Security and Privacy in Cloud-Based E-Health System Using Advanced Encryption Standard (AES)

by
Anon Sarkar, Mahmud Hasan Shanto, Humaera Hossain

United International University,
United City, Madani Avenue, Badda, Dhaka 1212, Bangladesh.

Abstract. : In the evolving landscape of e-health systems, ensuring the security and privacy of sensitive patient data is paramount. As personal health records (PHRs) are increasingly stored in cloud environments, robust encryption techniques are required to safeguard this information from unauthorized access. This paper explores the application of four major encryption algorithms—Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), and Data Encryption Standard (DES)—to secure cloud-based e-health systems. A particular emphasis is placed on the efficiency and security of the AES algorithm due to its ability to handle large volumes of data while maintaining high performance. AES is used in combination with ECC for stronger cryptographic protection in transit and at rest. Additionally, this paper compares the algorithms based on key length, security rates, execution time, and performance, highlighting AES's superiority in most aspects. By deploying AES in cloud-based healthcare, this study addresses privacy concerns and enhances the overall security framework. The proposed model enables secure, fine-grained access control, allowing authorized personnel to search encrypted data while ensuring confidentiality, thereby creating a more reliable and secure e-health ecosystem.

Keywords: e-Health; cloud computing; security; privacy in health system; advanced Encryption Standard (AES)

1 Introduction

E-Healthcare systems are increasingly popular due to the introduction of wearable healthcare devices and sensors. Personal health records (PHRs) are collected by these devices and stored in a remote cloud. Due to privacy concerns, these records should not be accessible by any unauthorized party, and the cloud providers should not be able to learn any information from the stored records. Securing e-healthcare involves encrypting sensitive patient data, such as medical records, in a way that allows for search operations to be performed on the encrypted data without compromising the security of the patient's information. To address the above issues, one promising solution is to employ Advanced Encryption Standard (AES) for fine-grained access control and searchable encryption for keyword search on encrypted data. These methods can be used to create secure systems for e-healthcare that allow authorized personnel to search patient data while ensuring that the data remains confidential and protected from unauthorized access.A eHealth as a model of collaboration in patients' data collection and sharing eliminates such problems as geographic location and accessibility of the healthcare field. Technological developments have made it possible to gather patient information at any time and place, and store them in a central database and disseminating to the various institutions in an attempt to improve haelthcare. But it is crucial to ensure that data privacy is respected throughout storage and especially when sharing it so as to encourage the use of collaborative eHealth. The paper focuses mainly on the role of attribute based encryption (ABE) to ensure data privacy in such systems because of the efficiency that has been observed on cloud security. It overviews various ABE schemes for the eHealth applicability and addresses the issues that concern the implementation of such encryption schemes as well as the potential directions for further research. Furthermore, the paper gives a comparative comparison of the studied schemes using security, revocation flexibility, and effectiveness.

2 Related Works:

We looked at some papers that were connected to our topic and learned some important things about it. We chose a few papers that are related to our planned work from that list.

There have been several traditional solutions to deal with the problem of secure data sharing on cloud environments. In the context of blockchain technology, various studies have investigated the capability of blockchain to support e-health data sharing. Blockchain was exploited to ensure reliable EHRs accessibility for medical users.The authors focus on theoretical analysis and therefore, the feasibility of the proposed solution had not been confirmed in real EHRs sharing scenarios. [1]

In their article, they talked about Attribute based encryption was proposed for encryption as well as efficient key management. The concept is that the data will be encrypted under a set of attributes which enables multiple users to decrypt using the assigned key. The owner can encrypt the data without even knowing the Access Control List. The unique feature of ABE is that it prevents user collusion . [2]

In this study, the proposed approach solves the issues of privacy and storage in health-care systems. The easiest solution to avoid privacy issues is to use the Advanced Encryption Standard with data deduplication. [3]

As there are so many advantages of cloud computing, more and more data owners centralize their sensitive data into the cloud. In this paper, they propose a semantic keyword ranked search scheme over the encrypted cloud data, which simultaneously meets a set of strict privacy requirements.The proposed scheme could return not only the exact matching files, but also the files including the terms latent semantically associated to the query keyword. [4]

