ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar2029

Data Encryption and Access Control in Cloud-Based Healthcare Systems

Rushil Patel[1*]; Vidhi Sutaria[2]

[1]Asha M. Tarsadia Institute of Computer Science and Technology, Uka Tarsadia University, Surat, Gujarat, India
[2]Asha M. Tarsadia Institute of Computer Science and Technology, Uka Tarsadia University, Surat, Gujarat, India

Corresponding Author: Rushil Patel[1*]

Publication Date: 2026/04/09

Abstract: The growth of cloud computing has emerged as a critical enabling technology for today's healthcare systems, providing on-demand access to large amounts of medical data, including electronic health records (EHRs), diagnostic images, and clinical documentation. However, the benefits of cloud-based medical information will be contradicted by challenges with securing and maintaining the privacy of electronic medical records. The medical data hosted in cloud computing environments (such as hospitals) is at risk of being stored and opened inappropriately or accessed inappropriately. This research focused on the current practices used to secure sensitive data, including access control and virus protection. A number of different encryption mechanisms are available to ensure that sensitive medical records remain confidential at the time of storage and/or in transit. A number of different access control models are available to provide structured methods to manage user access, user authentication, etc. The proposed research presents a new layered security model integrating encryption with role-based authorization and identity authentication. A functioning example of this research demonstrates how authentication, authorization, and activity logging can be leveraged to prevent unauthorized access to healthcare records. The results of the study show that the use of encryption technologies with a structured access policy for accessing sensitive healthcare records will greatly improve the security and access to sensitive medical information for authorized medical personnel utilizing cloud-based healthcare systems.

Keywords: *Cloud Computing, Healthcare Data Security, Data Encryption, Access Control Models, Role-Based Access Control, Identity and Access Management, Cloud Security Framework.*

How to Cite: Rushil Patel; Vidhi Sutaria (2026) Data Encryption and Access Control in Cloud-Based Healthcare Systems. *International Journal of Innovative Science and Research Technology*, 11(3), 3684-3689. https://doi.org/10.38124/ijisrt/26mar2029

I. INTRODUCTION

By offering extremely scalable storage, efficient data management, and ability to remotely access medical record systems, cloud computing has become a dominant player in providing technology solutions to the rapidly changing landscape of modern-day healthcare systems [13]. Hospitals and healthcare providers are increasingly using cloud technologies for electronic health records (EHR), medical imaging data, lab results, and other patient information (laboratory data, patient demographics, etc.) to improve collaboration among the healthcare workforce, reduce overall infrastructure expenses, and provide fast access to historical and real-time patient data [9].

Despite the advantages of using cloud tools and services, organizations using cloud-based healthcare technologies continue to face significant security risks associated with the protection of patient records [5]. The types of sensitive patient data are extreme (e.g., patient identifying information) and include all of the information contained in a patient's medical record - including their medical history, any diagnostic reports, and any treatments provided to them [4].

Because of the sensitivity of healthcare data, and in light of the security risks associated with storing and sending patient records via cloud-based systems, it is critical that organizations utilizing these technologies protect patient data [1].

One of the biggest issues surrounding the use of cloud technology in healthcare organizations is the potential for unauthorized access to patient records [21]. In most cases, cloud systems are managed and operated by a third-party service provider, which requires the healthcare organization

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar2029

to ensure that the sensitive data remains protected during both storage and transit. Encryption is an excellent method for securing sensitive patient data by converting plain-text data to encrypted data that cannot be read without the appropriate decryption key [7].

Access control mechanisms, along with encryption, are very important to ensuring secure access to healthcare data [8]. Access control mechanisms regulate and enforce how users are allowed to interact with system resources, guaranteeing that only those individuals who have been given permission can access that information. Modern cloud-based systems will implement Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), two popular access control mechanisms, to efficiently manage user permissions [18].

This paper reviews the design and use of both encryption and access control mechanisms to provide secure access to healthcare data stored in the cloud. The proposed framework shows how the integration of structured access control policy and data encryption may provide a more secure and reliable method of protecting cloud-based healthcare data.

II. RELATED WORK

There have been a number of studies done on cloud computing security, with the majority of research breaking down into protecting sensitive data in distributed computing environments [29]. From there, there are many different forms of encryption and access control technologies developed for growing the confidentiality of data and restricting access to unauthorized individuals [5].

Multiple researchers noted the value of using encryption techniques in protecting sensitive cloud data [11]. Encrypted data changes from plain text to encrypted text. This transformation ensures that sensitive cloud data is protected while in storage or during transportation. Encryption algorithms (symmetric: AES and asymmetric: RSA) are used for encrypting and securing cloud data [7].

More research continues to investigate the use of hybrid cryptography technologies, where users can take advantage of both symmetric and asymmetric encryption methods to provide better security solutions [10]. Using hybrid encryption technology increases the confidentiality of data, while also providing users with greater control of their keys and facilitates secure communication between the cloud service provider and their respective clients [19].

