# Development of Secure Cloud-Based Healthcare Management Using Optimized Elliptic Galois Cryptography


**V. Gokula Krishnan, D. Siva, S. MuthuSelvi, T. A. Mohana Prakash, P. A. Abdul Saleem, and S. Mary Rexcy Asha**

**Abstract** The ever-increasing amount of e-medical data poses a security risk because of technological advancements in the healthcare business. An unstructured and large amount of unstructured data is generated by the healthcare data management system because of the wide variety of data formats that are used to capture patient information. Branches of hospitals can also be found in different parts of a city or state. Health information on patients that is kept in multiple places must be merged from time to time for research purposes. Cloud-based healthcare management systems can be an effective solution for storing and managing health care data more

V. Gokula Krishnan (✉)
Department of CSE, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (SIMATS), Thandalam, Chennai, Tamil Nadu 602105, India
e-mail: gokul_kris143@yahoo.com

D. Siva
Department of Computer Science, Faculty of Science and Humanities, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu 600089, India
e-mail: d.siva885@gmail.com

S. MuthuSelvi
Department of CSE, Vel Tech Multi Tech Dr Rangarajan Dr Sakunthala Engineering College, Avadi, Chennai, Tamil Nadu 600062, India
e-mail: muthuselvis@veltechmultitech.org

T. A. Mohana Prakash
Department of CSE, Panimalar Engineering College, Poonamallee, Chennai, Tamil Nadu 600123, India
e-mail: tamohanaprakash@gmail.com

P. A. Abdul Saleem
Department of CSE, CVR College of Engineering, Mangalpally, Hyderabad, Telangana 501510, India
e-mail: drsaleemprincipal@gmail.com

S. Mary Rexcy Asha
Department of IT, Panimalar Engineering College, Poonamallee, Chennai, Tamil Nadu 600123, India
e-mail: rexcyasha@gmail.com



J. Hemanth et al. (eds.), *Intelligent Cyber Physical Systems and Internet of Things*, Engineering Cyber-Physical Systems and Critical Infrastructures 3,
https://doi.org/10.1007/978-3-031-18497-0_38

effectively. However, security is the most pressing issue with a cloud-based healthcare system. Elliptic Galois Cryptography (EGC) is used in this study to encrypt medical data files, and the value of the Galois field is determined using the Mayfly Algorithm. As a result, the proposed model is referred to as a "optimal EGC". Use of the elliptic curve over a Galois field in elliptic curve cryptography reduces rounding errors. The healthcare data is protected in terms of both confidentiality and integrity when it is shared via the health cloud. Experiments have shown that the ideal solution can be computed more quickly in terms of file upload and download speeds as well as key generation and generation time. Additionally, it protects healthcare data from being tampered with during transmission via the health cloud.

**Keywords** Cloud computing · Security · Key generation · Mayfly algorithm · Elliptic Galois cryptography · Medical data

## 1 Introduction

When it comes to health care, the wearable technology is kindly spreading its tentacles to include not only all walks of hominid life, but also challenge the stowed huge health care data [1]. There are many different kinds of health care data, and they are made at a high rate, making it challenging to keep them locally. So the need for medical media applications like multimedia email, presentations, high quality audio and video sharing and shared papers has increased exponentially [2, 3]. In the healthcare industry, all patient records must be stored in the Cloud for future reference. This study examines the day-to-day operations of the health care business. Computational and processing challenges are plaguing the current health care business. Physical storage, security and medical errors are inherent issues in the traditional healthcare industry. It is critical to keep patient records safe since they include sensitive information. Patient data is being compromised by a number of issues in the current system. It takes up a lot of memory space, which is not cost-effective [4, 5].

