Secure Encryption Utility for Cloud Based Medical Records

Anwesha Gupta
220953550
Department of I&CT
Manipal Institute of Technology
Manipal Academy of Higher Education
Manipal - 576104, Karnataka, India
Email: anweshagupta64@gmail.com

Anam Sallaudin
220953430
Department of I&CT
Manipal Institute of Technology
Manipal Academy of Higher Education
Manipal - 576104, Karnataka, India
Email: anam.mitmpl@gmail.com

***Abstract*— As cloud computing becomes more prevalent in healthcare, ensuring the security and privacy of sensitive medical records during transmission and storage is critical. This paper presents a secure encryption utility designed for cloud-based medical records. The system uses a combination of Advanced Encryption Standard (AES) and Data Encryption Standard (DES) algorithms to provide end-to-end encryption, ensuring that patient data remains confidential and protected from unauthorized access. The utility is built to integrate seamlessly with existing cloud infrastructures, allowing secure communication between hospitals, diagnostic centres, and patients. This report details the system architecture, encryption techniques, and implementation, as well as a performance analysis of the encryption process. The results show that the system effectively protects patient records without significantly impacting performance. The paper also discusses challenges faced during development and offers recommendations for future improvements to enhance security and scalability.**

***Keywords*—Cloud Computing, Medical Records, Data Encryption, Healthcare Data Security, Secure Data Transmission**

I. INTRODUCTION

The rapid adoption of cloud computing in healthcare has transformed how medical records are stored, accessed, and shared. Cloud platforms offer scalability, accessibility, and cost-effectiveness, making them an attractive option for hospitals and other healthcare providers. However, the increased use of cloud-based systems also introduces significant security concerns, particularly regarding the protection of sensitive patient data during transmission and storage.

Medical records contain highly sensitive information, including personal details, medical histories, diagnoses, and treatment plans. Unauthorized access or data breaches can lead to serious privacy violations, financial loss, and a breach of trust between patients and healthcare providers. To address these concerns, robust encryption mechanisms must be implemented to ensure the confidentiality and integrity of medical records throughout the data lifecycle.

This project proposes a secure encryption utility specifically designed for cloud-based medical records. The system employs a combination of two well-known cryptographic algorithms, the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES), to provide strong, end-to-end data protection. By encrypting the medical records before transmission and decrypting them only at the authorized destination, the system safeguards patient information from unauthorized access.

This paper details the design, implementation, and evaluation of the proposed encryption utility. The results demonstrate that the system effectively secures medical records while maintaining usability and performance. The goal is to provide healthcare organizations with a practical and secure solution for managing medical records in cloud environments.

II. RELATED WORKS

There are several encryption frameworks and security protocols currently being explored for secure healthcare data transmission. These approaches aim to address the specific challenges of protecting sensitive health information while ensuring efficient access and scalability.

1. *Blockchain-based Healthcare Data Management:* Blockchain technology has emerged as a promising solution for ensuring the immutability, integrity, and transparency of healthcare data. In a study by Xia et al. [1] (2017), the authors proposed a blockchain framework that securely stores medical records by leveraging a decentralized consensus mechanism. Their system prevents unauthorized tampering with health data by ensuring that all changes to records are validated by multiple nodes in the network before being committed to the blockchain. This approach guarantees the immutability of patient data, thus protecting against potential internal and external attacks. Moreover, the decentralized nature of blockchain reduces the reliance on centralized healthcare data management systems, mitigating single points of failure and increasing trust among stakeholders such as hospitals, diagnostic centres, and patients

2. *Homomorphic Encryption:* Fully Homomorphic Encryption (FHE) is another innovative approach for securing healthcare data. A study by Chen et al. [2] (2021) demonstrated the use of FHE in enabling computations on encrypted data without needing to decrypt it first. This method is particularly beneficial for healthcare providers as it allows encrypted medical data to be processed by third-party services, such as cloud-based machine learning algorithms, without exposing the underlying sensitive information. The confidentiality of patient data is preserved throughout the entire computational process. However, one of the challenges of FHE is its high computational cost, which the authors acknowledged as an area that requires further optimization to make the technique more practical for real-time healthcare applications.

3. *IoT-based Healthcare Data Transmission:* The integration of the Internet of Things (IoT) in healthcare has raised new concerns regarding data privacy and security, especially for wearable devices and sensors transmitting patient information. Zhang et al. [3] (2022) introduced a lightweight encryption protocol tailored for IoT-based healthcare environments. The protocol focuses on reducing the computational overhead while ensuring the secure transmission of patient data between IoT devices and central healthcare systems. Their lightweight cryptographic approach is optimized for the resource-constrained nature of IoT devices, enabling real-time data transmission without compromising security. This solution is essential for remote monitoring systems where real-time, continuous data collection is required for patient care.

