HCT) that combines the fundamentals of ECC and AES encryption are used.

The deployment of the web server occurs on cloud using MS Azure and can thereby be accessed by the doctor as well as the patient.

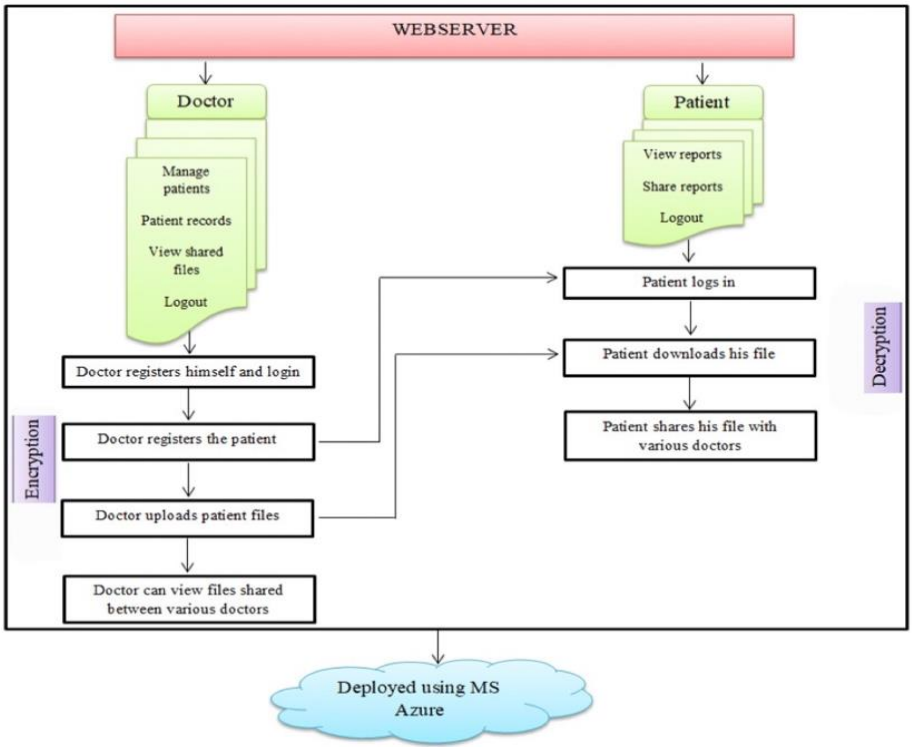

Figure 4.1: System Architecture

4.1.1. Web server accessed by doctor

Initially, the doctor registers himself on the server using his name, mail ID, mobile number and creates his password. He then logs into the app using the credentials thus created. The doctor is then redirected to an admin panel wherein a dashboard with the following options is visible:

1. Manage patients 2. Patient records 3. View shared files 4. Logout

A. Front End

1. In the section of manage patients; the doctor can register information of his patients and add them under his list. For this purpose; patient's information such as his name, mail

ID, contact information and address is required. Once the doctor adds this information, he can thus access the record files of the patient and thereby address their health issues.
2. The doctor then uploads the respective prescription and reports of the patient which is further downloaded on the other end by the patient.
3. In addition to registration and managing of patient records; the doctor can also view all the files which the patient shares with other doctors of his choice for second reference.

B. Back End

However, the above-mentioned process occurs on the front end on the app and is visible to the doctor. The backend of this step occurs through the process of cryptography carried out through hybrid encryption.

1. The doctor registers his patient; the patient is notified on his mail ID and is provided with a password.
2. Next; when the doctor uploads a prescription or the report of a patient; the process of hybrid encryption takes place, and a key is generated. This key is further sent to the patient on his mail ID.
3. Finally, the feature of file share between different doctors also occurs through encryption; wherein an OTP is generated and sent to the registered doctor so that patient data is not misplaced.