In order to protect patient information, the cloud offers a high level of security. Prescription retrieval is easy because the patient's info is stored in the cloud, so they may access it whenever they want [6]. Because the data is stowed in the cloud, anyone with a mobile device, such as a smartphone or PDA, can access it without requesting specific permission. One of the most dynamic sectors of the information technology business is the healthcare sector, where cloud computing is becoming increasingly important [7, 8]. Internet-enabled devices can access health-care information throughout the world thanks to cloud computing technology. The medical community can also benefit from the exchange of resources and information with other leading researchers in the same subject around the globe. To improve and develop the current health care industry, this study is being conducted. Anuradha et al. [9] Despite the advantages of cloud-based health care schemes, many doctors and healthcare institutions are reluctant to utilize them because of the risk of data

breach. Also, because of the subtle nature of the data being kept and retrieved, numerous health care organizations are avoiding public cloud and installing private cloud services in its place [10].

The electronic health annals must be securely transferred via networks in order to protect patient confidentiality and data integrity. In [11, 12], the drawbacks of using a cloud database to store health information are discussed. For the protection of electronic health records during transmission, a cryptosystem is typically needed. Security of user data has been achieved by the employment of conventional methods such as the Rivest–Shamir–Adleman (RSA)-based system [13, 14], and the encryption of user data [15]. Large keys and complicated computations make it difficult to use such systems on mobile devices, which is another drawback of these approaches. The use of Elliptic Curve Cryptography (ECC) in cryptosystems has grown in recognition and use during the past several years. In order to achieve great scalability and efficiency, ECC reduces the key complexity by using smaller key lengths. In order to store and share health data in the cloud, users must encrypt their data before uploading it to the servers. The health cloud will benefit from this research because of the optimized EGC implementation, which will allow it to provide better healthcare services while maintaining the integrity of patient data.

In order to build an Access Control List (ACL), the TTP-CS receives healthcare data, a list of CUs, and the necessary criteria from the data owner. Later, the encrypted data is transferred to the HC on behalf of the CU for storage. If the CU is interested in accessing health data files, the TTP-CS will get a download request. The following are a few of the methodology's most significant benefits:

- Stronger encryption methods ensure the safety of patient data in the health cloud.
- To ensure data security and speed, the health cloud uses an EGC mechanism that is tuned for scalability and uploading speed.
- It provides a high level of protection for data from insider threats.

The rest of this paper is prearranged as follows. Section 2 delivers a comprehensive review of the relevant scholarly literature. With the help of an overall system design, the proposed methodology is clarified in Sect. 3. Section 4 details the proposed system's performance evaluation, and Sect. 5 closes the article with recommendations for future research.

## 2 Related Works

In order to protect against smart health threats, Zhang et al. implemented CP-ABE (Ciphertext Policy Attribute Based Encryption). Smart healthcare's application of CP-ABE brings with it a unique set of challenges [16]. It was created to address these issues: a smart health access control system that takes privacy into account. In PASH, only the name attribute is made public, while the value of the access policy attribute is hidden in encrypted smart health records. In addition, attribute values

typically contain more private information than other types. In this decryption test, PASH is able to successfully decrypt SHR (it requires few bilinear-pairings).

Mobile Healthcare Social Networks are plagued by privacy concerns (MHSN). MHSN profile matching and data sharing are planned by Huang et al. [17] in the cloud. Identity Based Broadcast Encryption (IBBE) is used to outsource encrypted data to the cloud (IBBE). In addition, the doctor's group receives data fast and safely. Using attribute-based conditional data re-encryption, the doctor's referral is disseminated throughout the network to another doctor. A new enciphered text is generated from the encrypted one (without leaking the sensitive information).

While integrating and exchanging E-health information, this book sought to address security and privacy concerns by providing a solution for Internet applications. Bao and colleagues [18] have presented a signal scrambling technique based on the application layer. To protect patient information, a minuscule amount of data is used to scramble the original. VOLU It uses either a random generator or a piece of data to derive the small data.

Masood et al. [19] established a six-step architecture for measuring the patient's physiological characteristics in Sensor Cloud Infrastructure (SCI). It begins with a preliminary selection, followed by an assessment of the patient's physiological parameters and a security analysis. Finally, it estimates the functioning of the system. Cloud computing is a promising tool for healthcare data security. It's a requirement, along with other security measures, while communicating electronically. Mbonihankuye et al.'s [20] leading strategy is the Health Insurance Probability and Accountability Act (HIPAA): [20]. Different analytical and conservational procedures can be used to ensure that healthcare data is properly recorded and kept.