Within data protection, access control mechanisms have also seen vast research in the area of cloud computing [6]. These mechanisms regulate a user's interaction with the cloud's resources through the creation of defined user permissions and policies. They include established (external) models such as Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Identity-Based Access Control (IBAC) to represent a new model for managing dynamic user permissions within cloud applications – Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) [18].

Identity & Access Management (IAM) is a key factor in securing data stored in the Cloud [17]. IAM solutions use authentication methods, define authorization policies, and verify the identity of users for granting access to resources within the Cloud. A well-designed IAM solution protects both the confidentiality (data not disclosed), integrity (data not altered), and availability (data that is able to be accessed by users) of data stored in the Cloud [22].

While researchers have suggested many encryption methods and access control models for healthcare cloud systems, the challenge of integrating those solutions into healthcare cloud systems continues to exist for many vendors [21]. This research intends to provide a layered security framework that consists of a combination of encryption methods and structured access control policies to secure healthcare cloud systems from attack.

➢ *Problem Statement*

Today, more Healthcare Systems that manage Patient Data are embracing the Cloud to store and manage patient data [9]. While the use of Cloud technology improves scalability and availability, it also introduces a series of risks to Security (security breaches) that can compromise the sensitive nature of medical records, including:

- Unauthorized Access/Access Control Issues: One of the most serious issues related to Cloud storage (and the security of data in the Cloud) in the Healthcare Industry is that multiple parties (D/T/L/P) (doctors, technicians, lawyers, and pharmacy) may have access to electronic patient records [21]. If the appropriate Access Control measures are not in place, then a person who is NOT authorized to access that electronic medical record could gain access to a Physician's Confidentiality issue by virtue of the lack of Access Control Security.
- Vulnerable Data in Transit and At Rest: Another major Insufficiency related to the security of Healthcare Data while it is being transmitted via the network is that the data being sent by Healthcare Systems or Practice Management Systems to/from a Cloud Server can be INTENDED to be transmitted encrypted, but they are intercepted by attackers and access to the confidential nature of the Data [7].
- Insider Threats: The term "insider threat" is a term that can be used to describe an employee within an organisation (Facility) who possesses Access Privileges that provide them with the right to view or alter patient records [5]. These employees typically misuse their Access Privileges in order to view (or alter) sensitive patient records. Without appropriate Monitoring or Access Limitations, these types of activities can lead to serious Privacy Violations.

In order to address these three types of Security Threats, Cloud Storage Solutions must have a Thorough and Comprehensive Security Framework associated with their Cloud Storage Solution that takes into account encryption

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar2029

technology and structured Access Control Policies associated with each employee's Access Privileges [8]. Only provide Access to employee's (Healthcare) Data while the data is encrypted when in Storage and when transmitted on the computer network.

➢ *Proposed System: Secure Healthcare Cloud Framework*

The new system is a layered security framework to keep the privacy of healthcare data being managed in the cloud secure from theft or data breaches [5]. This type of architecture uses encryption and role based access control policies, along with the other components, to ensure that only authorized individuals have access to sensitive patient information [8].

The proposed system has three primary components:

- Encryption Layer- In this layer, healthcare data is protected prior to being stored in the cloud or prior to being transmitted [7]. The types of encryption used include AES (advanced encryption standard), RSA (reversible serial encryption), and other algorithms designed to take plain text medical information and convert it into encripted formats that would require special decryption keys to view the original plain text information [10].
- Access Control Layer - In this layer, user permissions are managed based on role based access control policies [18]. Each user is assigned a specific role (physician, nurse, administrator), and their access permission is determined according to the role they were assigned. Thus, if user's job requires that they only view specific patient medical records, the system will restrict access based on the roles defined for each type of users [8].
- Identity Management Layer - The identity management layer provides the ability to verify users and prove they are authorized prior to providing access to the system and the data that the user is requesting to access within the system [17]. To verify an individual's identity, login credentials and/or some form of identity verification is required [22].

The combination of these three layers of security provides a full solution to protecting patient medical records being managed in the cloud [21].

➢ *System Architecture*

The system architecture of the proposed framework consists of multiple layers designed to ensure secure access to healthcare data stored in cloud environments [9].

Fig. 1 shows the secure cloud architecture for healthcare data encryption and access control.