4.1.2. Web server accessed by patient

Initially, the patient login into the web app; by entering his mail ID and password. The password entered here by the patient; is the one sent to him on his mail when he was initially registered by the doctor as mentioned in section 4.1.1 – A (1). The patient is then redirected to an admin panel wherein a dashboard with the following options is visible:

1. View reports 2. Share reports 3. Logout

A. Front End

1. In the section of view reports; the patient can view the name of his doctor, his contact number and the prescription given on a specific date.
2. The view report also contains the file which is uploaded by the doctor. The patient can thus download the respective file using an option provided.
3. Another option provided to the patient is that of sharing his reports; wherein the patient can share his downloaded reports with another doctor for a second opinion.

B. Back End

However, the above-mentioned process occurs on the front end on the app and is visible to the patient. The backend of this step occurs through the process of cryptography carried out through hybrid decryption.

1. The patient gets access to the web app by entering his credentials.
2. Next; when the patient downloads his reports; the process of hybrid decryption takes place. The key used here to decrypt the cipher text to the original text is already received by the patient on his mail by the doctor as mentioned in 4.1.1 – B (2).
3. Finally, the feature of file share between different doctors also occurs through encryption; wherein an OTP is generated and sent to the registered doctor so that patient data is not misplaced.

5 Results

The files utilized in the experiment range in size from 1 to 30 MB. As mentioned below, this study gives a very excellent performance assessment of a design system to execute two effective comparison approaches. The proposed EHR system is first compared to compute the values of encryption and decryption times of various popular formats for storing medical records (PDF, JPEG, PNG, XLS, DOCX, PPTX,.TXT) where the base size of all file is 1 Mb . In Figure 5, the suggested design gave complete information about the encryption and decryption operations, including the execution time, original text file, resulted encrypted text file, and resulted decrypted file. In accordance with the results, the Txt file type surpassed the other file types in terms of total time necessary to complete the encryption and decryption processes, as well as calculating the assessed time of a cryptographic method during the encryption and decryption procedures, because it utilized less time.

