ENHANCING THE SEQURITY OF HEALTH CARE DATA IN CLOUD COMPUTING ENVIRONMENT

Minhaj Begum , P.Sirignya Reddy, G.Sriya , C.Varsha

1 Associate Professor, Department of Information Technology, Bhoj Reddy Engineering College for Women

2.3.4 B,tech students, Department of *Information Technology, Bhoj Reddy Engineering College for Women*

sriya2004gajawada@gmail.com

ABSTRACT

Cloud computing has revolutionized the healthcare sector by enabling scalable infrastructure, efficient data sharing, and cost-effective storage solutions. However, the rapid growth in the volume of sensitive patient data stored in cloud environments has introduced significant security challenges, including cyberattacks, data breaches, and insider threats. Traditional security mechanisms such as passwords, firewalls, VPNs, and basic encryption techniques are no longer sufficient to address these evolving threats.

This paper proposes a robust multi-layered security framework designed to enhance the confidentiality, integrity, and availability of healthcare data in cloud environments. The framework integrates Advanced Encryption Standard (AES) for secure data encryption, SHA-256 hashing for ensuring data integrity, and fine-grained access control mechanisms to regulate user permissions. Additionally, a Zero-Trust authentication model is incorporated to continuously verify users and devices, thereby minimizing insider risks. To further strengthen security, machine learning techniques, specifically the Isolation Forest algorithm, are employed for real-time anomaly detection and proactive threat identification within healthcare datasets.

The proposed system also ensures compliance with international data protection regulations such as HIPAA and GDPR, promoting secure and ethical data handling practices. Experimental analysis demonstrates that the framework significantly improves security, scalability, and reliability, making it a viable solution for modern cloud-based healthcare systems.

KEYWORDS

Cloud Computing, Healthcare Security, AES Encryption, Zero-Trust Model, SHA-256, Access Control, Isolation Forest, Anomaly **Detection**, **HIPAA** Compliance, GDPR Compliance.

OBJECTIVE

The objective of this project is to design and develop a robust multi-layered security framework to protect sensitive healthcare data in cloud environments by overcoming the limitations of traditional security mechanisms. The framework incorporates advanced techniques such as AES for strong data encryption, ECC for secure key exchange, and SHA-256 for ensuring data integrity. It also implements fine-grained access control using RBAC and ABAC to regulate user permissions effectively. A Zero-Trust security model is integrated to enable continuous verification of users and devices, thereby minimizing insider threats. Furthermore, the project utilizes the Isolation Forest algorithm for early anomaly detection and proactive identification of potential cyber threats. Overall, the aim is to enhance the confidentiality, integrity, and availability of healthcare data while ensuring regulatory compliance, improving system reliability, and building trust in cloud-based healthcare systems.

NEED FOR STUDY

The objective of this project is to design and develop a robust multi-layered security framework to protect sensitive healthcare data in cloud environments by overcoming the limitations of traditional security mechanisms. The framework incorporates advanced techniques such as AES for strong data encryption, ECC for secure key exchange, and SHA-256 for ensuring data integrity. It also implements fine-grained access control using RBAC and ABAC to regulate user permissions effectively. A Zero-Trust security model is integrated to enable continuous verification of users and devices, thereby minimizing insider threats. Furthermore, the project utilizes the Isolation Forest algorithm for early anomaly detection and proactive identification of potential cyber threats. Overall, the aim is to enhance the confidentiality, integrity, and availability of healthcare data while ensuring regulatory compliance, improving system reliability, and building trust in cloud-based healthcare systems.

EXISTING SYSTEM

he current healthcare security systems largely rely on conventional security mechanisms such as password-based authentication, firewalls, Virtual Private Networks (VPNs), and traditional encryption techniques like RSA and DES. These methods provide only a basic level of protection and are increasingly inadequate in defending against modern and sophisticated cyber threats. Although they restrict access to authorized users, they do not fully guarantee the confidentiality and integrity of sensitive healthcare data, making systems susceptible to data breaches and insider misuse.

Furthermore, cloud-based Electronic Health Record (EHR) systems implement standard access control mechanisms and audit trails to track user activities. However, these traditional approaches lack the capability to effectively detect or prevent advanced cyberattacks. As a result, existing systems fall short in providing comprehensive security, emphasizing the need for more robust, intelligent, and multi-layered security frameworks in healthcare environments.