In this paper The ECC and SHA-256 encryption algorithms, combined with the tamper-proof nature of Blockchain, have safeguarded sensitive patient medical information from unauthorized access and malicious attacks by combining the power of ECC, SHA-256, and multi-authority mechanisms, E-Health systems can establish a formidable defense against privacy.To solve this problem, they have created and implemented a secure, granular access control system with access policy updates for outsourced E-Health Records. Ciphertext policy attribute-based encryption (CP-ABE) is the basis of the plan they have suggested. [5]

In this paper,The key challenge identified is the need to enhance system security while maintaining data integrity and minimizing the risks associated with data breaches and unauthorized access in cloud environments. The solution is A hybrid approach using AES and ECC improves security but incurs higher computational and time costs.This method integrates ECC to secure data storage and transfer, providing robust and flexible protection. Combining symmetric (AES) and asymmetric (ECC) encryption improves privacy, integrity, and overall cryptographic efficiency, strengthening user trust in cloud systems. [6]

The key challenge is ensuring the confidentiality, integrity, and security of data stored and transmitted in cloud computing systems, particularly in preventing third parties or attackers from accessing or tampering with sensitive data. The authors propose a two-level cryptographic technique combining AES for encrypting data at rest and ECC for securing data in transit. [7]

In Chandrika and Perumal's (2022) study, the problem is the high computational complexity, long key generation time, and security issues in traditional encryption methods for multi-tenant cloud environments. They propose a Modified Elliptic Curve Cryptography (MECC) algorithm. This enhances the Elliptic Curve Cryptography (ECC) by integrating Diffie-Hellman key exchange for secure key generation and transfer. MECC reduces encryption/decryption times and key sizes while improving security by dividing and separately encrypting private keys, ensuring more efficient and secure data transmission in multi-tenant cloud systems. [8]

Cloud-based encryption and decryption algorithms can improve the online examination system [26]. For this process testing, they did not apply any encryption or decryption algorithms. Although online tests have been widely employed by universities and colleges at all academic levels, they do have one major drawback: the internet connection can be lost. A cutting-edge online examination system capable of overcoming the aforementioned flaw was proposed. Examinees can answer e-question papers without fear of losing Internet connection if the proposed approach is implemented. [9]

The proposed algorithm provides a security strategy and better stockpiling utilizing encipherment algorithms over the cloud architecture. The results show that if the security challenges are fixed, then small and large enterprises will be safe when storing data in the cloud. Subashanthini and Pounambal [10]

The main contribution of our research are :

AES-based security can help healthcare systems ensure the confidentiality and integrity of sensitive patient data, while also meeting regulatory and compliance requirements.

We have majorly focused on this need of the users. We tried to overcome the issues affected by the security to the users for better use of the system.

We provide a security analysis and extensive evaluation in various performance metrics to highlight the advantage of the proposed framework over current solutions.

2.1 Gap Analysis

After reviewing the other literature, we have found that there are other projects that offer similar technology but offer very different facilities compared to ours.

Features	**DES**	**RSA**	**ECC**	**AES**
Key Length	56-bits	Based on No. of bit	135 bits	128,192 &256 bits
Factors Contributor	IBM-75	Rivest Shamir 78	Neal Koblitz	Rijman Joan
Block Size	64-bits	Variant	Variant	128-bits
Security Rate	Not Enough	Good	Less	Ecellent
ExecutionTime	Slow	Slowest	Faster	More Fast
Response Time	Slow	Average	Faster	More Fast
Performance	Slower	Slower	Faster	More Efficient

Table 1. Gap Analysis

3 Proposed Work

The key idea is, initially, through the admin process hospital registration is done only after getting license for that particular hospital. Then the doctors will get registered and patients also get registered. The patients' general information profile can be seen only by doctors who are having the Patient ID. The Patient ID can be shared to others by the patients (PHR owners). The patients can also share their information with others by uploading to the cloud. A patient's health record comprises different types of data related to various areas like dentistry, cardiology, oncology, etc. The data in each area can also be of different types like lab reports, medical treatment, discharge summary and so on. Each of these files is based on a particular attribute. The owner will upload these files using Advanced Encryption Standard. A patient may want to share specific data with his doctor and may not want others to see the information. Therefore based on the attributes the owner will grant access to only that part of the record to those persons only with whom he wishes to share the data. Additionally, in this framework, the data in the database is also encrypted. So that even if the intruders get access to the database, they cannot read the data in the database. The data can be read only by the authorized persons in the framework like PHR owners, doctors.

