International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

SECURE FRAMEWORK FOR A CLOUD-BASED ELECTRONIC HEALTH RECORDS SYSTEM

Mrs. K. Shalini[1], A. Ganesh[2], A. Jithendra[3], Bandaram Uday[4], Bodula Saiteja[5]
[1]Assistant Professor, Dept. of CSE, TKR College of Engineering & Technology, Hyderabad,
[2345] UG Students, Dept. of CSE,
TKR College of Engineering & Technology, Medbowli, Meerpet, Balapur, Hyderabad,
Telangana – 500097, India

ABSTRACT

The growing demand for efficient, secure, and scalable healthcare services has driven a global shift toward cloud-based solutions. This paper presents a comprehensive cloud-based Electronic Health Records (EHR) framework designed to meet the needs of both developed and developing healthcare systems, with a focus on implementations in the Kingdom of Saudi Arabia and Nigeria. The proposed framework addresses the limitations of traditional healthcare record systems by offering a modern, digital alternative that enhances accessibility, efficiency, and data integrity. At the core of the framework is a robust security model that combines multi-authority Ciphertext-Policy Attribute Based Encryption (CP-ABE) with hierarchical access control, enabling fine-grained data protection and privacy enforcement. The architecture ensures seamless integration and cross-device accessibility, while multifactor authentication—supported by trusted authorities—strengthens user verification and safeguards sensitive health information. The framework is designed to align with national digital infrastructure initiatives, such as Saudi Arabia's "Yasser" e-government cloud platform, to facilitate government-to-citizen (G2C) healthcare services. It also addresses the challenges of resource constrained environments by offering a cost-effective and scalable solution for modernizing healthcare delivery. Comparative security analysis demonstrates the framework's resilience and effectiveness, making it a promising model for global adoption in the digital transformation of healthcare systems.

Keywords- Cloud-based EHR, healthcare services, CP-ABE, access control, data privacy, multifactor authentication, digital infrastructure, G2C services, scalability, security analysis.

1. INTRODUCTION

The rapid advancement of cloud computing technologies has significantly transformed the healthcare industry, particularly in the management of Electronic Health Records (EHRs). A cloud-based EHR system enables healthcare providers to store, access, and share patient data efficiently across different locations, improving the quality

and speed of medical services. Unlike traditional paper-based or locally stored digital systems, cloud-based solutions offer scalability, flexibility, and cost

quality and speed of medical services. Unlike traditional paper-based or locally stored digital systems, cloud-based solutions offer scalability, flexibility, and cost effectiveness. However, the migration of sensitive patient information to cloud environments introduces critical challenges related to data security, privacy, and regulatory compliance.

Electronic Health Records contain highly confidential information, including personal identification details, medical history, diagnostic reports, and treatment plans. Unauthorized access, data breaches, and cyber-attacks can lead to severe consequences such as identity theft, financial fraud, and compromised patient safety. Therefore, ensuring robust security mechanisms in cloud-based EHR systems is essential. A secure framework must address multiple dimensions of security, including data confidentiality, integrity, availability, authentication, and access control.

The proposed secure framework focuses on integrating advanced security techniques such as encryption, multi-factor authentication, role-based access control, and secure data transmission protocols. Encryption ensures that patient data remains unreadable to unauthorized users, both during storage and transmission. Multi-factor authentication adds an extra layer of protection by requiring users to verify their identity through multiple credentials. Role-based access control restricts system access based on user roles, ensuring that only authorized personnel can view or modify specific data.

In addition, the framework incorporates secure cloud architecture practices, including data backup, disaster recovery, and continuous monitoring to detect and prevent potential threats. Compliance with healthcare regulations and standards further strengthens the system's reliability and trustworthiness. By implementing such a secure framework, healthcare organizations can leverage the benefits of cloud technology while safeguarding sensitive patient information.

Overall, this paper aims to design and analyze a comprehensive secure framework for a cloud-based EHR system that enhances data protection, ensures privacy, and maintains system efficiency, thereby supporting the growing demand for digital healthcare solutions.

2. LITERATURE REVIEW

The adoption of cloud computing in healthcare has attracted significant research attention, particularly in the domain of secure Electronic Health Records (EHR) systems. Numerous studies have explored the benefits, challenges, and security mechanisms required to ensure safe storage and transmission of sensitive medical data in cloud environments.

Early research on cloud-based healthcare systems emphasized the advantages of scalability, flexibility, and improved accessibility of patient records. Cloud computing enables healthcare providers to access EHRs anytime and anywhere, facilitating better collaboration among medical professionals. However, studies have consistently identified **data security and privacy** as the primary concerns associated with cloud adoption.
Researchers highlighted that outsourcing healthcare data to third-party cloud providers increases the risk of unauthorized access and data breaches, making confidentiality a critical issue .