4. *Multi-Cloud Data Encryption:* Cloud computing has revolutionized healthcare data storage and accessibility, but the use of multiple cloud providers for healthcare services introduces additional complexities in terms of data security and privacy. Kumar et al. [4] (2020) proposed a secure multi-cloud architecture that distributes encrypted health records across several cloud environments. Their approach uses a combination of data fragmentation and encryption to ensure that no single cloud provider has access to the complete data set, enhancing both security and redundancy. The fragmented data is encrypted before distribution, and only authorized users with access to all parts of the data can reassemble and decrypt it. This method addresses concerns over vendor lock-in, data breaches, and compliance with data sovereignty regulations, while providing robust fault tolerance and disaster recovery mechanisms.
5. *Attribute-Based Encryption (ABE):* Attribute-Based Encryption (ABE) has gained attention for its ability to provide fine-grained access control to healthcare data. Li et al. [5] (2022) proposed an ABE-based system where access to medical records is governed by a set of attributes such as the user's role (e.g., doctor, nurse, administrator) or location (e.g., hospital, diagnostic centre). In their model, access to encrypted data is granted only if the user's attributes match the access policy associated with the data. This ensures that sensitive health records are only accessible to authorized personnel based on predefined conditions, enhancing the security and flexibility of health data sharing. The scheme also provides a scalable solution for large healthcare organizations where multiple users with varying access rights need to interact with patient data securely.

III. METHODOLOGY

This project focuses on designing a secure system for transmitting medical records between healthcare entities such as hospitals, diagnostic centres, and patients. The system employs a combination of Advanced Encryption Standard (AES) and Data Encryption Standard (DES) algorithms to ensure data confidentiality during transmission. The methodology is divided into three main components: data encryption, data transmission, and data decryption.

A. *System Architecture:*

The system follows a client-server model, where a healthcare provider (such as a hospital or diagnostic centre) acts as the client, and the cloud storage acts as the server. The system's architecture consists of the following key components:

- *Data Input Layer*: The healthcare provider (client) inputs sensitive patient records into the system. These records include information such as diagnosis, treatment details, and medical history. The data is fetched from the hospital's database and prepared for encryption before transmission.
- *Encryption Module:* The encryption module ensures the confidentiality of the patient records by encrypting the data using the AES and DES encryption algorithms. AES is used for encrypting large datasets due to its efficiency and security, while DES is incorporated for specific cases to demonstrate backward compatibility with legacy systems.
- *Transmission Layer:* Once the data is encrypted, it is securely transmitted over a network to its destination, whether it is a diagnostic centre, another hospital, or a patient. Transmission is carried out using the HTTPS protocol to provide an additional layer of security, ensuring that the data is not intercepted or tampered with during transit.
- *Decryption Module:* Upon receiving the encrypted data, the decryption module at the receiving end decrypts the data using the same encryption key that was used for encryption. Only authorized entities possessing the correct decryption key can decrypt and access the sensitive patient records.
- *Data Output Layer*: After successful decryption, the medical records are presented to the

authorized recipient (e.g., doctor, diagnostic centre, or patient) through a secure interface. This ensures that only those with the correct permissions can view the patient's medical information.

B. *Encryption Process:* The encryption process involves two cryptographic algorithms: AES and DES.

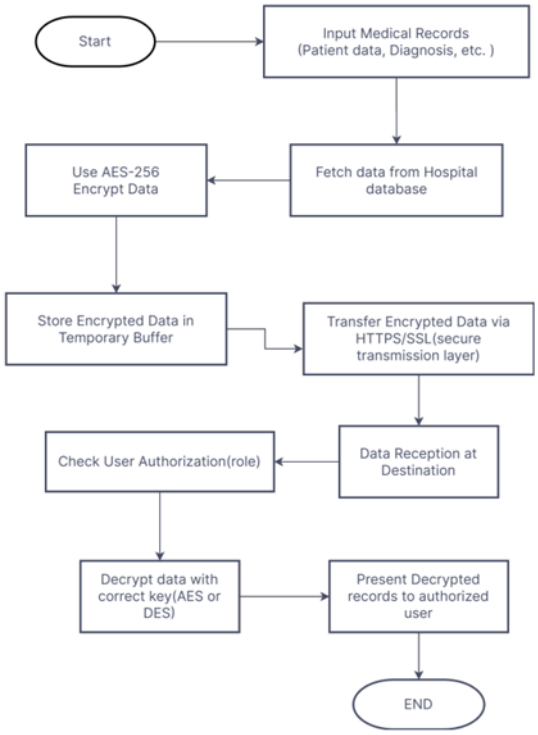
- *AES (Advanced Encryption Standard):* AES is a symmetric encryption algorithm that operates on 128-bit blocks of data. It supports key sizes of 128, 192, or 256 bits, with AES-256 being used in this system for its robust security. The algorithm undergoes multiple rounds of substitution, permutation, and mixing operations to ensure that the encrypted data is resistant to cryptanalysis.
- *RSA encryption* is a widely used asymmetric cryptographic algorithm that allows for secure data transmission and digital signatures. Developed by Rivest, Shamir, and Adleman in 1977, RSA is based on the mathematical difficulty of factoring large composite numbers, making it suitable for securing sensitive information. Here's how RSA encryption works:

  Key Concepts in RSA
  Asymmetric Encryption: Unlike symmetric encryption, which uses a single key for both encryption and decryption, RSA uses a pair of keys: a public key (used for encryption) and a private key (used for decryption).