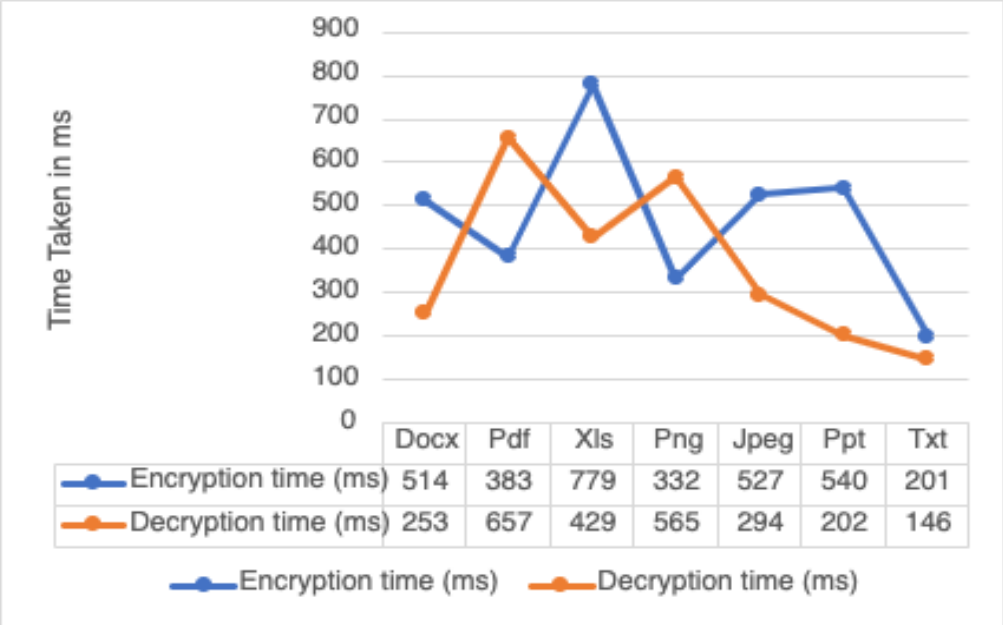

Figure 5: Time Evaluation of different files in proposed algorithm

The second contrast is between three hybrid encryption techniques in which RSA (Rivest-Shamir-Adleman) is public key encryption method which provides great security and is frequently used for key exchange and digital signatures and DES (Data Encryption Standards) is a symmetric key encryption algorithm that is widely used in cryptography it was one of the first widely used symmetric algorithms. Three methods are employed in this experiment to encrypt and decrypt the distinct size of pdf files. To improve the accuracy of the experimental findings, the approach of averaging the results of numerous runs is used, and the value with a big error is deleted. To achieve the experimental results, eight pdf files (1.19 MB, 3.57 MB, 7.14 MB, 10.7 MB, 17.8 MB, 21.4 MB, 25 MB, and 28.5 MB) were used. In each experiment, three hybrid algorithms (AES and ECC, AES and RSA, DES and ECC) were compared, and the differences in encryption and decryption time were analyze. The encryption algorithm of the three is provided in Fig 5.1 for different file sizes.

The execution time of the DES and ECC hybrid algorithm grows continuously with file size. The AES and ECC hybrid encryption time grows with the file, although at a modest rate. The encryption time of the AES and RSA hybrid method grows at a slow but steady rate.

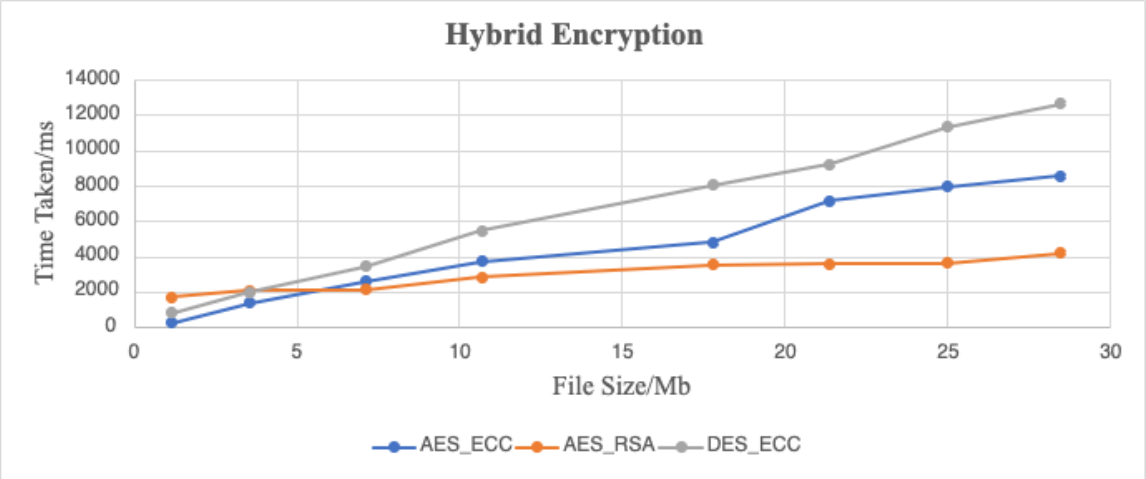

Figure 5.1: Encryption evaluation of hybrid cryptography algorithms

When the file size is 1.19 MB, the efficiency of the AES and ECC hybrid algorithm is 67.15 times that of the AES_RSA algorithm and 2 times that of the DES and ECC algorithm, but when the file size is 28.5 MB, the efficiency is 5.06 times that of AES and RSA but the ratio is the same as 2 times in the DES and ECC algorithm. Figure 5.1 shows how efficiency tends to rise as the file size grows.

According to experimental results, the decryption time of the AES and ECC, DES and ECC hybrid algorithms grows at a slow but steady pace as file size increases. The AES and RSA algorithm improves significantly. The AES and ECC, DES and ECC hybrid algorithms' decryption times are steady at a specific number, although AES and RSA values are from both algorithms. When compared to the other two hybrid methods AES and RSA, the increase in decryption performance has a considerable influence when dealing with huge data. When the file is 21.4 MB in size. It has 1.5 times increased. Using the proposed program, the performance of every approach was tested in terms of speed, memory file size, and throughput. The decryption time schedules of the three techniques are analyse, as shown in Figure 5.2.