3.1 System Architecture

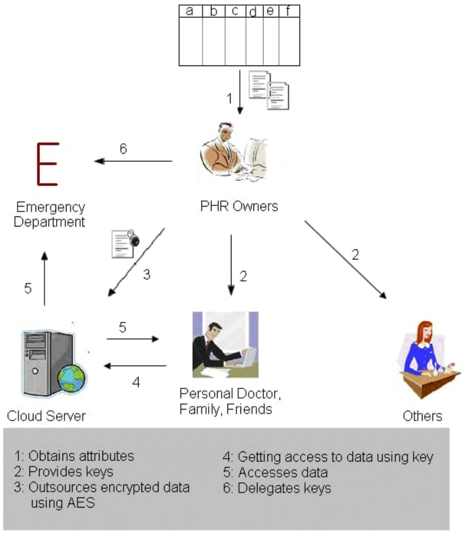

Fig. 1. System Architecture

This is a model of a cloud-based Personal Health Record (PHR) system secured using Advanced Encryption Standard (AES). In this model, PHR owners (patients) hold the authority to manage their health records and delegate access to specific entities, such as personal doctors, family members, or others. The process begins with PHR owners obtaining attributes (step 1), which are used to generate encryption keys that secure the PHR data. The PHR owners then provide these keys (step 2) to authorized users like doctors, family, or others, allowing them controlled access to the data. The cloud server stores the encrypted PHR data (step 3) using AES encryption, and authorized entities can retrieve the data by using the provided keys (step 4). Emergency departments can gain access to this data (step 6) during critical situations via key delegation. This system ensures secure and selective access to sensitive health records, balancing privacy with accessibility through cryptographic control.

3.2 AES ENCRYPTION:

The Advanced Encryption Standard (AES) is an algorithm that uses the same key to encrypt and decrypt protected data. Instead of a single round of encryption, data is put through several rounds of substitution, transposition, and mixing to make it harder to compromise.

A sender encrypts plaintext data using a secret key via an encryption server. The encryption process transforms the plaintext into ciphertext, which is transmitted over a secure channel to the receiver. The receiver, using the same secret key, decrypts the ciphertext back into its original plaintext through a decryption server. This symmetric encryption model ensures that only entities with the correct secret key can access the original data, maintaining secure communication between the sender and receiver.

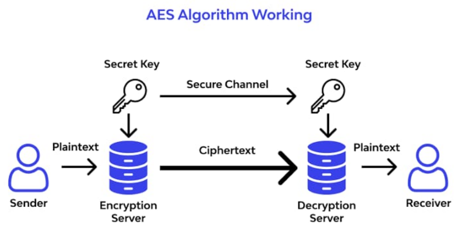

Fig. 2. Caption

4 Result

The result is concluded on the performance evaluation of time of encryption, decryption, execution, total time and security rate which are described below:

a. **Encrypting time:** The time taken in the process of converting ciphertext into plaintext with the appropriate encryption method.
b. **Decrypting time:** The time taken in the process of converting plaintext into ciphertext with the appropriate decryption method.
c. **Throughput:** It is the division of encrypted plaintext to encryption time. For the scheme of encryption, throughput is how fast the encryption is done. When it increases, power consumption decreases.