PROPOSEDSYSTEM

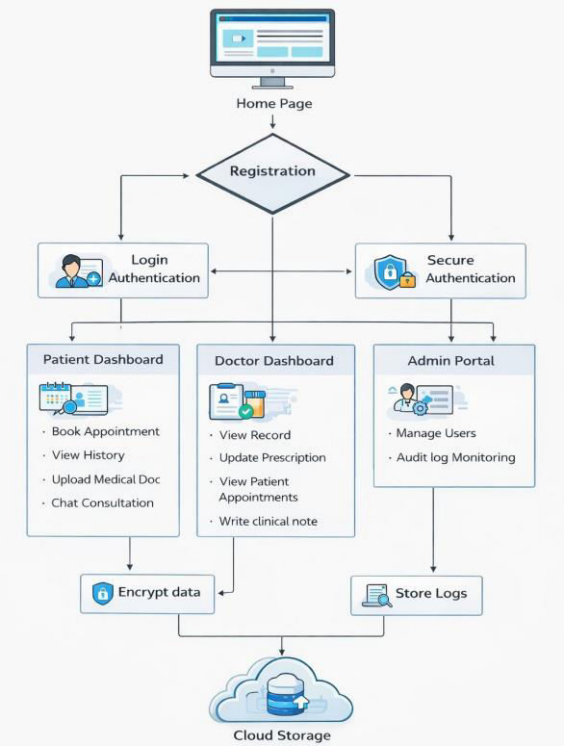
The proposed system introduces a robust multi-layered security framework designed to enhance the protection of sensitive healthcare data in cloud environments. It utilizes Advanced Encryption Standard (AES) for secure data encryption and Elliptic Curve Cryptography (ECC) for efficient and secure key exchange. To ensure precise and flexible access management, the system integrates Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), enabling fine-grained control over user permissions. Data integrity is maintained using the SHA-256 hashing algorithm, ensuring that information remains accurate and tamper-proof.

In addition, the system adopts a Zero-Trust security model, which continuously verifies users and devices, thereby significantly reducing the risk of insider threats. To further strengthen security, the framework incorporates the Isolation Forest algorithm for anomaly detection, allowing early identification of unusual patterns and potential cyber threats within healthcare datasets. Overall, the proposed approach improves security, scalability, and reliability, while also enhancing patient trust in cloud-based healthcare systems.

Functional Requirements

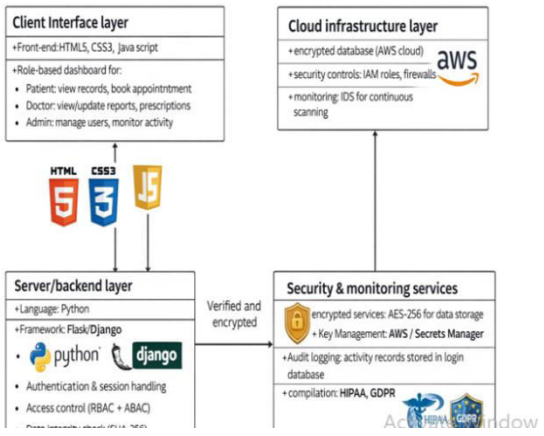
The functional requirements of this project focus on ensuring secure access and protected data handling within a cloud-based healthcare system. The system is designed to implement strong user authentication using a Zero-Trust approach, ensuring continuous verification of users and devices. It enforces fine-grained access control through Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), allowing only authorized users to access sensitive healthcare information. All data, both at rest and in transit, is secured using advanced encryption techniques such as AES and ECC, while SHA-256 is used to maintain data integrity. Additionally, the system incorporates an anomaly detection mechanism using the Isolation Forest algorithm to identify unusual activities and potential security threats. These functionalities collectively ensure a secure, reliable, and efficient healthcare data management framework.

- **User Authentication & Zero-Trust:** The system provides secure login with multi-factor authentication and continuously verifies users and devices based on a Zero-Trust model.
- **RBAC & ABAC Access Control:** The system enforces fine-grained access control based on user roles and attributes to ensure only authorized access.
- **Data Encryption & Integrity:** The system encrypts data using AES, supports secure key exchange through ECC, and ensures integrity using SHA-256.
- **Anomaly Detection & Monitoring:** The system uses Isolation Forest to detect irregular patterns and generate alerts for potential threats.