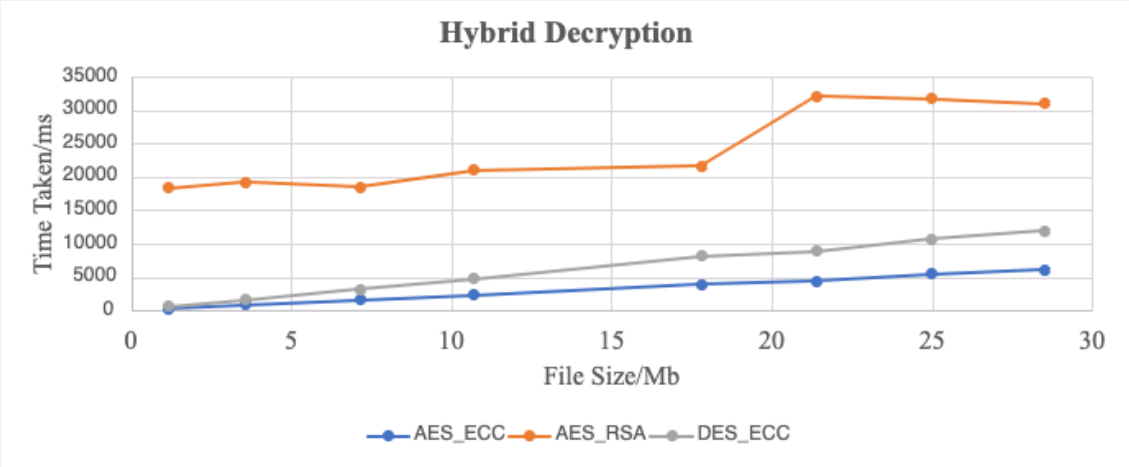

Figure 5.2: Decryption evaluation of hybrid cryptography algorithms

The encryption and decryption time of any cryptography technique is the amount of time it takes for the encryption algorithm to convert plain text to cipher text and cipher text to plain text. The encryption and decryption times are used to compute the throughput of any cryptographic operation, which is determined as the total encrypted plaintext (in bytes) divided by the encryption or decryption time (in milliseconds).

$$\text{Throughput} = \frac{\text{Total Text files size in (MB)}}{\text{Total Evaluation Time of Algorithm in (ms)}}$$

Any cryptographic algorithm's throughput reflects its speed during the encryption and decryption procedures. As the throughput value of a cryptographic technology increases, the power consumption of that technique decreases due to the lowered time during the encryption and decryption procedures [35].

Hybrid Cryptography	Total Average Time for Encryption	Total Average Time for Decryption	Encryption	Decryption
AES and ECC	36274	24721	3.178	4.664
AES and RSA	23546	193142	4.896	0.596
DES and ECC	52784	49624	2.184	2.323