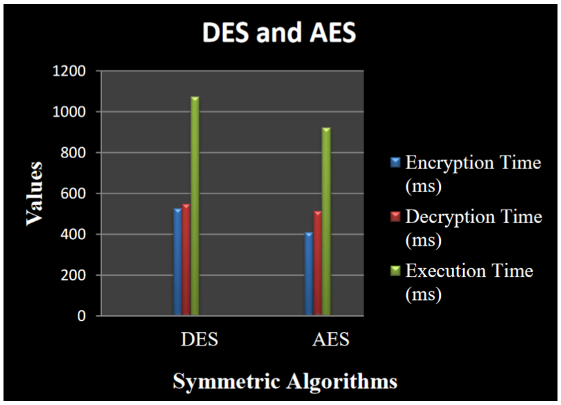

Fig. 3. Caption

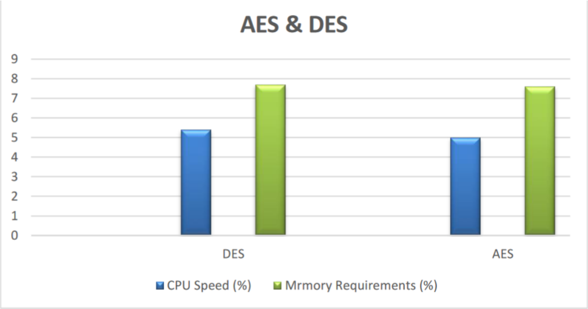

Fig. 4. Caption

Algorithms	**Key-Size (bits)**	**Encryption Key Time (ms)**	**Decryption Key Time (ms)**	**Total Time (ms)**	**CPU Speed (%)**	**Memory Requirement (%)**	**Security Rate (%)**
DES	56-bits	525	548	1073	5.4	7.7	86
RSA	256-bits	939	608	1547	6.5	7.8	88
ECC	256-bits	550	542	1092	2.4	7.6	92
AES	128-bits	408	525	933	5.0	7.6	96

Table 2. Table 1.2

From the results of Table 1.2, it can be concluded that AES provides lesser encrypting and decryption time as compared to DES. Memory requirement in AES is lesser in AES as compared to DES. Hence it is concluded that AES outperforms DES. it is concluded that ECC provides lesser encryption and decryption key time as compared to RSA.ECC has less memory requirement than RSA after being analyzed. It shows that AES is a highly efficient algorithm for providing security.

5 Conclusion

With the excessive growth of the Internet, data security becomes a serious concern for any individual or organization. The security of data is highly important as it can be of high risk, if not taken into consideration. Cryptography algorithms are getting versatile and involve private keys for encryption which provide secure transmission of data. The schemes used for cryptography are symmetric and asymmetric. The former can be used with the help of DES and AES. From the above results, it is clear that AES provides more security as compared to DES as it has lower encryption and decryption time. AES also has lesser memory requirements as compared to DES. ECC provides better results than RSA which makes it a more secure and reliable algorithm. It can be concluded that AES outperforms other cryptography algorithms and can be used for applications that require lesser time to encrypt the data. From the above results achieved; AES provides better security in terms of performance analysis. For future work, AES can be used to further reduce the execution time for better outcomes.

References

1. V. Ramani, T. Kumar, A. Bracken, M. Liyanage, and M. Ylianttila, “Secure and efficient data accessibility in blockchain based healthcare systems,” in Proc. GLOBECOM, Dec. 2018, pp. 206–212.
2. Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters, Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data ACM CCS (2006)

3. D. B, P. J, S. C. M, S. Rajagopal and B. Jegajothi, ”Secure Cloud-based E-Health System using Advanced Encryption Standard,” 2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2022, pp. 642-646, doi: 10.1109/ICESC54411.2022.9885501.
4. Xia, Z., et al., (2013). An efficient and privacy-preserving semantic multi-keyword ranked search over encrypted cloud data. Advanced Science and Technology Letters, 31, 284.
5. Ensteih Silvia, Mohd Tajuddin. (2024). E-Health Privacy and Security through ECC, SHA-256, and Multi-Authority Approaches. Journal of Information Technology and Cryptography (e-ISSN: 3048-5290), 1(1), 9–13. https://doi.org/10.48001/joitc.2023.119-13.
6. K. Gai, M. Qiu, and H. Zhao, “Privacy-preserving data encryptionstrategy for big data in mobile cloud computing,” IEEE Transactions on Big Data, vol. 7, no. 4, pp. 1–1, 2017, doi: 10.1109/TBDATA.2017.2705807.
7. M. M. Potey, C. A. Dhote, and D. H. Sharma, “Homomorphic encryption for security of cloud data,” Procedia Computer Science, vol. 79, pp. 175–181, 2016, doi: 10.1016/j.procs.2016.03.023.
8. V. Vijayakumar, M. K. Priyan, G. Ushadevi, R. Varatharajan, G. Manogaran, and P. V. Tarare, “E-health cloud security using timing enabled proxy re-encryption,” Mobile Networks and Applications, vol. 24, no. 3, pp. 1034–1045, Jun. 2019, doi: 10.1007/s11036-018-1060-9.
9. H. Abroshan, “A hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography algorithms,” International Journal of Advanced Computer Science and Applications, vol. 12, no. 6, pp. 31–37, 2021, doi: 10.14569/IJACSA.2021.0120604.
10. K. Dubey, S. C. Sharma, and M. Kumar, “A secure IoT applications allocation framework for integrated fog-cloud environment,” Journal of Grid Computing, vol. 20, no. 1, p. 5, Mar. 2022, doi: 10.1007/s10723-021-09591-x.