Data leaks and attacks on the cloud distributor may occur when the medical data is being published. The AFBS WOA algorithm, created by Thanga Revathi, et al. [21], combines AFBSO (Adaptive Fractional Brain Storm Optimization) with the Whale Optimization technique to address this issue [20, 21] (WOA). A new AFBS WOA algorithm generates the key matrices coefficients needed to retrieve a corrupted database and keep patient information private in the cloud. The secret key was calculated using a fitness function that incorporated utility and privacy considerations. A secure database can be built by multiplying the input database by a key matrix created by Tracy–Singh using the Tracy.

Kumar et al. [22] extremely difficult to constantly monitor the central storage of health records that are vulnerable to security risks. For this reason, in order to protect confidential patient information, this study uses a block chain technology and a digital signature with authentication to protect it, as well as a cloud-based model to ensure the information's authenticity and reliability. Traditional methods for preserving medical records were studied and compared to the model presented in the study, in terms of response time and the cost of storing and retrieving records.

Smys [23] new technologies, such as sensor networks and smart monitors, have altered this picture by leveraging mobile devices and internet services. This has improved practical healthcare through predictive modeling and the acquisition of

more detailed individual measurements. A large amount of data allows researchers to analyse patterns [24] and trends in order to provide solutions that improve medical treatment while keeping costs down, while also ensuring that human lives are not put at risk. The survey on the accuracy and predictive power of big data analysis in the health care system is presented in this study.

## 3 Proposed System

An outline of a way for safely transferring healthcare data between cloud systems is provided here.

### *3.1 Architecture Overview*

The following entities make up an efficient healthcare system based on EGC's overall architecture (Fig. 1):

**HC**: Users can store, update, and back up healthcare data using cloud services provided by the HC All cloud services are supported by the HC's server, which houses all of the healthcare data. The health cloud's data had to be protected from a variety of dangers. Encryption of data in the health cloud ensures the privacy of patient records.

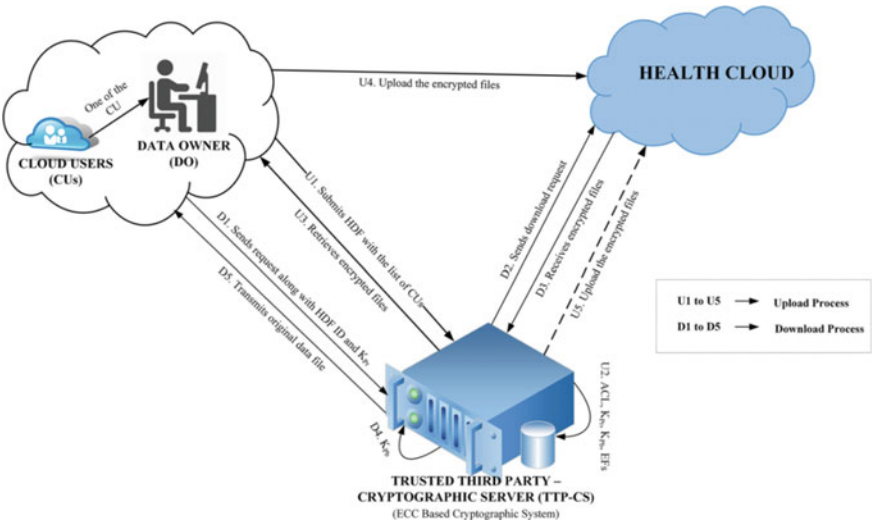


**Fig. 1** Architecture of optimized EGC-based secure health cloud

**TTP-CS**: TTP-CS is the third-party-owned trusted entity that performs the cryptographic process outside of the cloud. The ECC algorithm has been modified in this mechanism's design to ensure the security of sensitive healthcare records. In order to ensure that healthcare data may be shared in a secure manner, it is responsible for data confidentiality, integrity, key management.