Table 3: Throughput of Hybrid Cryptography algorithms

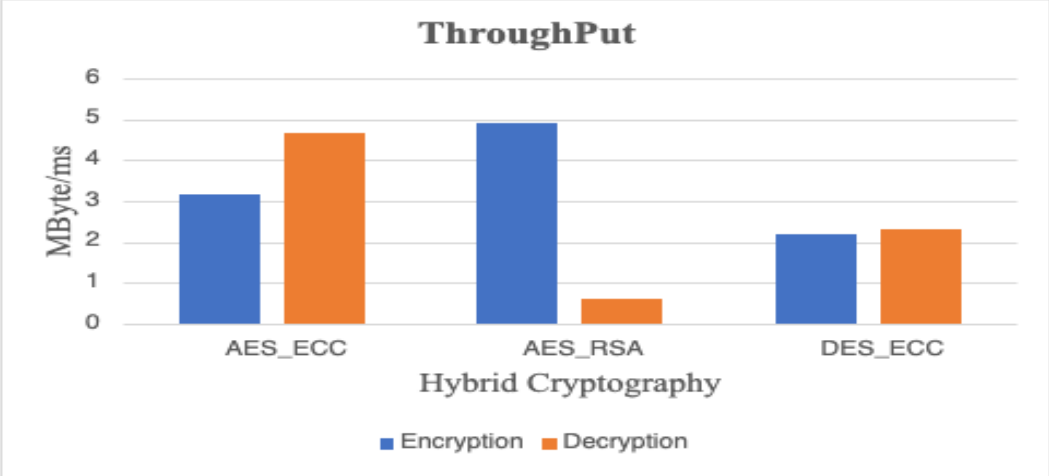

Figure 5.3: Throughput of Hybrid Cryptography algorithms

The throughput of each hybrid algorithm evaluating the same pdf files was shown in Table 3 and Fig 5.3. AES and RSA had the larger throughput; it can encrypt more than 4.89 MB in one millisecond, the second better algorithm in terms of encryption is AES and ECC; it can encrypt more than 3.17 MB in one millisecond, while DES and ECC encrypt 2.18 MB in one millisecond, which is the lowest among them, but in decryption there is a significant difference in AES and RSA encryption and decryption performance, however there is no difference between DES and ECC and AES and ECC encryption and decryption throughput. Despite this, AES and ECC has a better standing performance among other algorithms in terms of processing time.

Based to the results, AES and ECC is the fastest encryption approach in terms of speed and throughput implying that may achieve more efficiency in less time. DES and ECC performed second best throughout the encryption and decryption operations, whereas AES and RSA performed similarly. Finally, in terms of speed and throughput, DES and ECC had the lowest performance level. In an emergency, time is of the essence for effective and quick treatment.

6 Discussion

Health care experts must quickly assess the patient's condition. The medical conditions of the patients and their diagnosis reports create a lot of data, which must be transmitted quickly across treatment teams during the entire process. In this situation, our proposed algorithm is faster than compared hybrid algorithms. To monitor real-time EHR activities on the cloud with HCT, when AES and ECC used together can provide a strong and fast hybrid cryptographic technique for securing real-time EHR on cloud activities This makes them a good choice for securing real-time EHR on cloud activities.

7 Conclusions and Future Scope

Patient health care and monitoring systems in the existing domains are going through multiple challenges of security. This occurs because the system is deployed on cloud and storing sensitive data in such a scenario is a difficult task. Hence protecting this data is mandatory, to ensure that the privacy of the patient is maintained. For this to occur, all the respective security issues must be taken into consideration throughout the initial phase of designing the system model. Once the current scenario and parametric conditions of a patient is known such as his BP rate, pulse etc. he is expected to be monitored using the health care server. This not only helps the doctor to treat the patient; but also assists in keeping a historical record of the patient. The primary aim of the research study thus proposed; is to conduct the implementation of the same using the concepts of cryptography wherein two encryption algorithms are combined together so as to form a Hybrid Cryptographic Technique (HCT). The adaption of an HCT enables to reduce the size of the key thus generated and thereby increase the performance of the overall system. The workflow of the study follows with a health care server deployed on cloud using MS Azure. The website can be accessed by the doctor as well as the patient. The doctor can register himself and log in using his credentials. The doctor is also given the authority to register the respective patients from his domain and upload prescriptions according to the treatment thus required. The encryption process used in this scenario; is done through the implementation of ECC encryption; wherein the upload of patient files takes place by encrypting the original text to cipher text using a random key thus generated. This key is further sent to the registered patient on his mail ID, and he can thus download his reports on the web server. The decryption process used in this scenario; is done through the implementation of AES encryption. Therefore, in this manner a combined approach of ECC and AES encryption techniques are used. In the future, the same work can be extended to be simultaneously deployed on cloud so that the implementation of the website can be accessed from the mobile devices as well.

References

[1] Ross, M.K., Wei, W. and Ohno-Machado, L., 2014. "Big data" and the electronic health record. *Yearbook of medical informatics*, *23*(01), pp.97-104.

