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

Humaera Hossain, Anon Sarkar, Mahmud Hasan Shanto

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

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.

Literature Review :

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].

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].

(Another)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.

Proposed Solutions:

- **AES and ECC Combination**: A hybrid approach using AES and ECC improves security but incurs higher computational and time costs.
- **Polynomial-based Encryption**: This method integrates ECC to secure data storage and transfer, providing robust and flexible protection.
- **Two-tier Cryptographic Model**: Combining symmetric (AES) and asymmetric (ECC) encryption improves privacy, integrity, and overall cryptographic efficiency, strengthening user trust in cloud systems.

  4o

(Another)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.

Proposed Solution:
The authors propose a **two-level cryptographic technique** combining **AES** for encrypting data at rest and **ECC** for securing data in transit.

- **AES** efficiently handles large data volumes, ensuring fast encryption and decryption for cloud-stored data.

- **ECC** provides secure key generation and digital signatures for data transmission, offering stronger security with smaller, faster keys compared to RSA.

(Another)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.

Solution: 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

(Another)In Awan et al. (2020), the **problem** identified is the **inefficiency of the traditional AES algorithm** in handling emerging security threats in cloud computing environments. Specifically, the standard AES algorithm suffers from **high energy consumption, increased network usage, and delays** during encryption and decryption processes.

Solution: To solve these issues, the authors propose a **modified AES algorithm**. This enhancement includes a **double round key feature** that improves encryption speed (processing 1000 blocks per second compared to 800 in the traditional AES). The modified algorithm also reduces **power consumption, network usage, and delay** by 14.43%, 11.53%, and 15.67%, respectively. The proposed framework ensures better **load balancing, trust management, and resource optimization**

Gap Analysis :

Comparison between mostly used algorithms.

	DES	RSA	ECC	AES
Factors Contributor	IBM-75	RivestShamir 78	Neal Koblitz	Rijman,Joan
Key Length	56-bits	Based on No.	135 bits	128,192, &

		Of bit		256
Block Size	64-bits	Variant	Variant	128 bits
Security Rate	Not enough	Good	Less	Excellent
Execution Time	Slow	Slowest	Faster	More Fast
Response Time	Slow	Average	Faster	More Fast
Performance	Slower	Slower	Faster	More Efficient

CONTRIBUTION :

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.

PROPOSED FRAMEWORK :

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.

SYSTEM ARCHITECTURE :

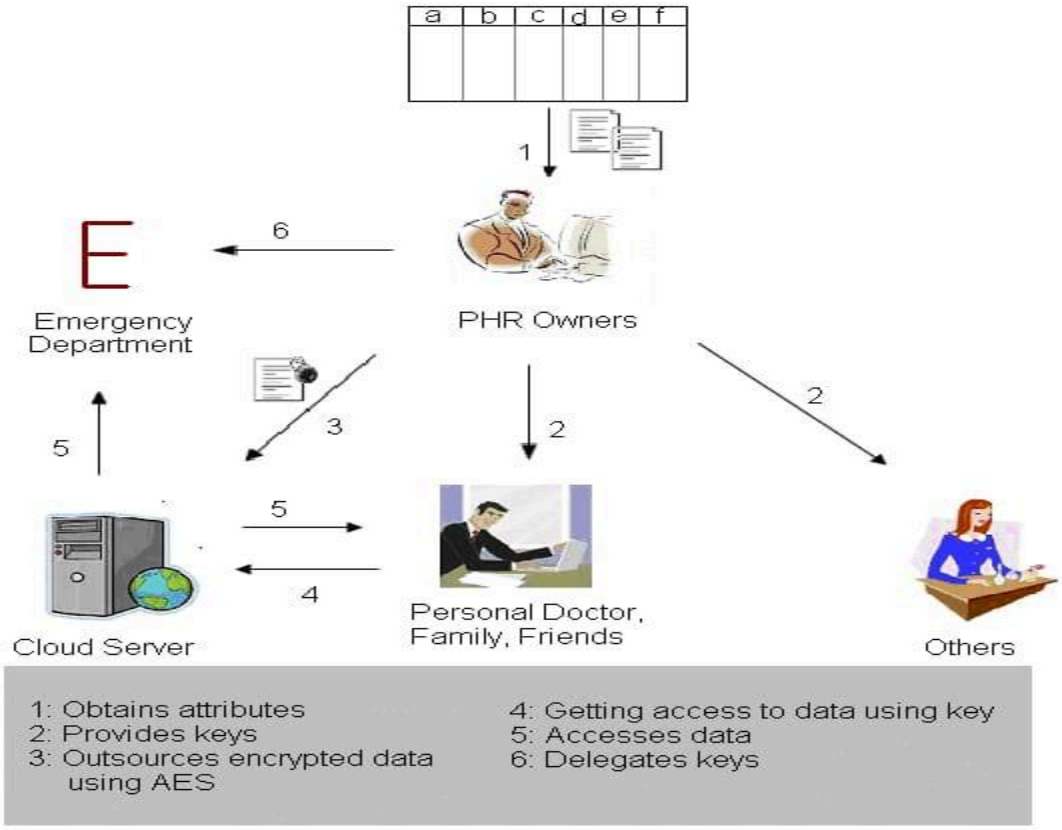
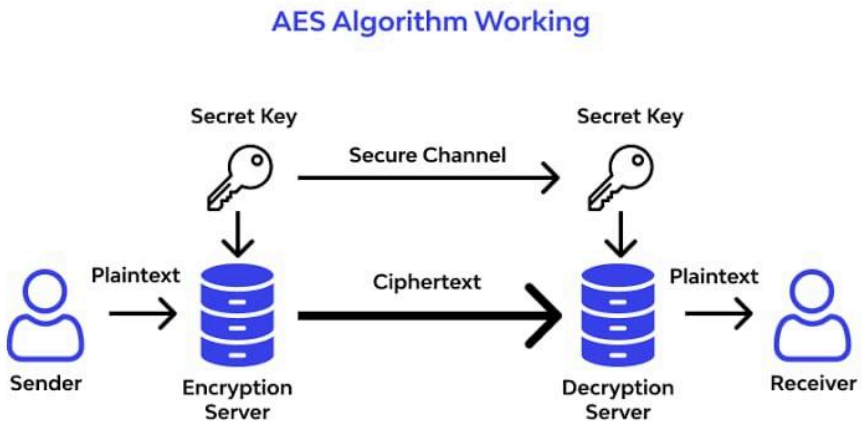


Figure 1: System Architecture

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.



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. https://doi.org/10.48001/joitc.2023.119-13