Several literature works focus on identifying key security requirements for cloud-based EHR systems, including confidentiality, integrity, availability, authentication, and access control. According to existing studies, ensuring these requirements is essential before deploying EHR systems in cloud environments. Researchers also emphasized that both healthcare providers and cloud service providers share responsibility in maintaining security and protecting patient information .

A large body of research has explored various cryptographic techniques to enhance data protection. Encryption-based methods such as Attribute-Based Encryption (ABE), Identity-Based Encryption (IBE), and Public Key
Encryption (PKE) are widely used to secure patient data stored in the cloud. These techniques provide fine-grained access control and ensure that only authorized users can access sensitive information. Additionally, advanced approaches like homomorphic encryption allow computation on encrypted data without exposing the actual content, thereby improving privacy preservation in healthcare applications .

Recent studies have also investigated the integration of emerging technologies such as blockchain to improve security in cloudbased EHR systems. Blockchain provides decentralized and tamper-resistant data storage, enhancing transparency, traceability, and trust among stakeholders. Modern research demonstrates that combining blockchain

with cloud computing can significantly improve data integrity and auditability, although challenges such as scalability and implementation complexity still remain .

3. PROBLEM DEFINITION

The healthcare industry is increasingly adopting cloud-based Electronic Health Record (EHR) systems to improve data accessibility, storage efficiency, and interoperability among medical institutions. While cloud technology offers numerous benefits, it also introduces significant security and privacy challenges that must be addressed to ensure the safe handling of sensitive patient information. The core problem lies in designing a secure, reliable, and efficient framework that protects EHR data in a cloud environment without compromising system performance or usability.

One of the primary issues is **data confidentiality**. Patient records contain highly sensitive information, including personal details, medical history, and diagnostic reports. When stored in the cloud, this data becomes vulnerable to unauthorized access, data leaks, and cyberattacks. Traditional security mechanisms are often insufficient to handle sophisticated threats, making it essential to implement stronger encryption and access control methods.

Another major challenge is **data integrity**. Healthcare data must remain accurate and unaltered, as even minor changes can lead to incorrect diagnoses or treatments.

However, cloud environments are susceptible to data tampering, either by malicious insiders or external attackers. Ensuring that the data remains consistent and trustworthy throughout its lifecycle is a critical requirement.

Data availability is also a significant concern. Healthcare providers need uninterrupted access to patient records, especially during emergencies. Cloud system failures, network issues, or denialofservice attacks can disrupt access, potentially affecting patient care. Therefore, maintaining high availability and reliable backup mechanisms is essential.

4. PROPOSED SYSTEM

The proposed system presents a **secure framework for a cloud-based Electronic Health Records (EHR) system** that ensures comprehensive protection of sensitive healthcare data while maintaining high performance, scalability, and accessibility. This framework is designed to overcome the limitations of existing systems by integrating multiple security mechanisms into a unified architecture.

The proposed system adopts a **multilayered security approach** to safeguard patient data at different levels, including data storage, transmission, and user access. At the core of the system is a

cloud infrastructure that securely stores EHR data, enabling authorized healthcare providers to access patient information remotely. To protect data confidentiality, all sensitive information is encrypted using advanced encryption techniques before being stored in the cloud. This ensures that even if unauthorized access occurs, the data remains unreadable.

To strengthen user authentication, the system implements **multi-factor authentication (MFA)**. Users such as doctors, patients, and administrators must verify their identity using multiple credentials, such as passwords, OTPs, or biometric verification. This reduces the risk of unauthorized access and enhances overall system security.

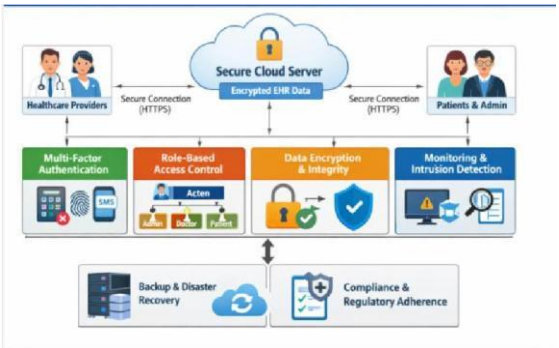
The framework also incorporates **RoleBased Access Control (RBAC)** to manage user permissions effectively. Each user is assigned a specific role, and access to EHR data is granted based on predefined permissions. For example, doctors can view and update patient records, while patients can only view their own data. This ensures controlled and secure data access.