**CUs**: The health cloud's clients are the cloud's users (such as researchers, analysts, physicians, and others). Registration of CUs with the TTP-CS is required in order to carry out security services. Only one CU will own each data file, while all other CUs will be consumers of that information.

## *3.2 System Model*

For the safe transfer of medical data files to and from the cloud, this architecture supports asymmetric or public key cryptography. The TTP-CS receives a list of CUs and a patient health information file from the DO. It is as a result of this that TTP-CS generates two random 256-bit keys, the public key (K Pb) and private key (K Pr). An asymmetric key algorithm can be made to run for a shorter or longer period of time using several techniques. K Pb and K Pr are generated by using the SHA-256 hash function on a random number RN. For the encryption and decryption of healthcare data, it is used further. After the encryption or decryption procedure, no one has access to the complete key. For each CU, TTP-CS generates a unique K Pb that can be freely shared and used in the encryption process. However, K Pr is only known to the decryption unit and is not shared with any other units. Security objectives can be achieved by implementing these cryptographic operations.

### 3.2.1 Loading a File to HC

The TTP-CS receives the request for encryption when a CU wants to upload healthcare data to the health cloud. Access privileges are mentioned in the HDF and the cloud user's list. Access to HDF may be Read-only or Read–Write depending on the CUL's permissions for each CU. The TTP-CS creates the Access Control List (ACL) for healthcare data using CUL. The data owner will inform the novel CUL to the TTP-CS while the HDFs are being shared with a new center. Otherwise, it only transmits the center ID of the last remaining center in the chain of transmission. ACLs for each HDF are created and maintained by the TTP-CS once the encryption requisition has been received. The ACL is made up of data about files, such as the file's ID, size, and owner ID, as well as metadata describing how the item was shared. The TTP-CS makes K Pr and K Pb for each CU after constructing the ACL. The HDF is then encrypted with an EGC-optimized encryption technique.

Elliptic Galois Cryptography

Because of its foundation in elliptic curve theory, ECC is usually referred to as the public key encryption method. Instead of using conventional methods, the keys are created by utilizing the features of elliptic curve equations. EGC is employed in the proposed project. Elliptic curves over Galois fields (Fa) are used to improve calculation efficiency and eliminate rounding mistakes. It is possible to determine the Galois field's value by utilizing the Mayfly algorithm's best answer for the ideal value.

**Mayfly Algorithm**

The Mayfly method is used in this work to maximize CNN's learning rate. To put it another way, Zervoudakis and his colleagues have presented a variation on PSO that incorporates the best of PSO, GA and FA. Because it has been demonstrated that PSO requires some modifications to ensure an optimal point when performing in high-dimensional spaces, researchers trying to improve the performance of the PSO algorithm using techniques like crossover and local search now have a powerful hybrid algorithmic structure based on the behavior of mayflies. A possible solution to the problem can be found by examining the mayfly's location in the search space. The following is the flowchart for the algorithm. In the beginning, two groups of mayflies, one for each sex, are randomly formed. Each mayfly is randomly placed in the problem space as a potential solution and its performance is evaluated using the predetermined objective function, f, which is represented by the vector x =(x 1,…,x d) (x). The velocity of a mayfly is defined as the change in its position, and the flying direction of each mayfly is a dynamic interaction of individual and communal flying experiences. It is also possible for each mayfly to modify their trajectory toward their personal best (pbest) and the best position obtained by any swarm mayfly to date (gbest).

(a) **Movement of male mayflies**
It follows that the location of each male mayfly in a swarm is determined by both its own knowledge and that of its neighbors, as the males gather in swarms.

(b) **Movement of female mayflies**
Female mayflies do not form swarms, unlike their male counterparts. For the purpose of mating, they prefer to fly toward males.