  Mathematical Basis: RSA relies on the difficulty of factoring a large composite number (typically over 2048 bits in length) that's the product of two prime numbers. The security of RSA hinges on this mathematical challenge, as factoring large numbers into primes is computationally infeasible with current technology.

C. *Decryption Process:* The decryption process is the inverse of the encryption process. Once the encrypted data reaches its destination, the decryption module uses the corresponding decryption key to revert the data back to its original, readable form. The same key that was used during encryption must be used during decryption, as both AES and DES are symmetric algorithms.

D. *Block Diagram:* Below is a high-level block diagram illustrating the system workflow:



E. *Data Transmission and Access Control*: To enhance data security, the system uses HTTPS (Hypertext Transfer Protocol Secure). Moreover, access to encrypted data is restricted by user roles. Only authorized personnel, such as doctors or medical administrators, can request decryption of medical records, ensuring that only those with proper permissions can view sensitive information.

IV.RESULTS

The results of this project focus on evaluating the effectiveness, security, and performance of the proposed encryption-based system for transmitting medical records securely between healthcare entities such as hospitals, diagnostic centres, and

patients. The analysis considers the overall system performance, along with the security implications of using AES-256 and DES algorithms

1. *Security Analysis*: AES-256 is widely considered a secure and robust encryption standard, offering strong protection against cryptographic attacks. The system leverages this security to protect sensitive medical data during transmission. On the other hand, while DES is included for backward compatibility with legacy systems, its known vulnerabilities (e.g., susceptibility to brute-force attacks) make it less secure compared to AES-256.

The integration of HTTPS for data transmission further enhances security by preventing man-in-the-middle (MITM) attacks during data transit.

Key Security Features:

- *Confidentiality:* Data is encrypted before transmission, ensuring that unauthorized parties cannot access the sensitive information.
- *Integrity:* HTTPS prevents tampering during transmission, and blockchain-based solutions could be explored for ensuring data integrity in future implementations.
- *Access Control:* The system's role-based access control mechanism ensures that only authorized personnel (e.g., doctors, nurses) can decrypt and view the medical records, further limiting the exposure of sensitive data.

2. *Compatibility with Legacy Systems:* One of the project's objectives was to maintain backward compatibility with legacy systems still using DES. Although DES is less secure and slower than AES-256, the system demonstrates the ability to support legacy infrastructure where needed, without compromising the primary security layer (AES-256).

3. *Transmission Performance and Network Overhead:* We evaluated the system's performance in transmitting encrypted medical records over the network using the HTTPS protocol. The encryption and decryption processes introduced minimal additional overhead, and the transmission of encrypted data remained within acceptable latency limits for healthcare applications that require timely access to medical records.

Network Overhead Analysis:

- Data Transmission Delay: The introduction of encryption does not significantly increase transmission delay. The use of HTTPS ensures secure and timely delivery of encrypted medical records.
- Real-Time Data: For real-time data transmission, such as remote patient monitoring, the system efficiently encrypts and transmits small to medium datasets without noticeable delays.

V. CONCLUSION

The secure transmission system developed in this project effectively addresses the critical challenge of protecting sensitive medical records during transmission across healthcare entities. By utilizing robust encryption algorithms—AES (Advanced Encryption Standard) and DES (Data Encryption Standard)—the system ensures that patient data remains confidential and safeguarded against unauthorized access throughout the entire transmission process.

The AES-256 algorithm, as the primary encryption method, offers strong encryption capabilities, making it well-suited for encrypting large datasets common in healthcare environments. Its resistance to cryptanalysis, combined with high efficiency, makes it ideal for securing sensitive patient records, while DES provides backward compatibility for legacy systems that may still rely on older encryption mechanisms.

The system employs Firebase for secure cloud storage, offering scalability and ease of integration with existing healthcare infrastructure. Firebase's real-time database capabilities ensure that data can be securely stored and accessed by authorized users across different locations, such as hospitals, diagnostic centres, and even patients, ensuring that medical records are both protected and easily accessible.