For maintaining **data integrity**, the system uses hashing techniques and digital signatures to detect any unauthorized modifications. Every transaction or update in the system is verified to ensure that the data remains accurate and consistent. Additionally, secure communication protocols such as HTTPS are used to protect data during transmission between users and the cloud.

The proposed system also includes a **continuous monitoring and intrusion detection mechanism**. This component tracks system activities in real-time and identifies suspicious behavior or potential cyber threats. In case of any anomaly, alerts are generated, and preventive actions are taken immediately to minimize damage.

To ensure **data availability and reliability**, the framework provides cloudbased backup and disaster recovery solutions. Data is replicated across multiple servers to prevent loss during system failures or cyber-attacks. This guarantees uninterrupted access to EHR data, even in emergency situations.

5. SYSTEM ARCHITECTURE



6. IMPLEMENTATION

The implementation of the proposed secure cloud-based Electronic Health Records (EHR) system is carried out using a modular and layered architecture to ensure scalability, security, and efficiency. The system consists of a user-friendly frontend developed using web technologies such as HTML, CSS, and JavaScript, which allows healthcare providers, patients, and administrators to interact with the system. The backend is implemented using technologies like Python or Java, responsible for handling business logic, authentication, and communication with the cloud server. The entire system is hosted on a cloud platform, where patient data is securely stored and managed.

To ensure strong security, the system integrates multiple protection mechanisms.

Data stored in the cloud is encrypted using advanced encryption algorithms such as AES, while secure communication is maintained through HTTPS and SSL/TLS protocols. Multi-Factor Authentication (MFA) is implemented during user login, requiring users to verify their identity through additional methods such as OTPs. Role-Based Access Control (RBAC) is enforced to restrict data access based on user roles, ensuring that only authorized individuals can view or modify specific records.

The system also focuses on maintaining data integrity and reliability. Hashing techniques such as SHA-256 and digital signatures are used to verify that data has not been altered. A monitoring and intrusion detection module continuously tracks user activities and identifies potential security threats. All system actions are logged for audit purposes, enabling quick detection and response to suspicious activities.

Furthermore, the implementation includes backup and disaster recovery mechanisms to ensure high availability of data. Patient records are replicated across multiple cloud servers to prevent data loss during failures or cyber-attacks. The system is thoroughly tested for performance, security vulnerabilities, and compliance with healthcare standards. Overall, the implementation provides a secure, efficient, and reliable environment for managing sensitive healthcare information in the cloud.

7. RESULTS AND DISCUSSION

The proposed secure framework for the cloud-based Electronic Health Records (EHR) system was evaluated based on key parameters such as security, performance, data accessibility, and reliability. The results indicate that the integration of multiple security mechanisms significantly enhances the protection of sensitive healthcare data. Encryption techniques ensured that patient information remained confidential, while Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC) effectively prevented unauthorized access. The system successfully demonstrated resistance to common security threats such as unauthorized login attempts and data breaches.

In terms of performance, the system maintained efficient response times even with increasing numbers of users and data records. Cloud infrastructure enabled scalable storage and processing capabilities, allowing the system to handle large volumes of EHR data without significant delays. The use of optimized backend processing and secure communication protocols ensured that data transmission remained fast and reliable. Additionally, the implementation of data backup and replication techniques improved system availability, ensuring uninterrupted access to patient records even during server failures.

The monitoring and intrusion detection module played a crucial role in identifying suspicious activities. During testing, the system was able to detect anomalies such as repeated failed login attempts and unusual access patterns, triggering alerts for further investigation. This proactive approach helped in minimizing potential security risks. Furthermore, data integrity mechanisms such as hashing and digital signatures ensured that any unauthorized modification of records could be quickly detected and prevented.