(c) **Mating of mayflies**
Using the operator, two mayflies' mating process is depicted as: One parent is chosen from the male, while the other is chosen from the female one. They attract each other in the same manner as parents attract their children. A random process or a fitness function can be used to make the selection. Likewise, the most beautiful woman is paired with the most attractive man. As a result of the mating, the following two children are born:

$$offspring1 = L * male + (1 - L) * female \quad (1)$$

$$offspring2 = L * female + (1 - L) * male \tag{2}$$

For example, L is a random variable that falls within a certain range for male and female parents. The starting velocities of offspring are set to 0 at the beginning of the game. The Mayfly Algorithm (MFA) can be stated in a pseudo code that shows the basic processes.

Algorithm 1: Pseudo Code of MFA

*Objective function* $f(x), x = (x1, \ldots, xd)^T$
*Initialize the male mayfly population* $x_i (i = 1, 2, \ldots, N)$ *and velocities* $v_{mi}$
*Initialize the female mayfly population* $y_i (i = 1, 2, \ldots, M)$ *and velocities* $v_{fi}$
*Evaluate solutions*
*Find global best gbest*
***Do While*** *stopping criteria are not met*
    *Update velocities and solutions of males and females*
    *Evaluate solutions*
    *Rank the mayflies*
    *Mate the mayflies*
    *Evaluate the offspring*
    *Separate offspring to male and female randomly*
    *Replace worst solutions with the best new ones*
    *Update pbest and gbest*
***End while***
*Post − process results and visualization*

The encrypted files as E f1 and f2 are the end result of this process. In this case, E f1 is the product of a random number k and a point on the elliptic curve Pt c that is randomly selected. HDF, k, and the public key, K Pb, are added together to form E f2. KPb is included into each CU's ACL for the next step in the procedure. The integrity of each encrypted file is safeguarded by the HMAC signature and key generated and stored by the TTP-CS. This information is sent to the person who requested it: the center ID, the encrypted files (E f1 and E f2), and their K Pr. Whereas, just the center ID and K Pr are transmitted across a Secure Socket Layer to the rest of the CUs (SSL). After the encryption procedure, a secure overwrite separates K Pr and K Pb from the TTP-CS. It is up to DO or TTP-CS to upload the encrypted files (E f1 and E f2) after they have been received (on behalf of CU).

The key generation procedure begins as soon as the encryption center is activated or the encrypted file is submitted. You have two options when it comes to uploading files: In either case, the DO can be promptly posted to the HC, as previously explained, or the TTP-CS can upload the file on behalf of the CU to the HC, which has the authority delegation. It is possible to upload a single file of medical data to the Health Center by following the steps listed below:

| | |
|---|---|
| *U1* | The TTP-CS receives the healthcare data file from the physician and the list of users |
| *U2* | The ACL, private key, and public key for the physician are generated by TTP-CS. Next, an efficient EGC encryption mechanism is used to protect the data |
| *U3* | Physicians can get their TTP-CS private key, centre ID, and encrypted files by using the TTP-CS |
| *U4* | The physician upload the encrypted files straight to the health cloud |
| *U5* | TTP-CS uploads encrypted files to the health on behalf of the doctor in special cases |

### 3.2.2 Downloading a File from the HC

It is either essential for the TTP-CS to receive an authentication request from the CU or for the DO to download encrypted files directly from the HC and then submit a decryption request. A locally upheld ACL authenticates the CU's authorization from the HC. The TTPCS obtains K Pb from the ACL. The requesting CU will receive an access forbidden message if the ACL does not contain the K Pb. Because each CU has its own K Pb, no CU can use the K Pr of another CU. As a result, the decryption procedure can begin after the TTP-CS verifies the file's integrity. Depending on whether or not the TTP-CS receives a valid K Pr, the decryption operation will either succeed or fail.