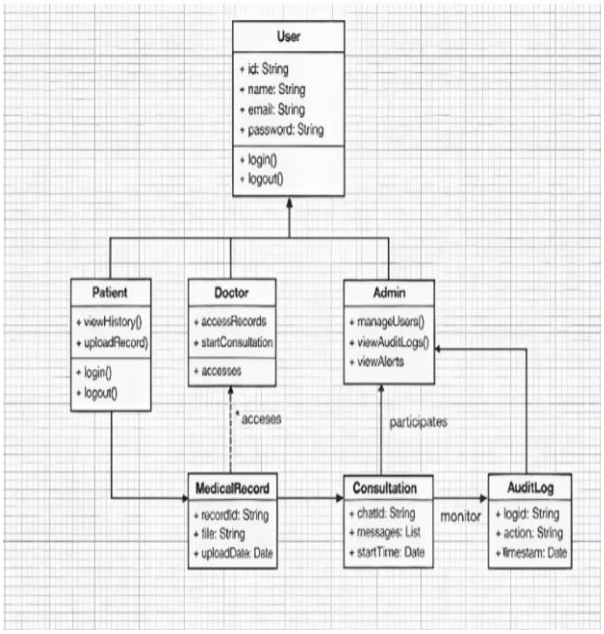


SYSTEM ARCHITECTURE

Technical Architecture



Class Diagram



SYSTEM REQUIREMENTS

1. Hardware Requirements

- **Processor:** Minimum Intel i5 or equivalent (Recommended: Intel i7 / AMD Ryzen 7 for faster model training)
- **RAM:** Minimum 8 GB (Recommended: 16 GB or higher for handling large datasets)
- **Storage:** At least 256 GB SSD (Recommended: 512 GB or higher for faster data access)
- **GPU (Optional):** NVIDIA GPU (for deep learning models and faster computation)

Hardware Requirements

- **Processor:** Intel i5 or higher
- **RAM:** Minimum 16 GB
- **Storage:** Minimum 1 TB Hard Disk

Non-Functional Requirements

The non-functional requirements ensure that the healthcare security system operates efficiently, reliably, and remains user-friendly. The system is designed to deliver high performance with fast processing speeds, scalability to accommodate increasing users and data volumes, and high availability to ensure uninterrupted services. It emphasizes usability through a simple and intuitive interface while maintaining strict compliance with standards such as HIPAA and GDPR. Furthermore, the system ensures strong security, low latency, and consistent accuracy in anomaly detection .

Scalability

- Supports growth in users, devices, and healthcare data.
- Allows seamless expansion of cloud resources as required.

Performance

- Ensures fast data processing and quick response times.
- Efficiently handles large-scale healthcare datasets without performance degradation.

Reliability

- Provides high system uptime with minimal interruptions.
- Ensures consistent and dependable access to data.

Usability

- Offers a user-friendly and intuitive interface.
- Enables easy navigation with minimal learning effort.

Security

- Ensures strong protection through encryption and fine-grained access control.
- Continuously monitors and detects potential cyber threats.

Compliance

- Adheres to regulatory standards such as HIPAA and GDPR.
- Ensures ethical and legal handling of patient data.

Interoperability

- Integrates smoothly with existing healthcare systems.
- Supports standard data formats for easy data exchange.

Data Integrity

- Maintains accuracy and consistency of data.
- Detects unauthorized changes using verification mechanisms.

Maintainability

- Supports easy system updates, bug fixes, and enhancements.
- Ensures integrity checks to identify and prevent unauthorized modifications.

MODULE DESCRIPTION

Authentication & Authorization Module: Ensures secure login and access using role-based control (Patient, Doctor, Admin). It follows a zero-trust model where every request is verified to prevent unauthorized access.

Patient Module:
Allows patients to book appointments, upload and share medical records securely, and view prescriptions and history. It also supports safe communication with doctors.

Doctor Module:
Enables doctors to manage appointments, access authorized patient data, write prescriptions, and communicate securely with patients.

Data Encryption & Integrity Module: Protects medical data using AES encryption and ensures data integrity using SHA-256 hashing.

Secure Cloud Storage:
Stores all data in encrypted form using AWS cloud to ensure safe and reliable storage.

Audit Logging & Monitoring Module: Tracks all user activities such as login and data access to detect suspicious actions and maintain system transparency.

Anomaly Detection Module:
Uses Isolation Forest algorithm to identify unusual behavior and generate alerts for potential threats.

Admin Security Dashboard:
Provides a centralized system for monitoring logs, managing users, and handling security alerts without exposing sensitive data..

CHALLENGES&RISKS

Data Security Threats: Risk of cyberattacks, data breaches, and unauthorized access to sensitive healthcare data.

Complex Implementation: Integrating encryption, access control, and machine learning increases system complexity.