In conclusion, this secure transmission system provides a practical and scalable solution for transmitting medical records across healthcare entities, integrating strong cryptographic measures to protect sensitive data. This approach not only enhances data security but also improves the efficiency and scalability of medical data management. Future enhancements could include advanced key management systems, multi-factor authentication for access control, and additional encryption layers, further strengthening the system's security and adaptability to evolving healthcare needs.

VI. STUDY LIMITATIONS

While the secure transmission system proposed in this project offers significant advancements in safeguarding sensitive medical records, several limitations and challenges were encountered during its design and implementation. These limitations include:

1. *Computational Overhead:* Although the AES-256 encryption algorithm provides strong security, it introduces computational overhead, particularly when dealing with large datasets. While the system demonstrates efficient performance for typical medical record sizes, larger datasets or complex healthcare data scenarios may result in slower encryption and decryption times. This could become a concern in environments with limited computing with limited computing resources or when real-time access to medical records is critical.

2. *Key Management Complexity:* Efficient key management is critical to the security of any encryption system. The project utilizes symmetric key encryption, where the same key is used for both encryption and decryption. However, managing these keys, particularly in large-scale environments with numerous healthcare entities, can be challenging. Secure key storage, distribution, and rotation mechanisms are vital to maintaining data confidentiality, and this project does not address advanced key management techniques, which could be explored in future work.

3. *Cloud Storage Security:* While Firebase provides secure cloud storage for medical records, the security of cloud-based platforms is ultimately dependent on the service provider's infrastructure. Although Firebase employs strong security measures, healthcare organizations must be cautious about potential data breaches or outages affecting the cloud provider. Furthermore, the project does not explore multi-cloud or hybrid cloud architectures that could provide enhanced security and fault tolerance by distributing data across different cloud environments.

4. *Scalability in Large Healthcare Systems:* The proposed system was designed for typical healthcare scenarios involving moderate data volumes and user access. However, large-scale implementations, such as nationwide healthcare networks or multi-hospital systems, could pose scalability challenges. Handling thousands or millions of records in real-time while maintaining security and performance is an area that requires further optimization and testing to ensure system reliability under heavy load conditions

VII FUTURE SCOPES

While the secure transmission system presented in this project addresses the fundamental concerns of confidentiality, integrity, and secure data transmission in healthcare environments, there are several areas where the system can be further enhanced and expanded. The following outlines potential future developments and research directions for this project:

1. *Incorporation of Advanced Encryption Techniques: Homomorphic Encryption:* As an alternative to traditional symmetric encryption methods, fully homomorphic encryption (FHE) could be explored to allow for computations on encrypted data without needing to decrypt it. This would be particularly useful in cloud-based healthcare applications where data needs to be processed by third-party services (e.g., for predictive analysis, machine learning) without compromising privacy.

2. *Integration with Internet of Things (IoT):* With the rise of wearable healthcare devices, IoT is becoming increasingly important in healthcare data transmission. Future research could explore the integration of IoT devices, such as heart rate monitors, glucose sensors, and fitness trackers, into the secure transmission system. This would require developing lightweight encryption methods tailored for resource-constrained IoT devices to ensure the secure transmission of real-time health data to healthcare providers or cloud systems.

3. *AI and Machine Learning Integration:* Machine learning (ML) algorithms could be integrated into the system to identify patterns in the encrypted data, helping to detect potential security threats, unauthorized access, or anomalies in medical records transmissions. Machine learning models could be trained on historical data to predict and pre-emptively mitigate security risks in the healthcare data transfer process.

VIII. REFERENCES

[1] Q. Xia, E. Sifah, K. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017

[2] H. Chen, I. Papakonstantinou, and T. Steinke, "FHE for Healthcare: Secure Computation on Medical Records," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3576–3588, 2021.

[3] J. Zhang, Y. Zhou, H. Xu, and W. Wang, "Lightweight cryptographic protocols for IoT-based healthcare," *IEEE Communications Magazine*, vol. 60, pp. 24–29, 2022.

[4] A. Kumar, D. Saxena, and P. Gupta, "Secure Multi-Cloud Architecture for Healthcare Data Management," *IEEE Cloud Computing*, vol. 7, pp. 52–62, 2020.

[5] M. Li, S. Yu, and Y. Zheng, "Attribute-based encryption for secure access to EHRs," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 618-633, 2022.

IS Report.docx

Match Overview

14%

14

1	fastercapital.com Internet Source	3%
2	easychair.org Internet Source	1%
3	citeseerx.ist.psu.edu Internet Source	1%
4	Jamuna S. Murthy, G. ... Publication	1%
5	wap.dgxieli.com Internet Source	1%
6	brightideas.houstontx.... Internet Source	1%
7	www.lansweeper.com Internet Source	1%
8	H L Gururaj, M R Pooja, ... Publication	1%
9	dzone.com	1%

High Resolution On