After a successful ECC decryption, the HDF is sent to the relevant CU over an SSL connection. The secure overwriting approach eventually removes K Pr and K Pb from the TTP-CS. The TTP-CS can also be used to download files on behalf of the CU, same like the file uploading process. TTP-CS receives this request for decryption along with login credentials, as previously stated. Once the TTP-CS has confirmed that the CU for the specified file is genuine, it will forward this request on to the HC for processing. Further transmission of encrypted data takes place via TTP-CS, with the HC acting as a conduit. The rest of the process is the same as described previously. Here is an example of how to obtain a medical data file from the HC:

| | |
|---|---|
| *D1* | The TTP-CS receives requests from the CU |
| *D2* | In order for TTP-CS to send a download request to the health cloud, ACL verification is required |
| *D3* | The health cloud sends encrypted files to TTP-CS |
| *D4* | TTP-CS retrieves from the ACL |
| *D5* | It is sent to the appropriate CU with the original data file in it |

### 3.2.3 File Restore

ACL and key generation are not performed while recovering a file, unlike when uploading a file. TTP-CS receives a restore request from CUs (who have already downloaded the file) if any modifications have been made. True or false, TTP-CS verifies whether or whether CU has WRITE access to a file. The TTP-CS computes the keys if a valid request for file restoration has been made. Additionally, the file is encrypted before being subjected to the HMAC algorithm. They're either re-encrypted and transmitted through email or uploaded to the HCI server. Finally, the K Pr and K Pb are left out of the equation.

The proposed model delivers the subsequent features to the healthcare data: Healthcare data must be protected from insider threats by preventing unauthorized access within the center. Secure sharing of healthcare data among the center.

### 3.2.4 Security Analysis

1. **Eaves dropping**
   The patient receives the private key from the certificate authority via a secure connection. As a result, hackers will be unable to access the encrypted data.
2. **Replay attack**
   The property and the secret key used to encrypt the files can be found in the tree structure. The EGC cryptography algorithms have been implemented by the doctors to their fullest potential. The optimization mechanism identifies the EGC values in order to identify the best solutions. As a result, a replay assault on the keyword provided by the patient is ruled out. Even if the hacker knows the characteristics and ciphertext, the secret key is not fixed in the EGC, therefore he can't calculate it.
3. **Masqurade and man in the middle attack (MIM)**
   Hackers can't use a masqurade attack because the properties are utilized to encrypt the files. The properties of the file must be known by the hacker if he wants to hack it. The hacker must know the property before he or she can change ciphertext files. Files are transmitted via cryptography rather than the MIM since we've utilized an EGC that operates on points instead than bytes.

## 4 Results and Discussion

Using an Intel Core i5-6200U CPU clocked at 2.40 GHz and 8.00 GB of RAM, the proposed solution is put into practice on a Windows 10 64-bit OS system. The HC, TTP-CS, and CUs are the three main components described in the system model. Uses JPBC v.2.0.0 Java Pairing Based Cryptography library for communication between entities. Both elliptic curve and pairing procedures can be implemented with the

**Table 1** Computation time for finding the value of EGC with different iterations

| No. of iterations | WOA | *AFBS_WOA* [21] | Mayfly |
|---|---|---|---|
| 5 | 1.594 | 1.534 | 1.494 |
| 10 | 1.741 | 1.606 | 1.598 |
| 15 | 1.888 | 1.798 | **1.645** |
| 20 | 2.193 | 2.110 | **2.001** |
| 25 | **2.356** | **2.190** | 2.129 |

**Table 2** Key generation time

| FS (MB) | Methodologies (time in second) | | | |
|---|---|---|---|---|
| | AES | ECC | EGC | Proposed optimized EGC |
| 10 | 1.594 | 1.534 | 0.004 | 0.00212 |
| 20 | 1.741 | 1.606 | 0.00425 | 0.00235 |
| 30 | 2.321 | 1.684 | 0.00476 | 0.00286 |
| 40 | 1.888 | 1.799 | 0.005 | 0.00302 |
| 50 | 1.952 | 1.866 | 0.00512 | 0.00328 |
| 60 | 2.193 | 1.923 | 0.0055 | 0.0035 |
| 70 | 2.286 | 2.034 | 0.00598 | 0.00398 |
| 80 | 2.694 | 2.129 | 0.00632 | 0.00427 |
| 90 | 2.827 | 2.388 | 0.00664 | 0.00463 |
| 100 | 2.887 | 2.545 | 0.00697 | 0.00499 |

help of its functions. It is possible to communicate between the entities thanks to the Java libraries. SSL encrypts all data sent and received. It was tested using the Cloudsim toolkit and evaluated in terms of key generation time, file upload and download times, and the time it took to discover EGC's value. Performance analyses of proposed mayfly algorithm are tabulated on Tables 1, 2, 3 and 4.