[2] Zhang, Q., 2021, January. An overview and analysis of hybrid encryption: The combination of symmetric encryption and asymmetric encryption. In *2021 2nd international conference on computing and data science (CDS)* (pp. 616-622). IEEE.

[3] Gupta, K. and Silakari, S., 2011. Ecc over rsa for asymmetric encryption: A review. *International Journal of Computer Science Issues (IJCSI)*, *8*(3), p.370.

[4] Barker, E., Chen, L., Keller, S., Roginsky, A., Vassilev, A. and Davis, R., 2017. *Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography*(No. NIST Special Publication (SP) 800-56A Rev. 3 (Draft)). National Institute of Standards and Technology.

[5] Oh, J.Y., Yang, D.I. and Chon, K.H., 2010. A selective encryption algorithm based on AES for medical information. *Healthcare informatics research*, *16*(1), pp.22-29.

[6] Nidhya, R., Shanthi, S. and Kumar, M., 2021. A novel encryption design for wireless body area network in remote healthcare system using enhanced RSA algorithm. In *Intelligent System Design: Proceedings of Intelligent System Design: INDIA 2019* (pp. 255-263). Springer Singapore.

[7] Pariselvam, S. and Swarnamukhi, M., 2019, March. Encrypted cloud based personal health record management using DES scheme. In *2019 IEEE International conference on system, computation, automation and networking (ICSCAN)* (pp. 1-6). IEEE.

[8] Bansal, V.P. and Singh, S., 2015, December. A hybrid data encryption technique using RSA and Blowfish for cloud computing on FPGAs. In *2015 2nd international conference on recent advances in engineering & computational sciences (RAECS)* (pp. 1-5). IEEE.

[9] Kartit, Z., Azougaghe, A., Kamal Idrissi, H., El Marraki, M., Hedabou, M., Belkasmi, M. and Kartit, A., 2016. Applying encryption algorithm for data security in cloud storage. In *Advances in Ubiquitous Networking: Proceedings of the UNet'15 1* (pp. 141-154). Springer Singapore.

[10] Akomolafe, O.P. and Abodunrin, M.O., 2017. A hybrid cryptographic model for data storage in mobile cloud computing. *International Journal of Computer Network and Information Security*, *9*(6), p.53.

[11] Singh, N. and Kaur, P.D., 2015. A hybrid approach for encrypting data on cloud to prevent DoS attacks. *International Journal of Database Theory and Application*, *8*(3), pp.145-154.

[12] Sarkar, M.K. and Kumar, S., 2016, December. Ensuring data storage security in cloud computing based on hybrid encryption schemes. In *2016 fourth international conference on parallel, distributed and grid computing (PDGC)* (pp. 320-325). IEEE.

[13] Kumar, C. and Vincent, P.D.R., 2017, November. Enhanced diffie-hellman algorithm for reliable key exchange. In *IOP conference series: materials science and engineering* (Vol. 263, No. 4, p. 042015). IOP Publishing.

[14] Prabu Kanna, G. and Vasudevan, V., 2019. A fully homomorphic–elliptic curve cryptography based encryption algorithm for ensuring the privacy preservation of the cloud data. *Cluster computing*, *22*(Suppl 4), pp.9561-9569.

[15] Bhatt Agarwal, R. (2019). A technological review on scheduling algorithm to improve performance of cloud computing environment. Int. J. Innov. Technol. Explor. Eng., 8(6), 166–172.

[16] Senthilkumar, S., Brindha, K., Kryvinska, N., Bhattacharya, S. and Reddy Bojja, G., 2021. SCB-HC-ECC–based privacy safeguard protocol for secure cloud storage of smart card–based health care system. *Frontiers in Public Health*, *9*, p.688399.

[17] Yang, Y., Li, X., Qamar, N., Liu, P., Ke, W., Shen, B. and Liu, Z., 2018. Medshare: a novel hybrid cloud for medical resource sharing among autonomous healthcare providers. *IEEE Access*, *6*, pp.46949-46961.