Performance Overhead: Security layers and encryption may affect system speed and response time.

Insider Threats: Authorized users may misuse access despite security controls.

Model Accuracy Issues: Anomaly detection (Isolation Forest) may produce false positives or miss real threats.

Scalability Challenges: Handling large volumes of healthcare data and users efficiently.
Compliance Risks: Failure to meet regulations like HIPAA and GDPR may lead to legal issues.

Key Management Risks: Secure storage and handling of encryption keys is critical and challenging

FUTURE ENHANCEMENT

Integration of Advanced AI Models: Implement deep learning techniques to improve accuracy in anomaly detection and threat prediction.
Blockchain Integration: Use blockchain technology for secure, tamper-proof storage and sharing of healthcare records.
Biometric Authentication: Add fingerprint or facial recognition for stronger user authentication.
Real-Time Threat Intelligence: Incorporate real-time monitoring systems to detect and respond to cyber threats instantly.
Multi-Cloud Support: Extend the system to work across multiple cloud platforms for better reliability and flexibility.
Mobile Application Development: Develop mobile apps for easier access by patients and doctors.
Automated Incident Response: Enable automatic actions (like account blocking) when suspicious activity is detected.
Enhanced User Interface: Improve usability with more interactive and user-friendly dashboards.
Integration with IoT Devices: Support data from wearable health devices for real-time monitoring.

Improved Compliance Features: Add automated tools to ensure continuous compliance with evolving regulations like HIPAA and GDPR.

Conclusion

In conclusion, this project presents a robust and secure multi-layered framework for protecting sensitive healthcare data in cloud environments. By integrating advanced techniques such as AES encryption, ECC for secure key exchange, RBAC and ABAC for fine-grained access control, and SHA-256 for data integrity, the system ensures strong protection of data confidentiality, integrity, and availability. The adoption of a Zero-Trust security model further enhances system security by continuously verifying users and devices, thereby reducing insider threats.

Additionally, the incorporation of machine learning through the Isolation Forest algorithm enables proactive anomaly detection, helping to identify potential cyber threats at an early stage. The system also aligns with regulatory standards such as HIPAA and GDPR, ensuring secure and ethical handling of healthcare data. Overall, the proposed framework improves security, scalability, and reliability, making it a suitable solution for modern cloud-based healthcare systems while fostering trust among users.

REFERENCES

1. P. Selvi and S. Sakthivel, “A hybrid ECC-AES encryption framework for secure and efficient cloud-based data protection,” Scientific Reports, 2025. (PubMed)

2. R. Walid, K. P. Joshi, and S. G. Choi, “Comparison of attribute-based encryption schemes in securing healthcare systems,” Scientific Reports, vol. 14, 2024. (Nature)

3. L. Zhao, G. Dong, and H. Yuan, “A blockchain-based verifiable CP-ABE scheme for medical data privacy protection,” Scientific Reports, 2025. (Nature)

4. S. Rehman et al., “Hybrid AES-ECC Model for the Security of Data over Cloud Storage,” Electronics, vol. 10, no. 21, 2021. (ResearchGate)

5. N. Abirami and M. S. Anbarasi, “An Efficient Multilayer Approach for Securing E-Healthcare Data in Cloud using Crypto-Stego Technique,” Engineering World, 2024. (OUCI)

6. C. Sri Sumanth, Y. R. R. Reddy, and N. S. Chaitanya, “De-duplicating Encrypted Data using ABE & ECC for Secured Cloud Environment,” International Journal of Engineering and Technology, 2018. (Science Publishing Corporation)

7. K. Sowjanya et al., “A lightweight ECC-based CP-ABE scheme for IoT healthcare systems,” Future Generation Computer Systems / IEEE-based references, 2021. (ScienceDirect

8. W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed., Pearson, 2017.

9. C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2010.

10. D. R. Stinson and M. B. Paterson, Cryptography: Theory and Practice, CRC Press, 2018.

11. T. Erl, R. Puttini, and Z. Mahmood, Cloud Computing: Concepts, Technology & Architecture, Prentice Hall, 2013.

12. K. Hwang, G. Fox, and J. Dongarra, Distributed and Cloud Computing: From Parallel Processing to the Internet of Things, Morgan Kaufmann, 2012.

13. National Institute of Standards and Technology (NIST), “Advanced Encryption Standard (AES)” https://nvlpubs.nist.gov

14. National Institute of Standards and Technology (NIST), “SHA-256 Secure Hash Standard”