## *4.1 Performance Analysis of Proposed Mayfly Algorithm*

See (Table 1).

## *4.2 Performance Analysis of Proposed Optimized EGC*

See (Tables 2, 3 and 4).

**Table 3** Time taken for uploading the encrypted files and downloading the decrypted files

| FS (MB) | Methodologies (time in second) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | AES | | ECC | | EGC | | Proposed optimized EGC | |
| | UL | DL | UL | DL | UL | DL | UL | DL |
| 0.1 | 1.4 | 0.99 | 1.48 | 1.15 | 0.80 | 0.80 | 0.70 | 0.70 |
| 0.5 | 1.48 | 1.03 | 1.89 | 1.31 | 0.94 | 0.96 | 0.80 | 0.82 |
| 1 | 2.06 | 1.48 | 2.90 | 1.85 | 1.24 | 1.18 | 1.20 | 1.24 |
| 10 | 14.95 | 9.90 | 14.59 | 10.45 | 6.43 | 6.48 | 5.60 | 5.68 |
| 50 | 58.56 | 35.57 | 60.37 | 35.90 | 9.01 | 10.24 | 8.25 | 8.78 |
| 100 | 112.41 | 59.14 | 115.15 | 61.59 | 17.39 | 20.68 | 16.35 | 18.98 |
| 500 | 492.03 | 229.81 | 872.09 | 400.21 | 33.24 | 39.25 | 31.10 | 38.22 |

**Table 4** Speed of file uploading

| File size (MB) | Uploading speed (Mb/s) |
|---|---|
| 0.1 | 11.5 |
| 0.5 | 12 |
| 1 | 11.9 |
| 10 | 12.92 |
| 50 | 12.5 |
| 100 | 13 |
| 250 | 13 |
| 500 | 13 |

## 5 Conclusion

Increasing e-health productivity is now possible because to cloud computing-based health clouds, which allow medical professionals to access patient records from anywhere at any time, on any device. Secure data exchange between general practitioners, medical providers, and insurance companies is a critical concern for any healthcare company. In order to deal with this problem, encryption technologies are used to safeguard critical healthcare data. EGC-based encryption is utilized for data security in the proposed health cloud architecture. TTP-CS is also responsible for the encryption and decryption operations. Using the EGC model surpasses other existing systems in terms of key generation time, file upload time, file download time and uploading speed. EGC has a smaller key size, which makes key administration more simpler. The results demonstrate that EGC-based approach is a promising choice for safe healthcare data sharing in the health cloud. Because it hasn't been developed to handle image-based data yet, this encryption approach can only be used to protect

plaintext. It is possible that this problem will be resolved in the future. Also implement the security mechanism in the cloud that are federated and then compare its efficiency with the existing methods.