[18] Goyal, V., Pandey, O., Sahai, A. and Waters, B., 2006, October. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM conference on Computer and communications security* (pp. 89-98).

[19] Kausar, F., 2021. Iris based cancelable biometric cryptosystem for secure healthcare smart card. *Egyptian Informatics Journal*, *22*(4), pp.447-453.

[20] Li, C.T., Shih, D.H. and Wang, C.C., 2018. Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems. *Computer methods and programs in biomedicine*, *157*, pp.191-203.
[21] Al-Saggaf, A. A., & Sheltami, T. R. (2019, March). Renewable and anonymous biometrics-based remote user authentication scheme using smart cards for telecare medicine information system. In 2019 Advances in Science and Engineering Technology International Conferences (ASET) (pp. 1-6). IEEE.
[22] Kumari, A., Jangirala, S., Abbasi, M.Y., Kumar, V. and Alam, M., 2020. ESEAP: ECC based secure and efficient mutual authentication protocol using smart card. *Journal of Information Security and Applications*, *51*, p.102443.
[23] Bala, B., Kamboj, L. and Luthra, P., 2018. Secure File Storage In Cloud Computing Using Hybrid Cryptography Algorithm. *International Journal of Advanced Research in Computer Science*, *9*(2).
[24] Batra, M., Dixit, P., Rawat, L. and Khalkar, R., 2018. Secure file storage in cloud computing using hybrid encryption algorithm. *International Journal of Computer Engineering and Application*, *12*(6), pp.30-36.
[25] G. Sai Akhil, G. Kaarthikeyan, D. Aswin, and V. B.S, (2020). DATA SLICING AND HYBRID CRYPTOGRAPHY. Dogo Rangsang Res. J., 10(07), 118–125.
[26] Soman, V.K. and Natarajan, V., 2017, July. An enhanced hybrid data security algorithm for cloud. In *2017 International conference on networks & advances in computational technologies (NetACT)* (pp. 416-419). IEEE.
[27] Omotosho, A. and Emuoyibofarhe, J., 2015. A criticism of the current security, privacy and accountability issues in electronic health records. *arXiv preprint arXiv:1501.07865*.
[28] Chenthara, S., Ahmed, K., Wang, H. and Whittaker, F., 2019. Security and privacy-preserving challenges of e-health solutions in cloud computing. *IEEE access*, *7*, pp.74361-74382.
[29] Abbas, A. and Khan, S.U., 2014. A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. *IEEE journal of Biomedical and health informatics*, *18*(4), pp.1431-1441.
[30] Ganesh, D., Seshadri, G., Sokkanarayanan, S., Bose, P., Rajan, S. and Sathiyanarayanan, M., 2020, October. Autoimpilo: Smart automated health machine using iot to improve telemedicine and telehealth. In *2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)* (pp. 487-493). IEEE.
[31] Sanjuan, E.B., Cardiel, I.A., Cerrada, J.A. and Cerrada, C., 2020. Message queuing telemetry transport (MQTT) security: A cryptographic smart card approach. *IEEE Access*, *8*, pp.115051-115062.
[32] Nechvatal, J., Barker, E., Bassham, L., Burr, W., Dworkin, M., Foti, J. and Roback, E., 2001. Report on the development of the Advanced Encryption Standard (AES). *Journal of research of the National Institute of Standards and Technology*, *106*(3), p.511.
[33] Rehman, S., Talat Bajwa, N., Shah, M.A., Aseeri, A.O. and Anjum, A., 2021. Hybrid AES-ECC model for the security of data over cloud storage. *Electronics*, *10*(21), p.2673.
[34] Rehman, S., Talat Bajwa, N., Shah, M.A., Aseeri, A.O. and Anjum, A., 2021. Hybrid AES-ECC model for the security of data over cloud storage. *Electronics*, *10*(21), p.2673.
[35] Latif, I. H. (2020, February 1). Time Evaluation Of Different Cryptography Algorithms Using Labview. IOP Conference Series: Materials Science and Engineering, 745(1), 012039.