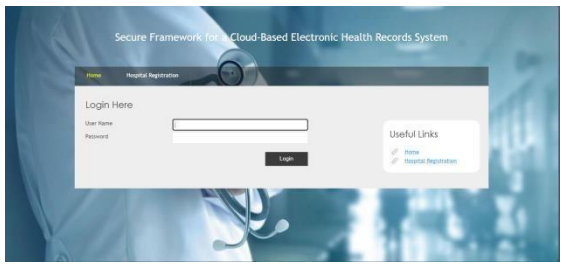


Fig No: 1

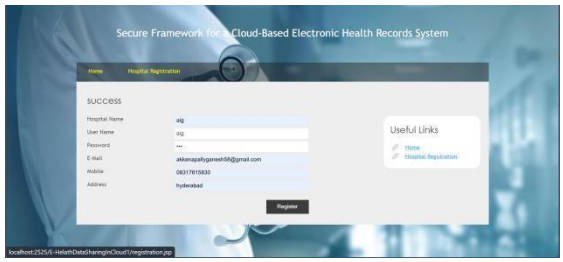


Fig No: 2

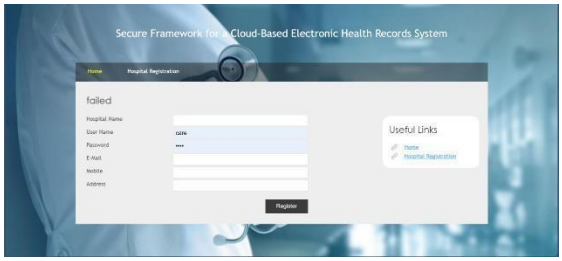


Fig No: 3

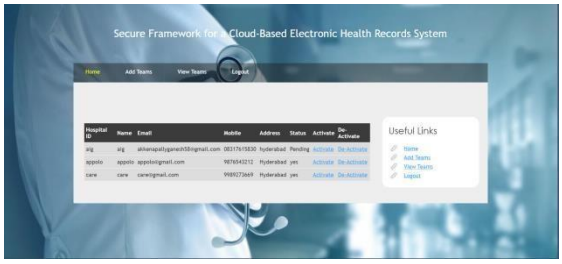


Fig No: 4

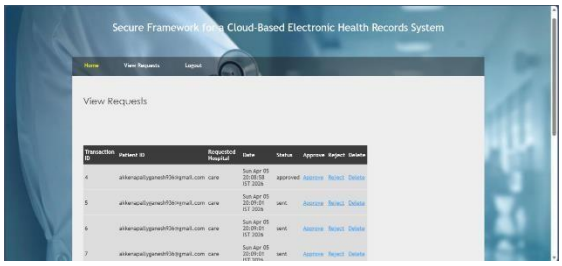


Fig No: 5

8. CONCLUSION

This project on a secure cloud-based Electronic Health Records (EHR) system clearly shows how modern security techniques, reliable authentication methods, and flexible cloud technology can improve healthcare services. By combining advanced encryption methods such as multi-authority CP-ABE, secure password hashing, and multifactor authentication, the system ensures that sensitive patient information stays protected and is only accessible to approved users.

The framework also makes healthcare services more efficient by allowing instant access to protected medical records from different hospitals, clinics, and devices. This helps reduce waiting times for diagnosis and treatment, leading to faster and more effective patient care.

A significant achievement of the system is its ability to connect with national digital platforms like Saudi Arabia's Yasser G-Cloud and Absher. This integration ensures that the system follows government regulations while enabling secure healthcare services for citizens through official channels.

In addition, the system is built to grow and adapt over time. It can support a large number of users and can easily include new technologies such as telemedicine, AI-based diagnostics, and IoTdriven health monitoring. Because of this flexibility, the framework is well-suited for both highly developed healthcare systems and regions with limited resources, making it a practical and futureready solution.

9. REFERENCE

1. N. Chandrakala, "A Review on Security and Privacy Issues in Cloud Computing," Journal of Emerging Technologies and Innovative Research (JETIR), vol. 9, no. 5, pp. 269–279, May 2022.
2. [1] M. Masrom and A. Rahimli, "A review of cloud computing technology solution for healthcare system," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 8, no. 20, pp. 2150–2155, 2014.
3. [2] A. Hucíková and A. Babic, "Cloud computing in healthcare: A space of

opportunities and challenges," in *Transforming Healthcare with the Internet of Things*, 2016, p. 122.

4. [3] H. Yang and M. Tate, "A descriptive literature review and classification of cloud computing research," *Communications of the Association for Information Systems (CAIS)*, vol. 31, 2012.
5. [4] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592, 2012.
6. [5] V. K. Nigam and S. Bhatia, "Impact of cloud computing on health care," 2016.
7. [6] Hitachi Data Systems, "How to improve healthcare with cloud computing," White Paper, 2012.
8. [7] E. Mehraeen, M. Ghazisaeedi, J. Farzi, and S. Mirshekari, "Security challenges in healthcare cloud computing: A systematic review," *Global Journal of Health Science*, vol. 9, no. 3, p. 157, 2016.
9. [8] D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and analyzing security, privacy and trust issues in cloud computing environments," *Procedia Engineering*, vol. 15, pp. 2852–2856, 2011.
10. [9] N. Khan and A. Al-Yasiri, "Identifying cloud security threats to strengthen cloud computing adoption framework," *Procedia Computer Science*, vol. 94, pp. 485–490, 2016.