## References


1. Jayaraman I, Stanislaus Panneerselvam A (2021) A novel privacy preserving digital forensic readiness provable data possession technique for health care data in cloud. J Ambient Intell Humaniz Comput 12(5):4911–4924
2. Manne R, Kantheti SC (2021) Application of artificial intelligence in healthcare: chances and challenges. Curr J Appl Sci Technol 40(6):78–89
3. Qiu H, Qiu M, Liu M, Memmi G (2020) Secure health data sharing for medical cyber-physical systems for the healthcare 4.0. IEEE J Biomed Health Inform 24(9):2499–2505
4. Rushanan M, Rubin AD, Kune DF, Swanson CM (2014) Sok: security and privacy in implantable medical devices and body area networks. In: 2014 IEEE symposium on security and privacy. IEEE, pp 524–539
5. Sun Y, Lo FPW, Lo B (2019) Security and privacy for the internet of medical things enabled healthcare systems: a survey. IEEE Access 7(2019):183339–183355
6. Timothy DP, Santra AK (2017) A hybrid cryptography algorithm for cloud computing security. In: 2017 International conference on microelectronic devices, circuits and systems (ICMDCS). IEEE, pp 1–5
7. Banos O, Villalonga C, Damas M, Gloesekoetter P, Pomares H, Rojas I (2014) Physiodroid: combining wearable health sensors and mobile devices for a ubiquitous, continuous, and personal monitoring. Sci World J
8. Abdullah A, Ismael A, Rashid A, Abou-ElNour A, Tarique M (2015) Real time wireless health monitoring application using mobile devices. Int J of Comput Netw Commun (IJCNC) 7(3):13–30
9. Anuradha M, Jayasankar T, Prakash NB, Mohamed Yacin Sikkandar, Hemalakshmi GR, Bharatiraja C, Sagai Francis Britto A (2021) IoT enabled cancer prediction system to enhance the authentication and security using cloud computing. Microprocess Microsyst 80(2021):103301
10. Jaiswal K, Sobhanayak S, Turuk AK, Bibhudatta SL, Mohanta BK, Jena D (2018) An IoT-cloud based smart healthcare monitoring system using container based virtual environment in edge device. In: 2018 international conference on emerging trends and innovations in engineering and technological research (ICETIETR). IEEE, pp 1–7
11. Nirabi A, Hameed SA (2018) Mobile cloud computing for emergency healthcare model: Framework. Proc Int Conf Comput Commun Eng:375–379
12. Kumar V, Bhardwaj A (2020) Deploying cloud-based healthcare services: a holistic approach. Int J Serv Sci Manag Eng Technol (IJSSMET) 11(4):87–100
13. Blakley GR, Borosh I (1979) Rivest-Shamir-Adleman public key cryptosystems do not always conceal messages. Comput Math Appl 5(3):169–178
14. Gola KK, Gupta B, Iqbal Z (2014) Modified RSA digital signature scheme for data confidentiality. Int J Comput Appl 106(13)
15. Ali A, Pasha MF, Ali J, Fang OH, Masud M, Jurcut AD, Alzain MA (2022) Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: a novel approach to cryptography. Sensors 22(2):528
16. Zhang Y, Zheng D, Deng RH (2018) Security and privacy in smart health: efficient policy-hiding attribute-based access control. IEEE Internet Things J 5(3):2130–2145
17. Huang Q, Yue W, He Y, Yang Y (2018) Secure identity-based data sharing and profile matching for mobile healthcare social networks in cloud computing. IEEE Access 6:36584–36594

18. Bao S-D, Chen M, Yang G-Z (2017) A method of signal scrambling to secure data storage for healthcare applications. IEEE J Biomed Health Inform 21(6):1487–1494
19. Masood I, Wang Y, Daud A, Aljohani NR, Dawood H (2018) Towards smart healthcare: patient data privacy and security in sensor-cloud infrastructure. Wireless Commun Mobile Comput 2018(Nov 2018), Art. no. 2143897
20. Mbonihankuye S, Nkunzimana A, Ndagijimana A (2019) Healthcare data security technology: HIPAA compliance. Wireless Commun Mobile Comput 2019(Oct 2019), Art. no. 1927495
21. Thanga Revathi S, Gayathri A, Kalaivani J, Christo MS, Pelusi D, Azees M (2021) Cloud-assisted privacy-preserving method for healthcare using adaptive fractional brain storm integrated whale optimization algorithm. Secur Commun Netw
22. Kumar D, Smys S (2020) Enhancing security mechanisms for healthcare informatics using ubiquitous cloud. J Ubiquitous Comput Commun Technol 2(1):19–28
23. Smys S (2019) Survey on accuracy of predictive big data analytics in healthcare. J Inf Technol 1(02):77–86
24. Zervoudakis K, Tsafarakis S (2020) A mayfly optimization algorithm. Comput Ind Eng 145:106559