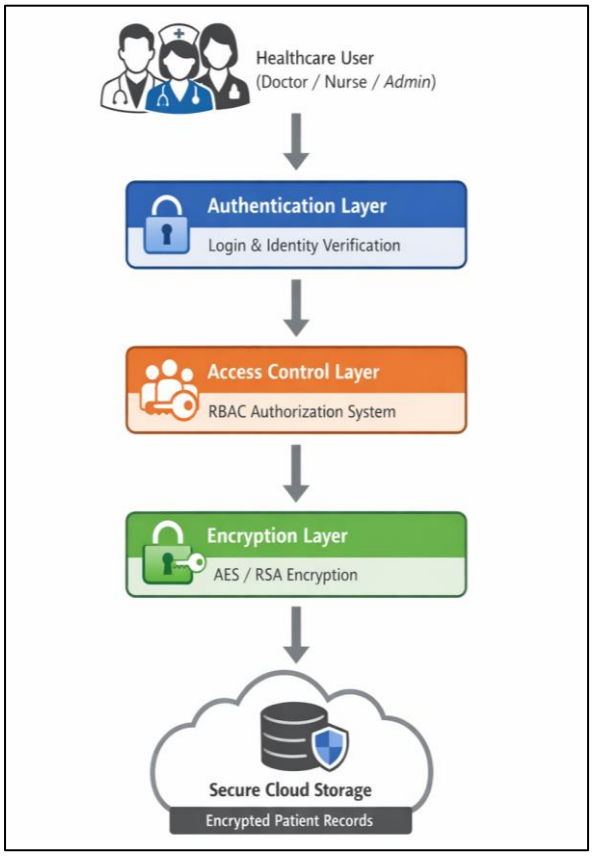

Fig 1 Secure Cloud Architecture for Healthcare Data Encryption and Access Control

The architecture includes the following components:

- Healthcare Application Layer – Provides interfaces for healthcare professionals to access patient records and medical data.
- Authentication Layer – Verifies user identities using login credentials and authentication mechanisms.
- Access Control Layer – Implements role-based policies to determine user permissions.
- Encryption Layer – Protects healthcare data using encryption algorithms before storage and transmission.
- Cloud Storage Layer – Stores encrypted healthcare records within secure cloud servers.

This layered architecture ensures that healthcare data remains protected at every stage of the system, from user authentication to data storage in the cloud.

➢ *Implementation*

A prototype was developed to demonstrate how access control and encryption can be utilized in the cloud for healthcare systems [8]. To create a secure health data management system, the prototype was written in Python and utilized SQLite as its database.

Fig. 2 shows the role-based access control workflow in the healthcare cloud system.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar2029

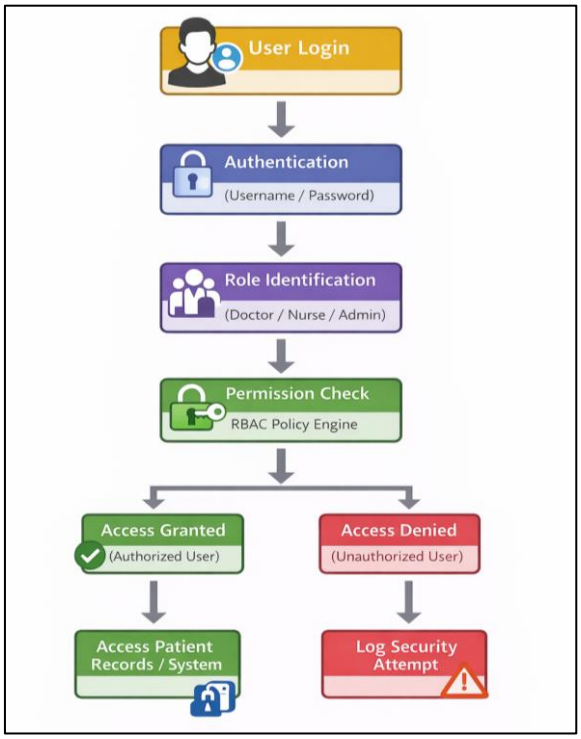

Fig 2 Role-Based Access Control Workflow in Healthcare Cloud System

The prototype includes authentication, access authorization, and logging modules. Users authenticate using their credentials stored in the SQLite database and receive role-based authorization [17].

Fig. 3 shows the encryption process for protecting healthcare data in cloud storage.

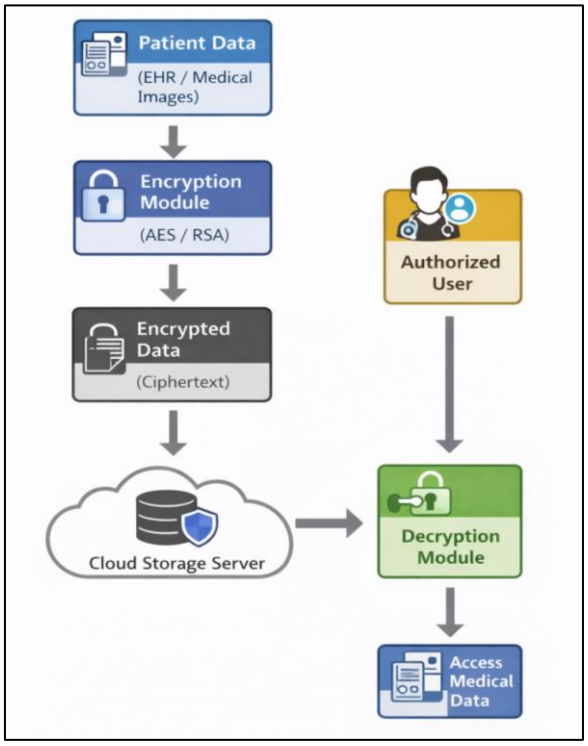

Fig 3 Encryption Process for Protecting Healthcare Data in Cloud Storage

Different types of healthcare workers have different access rights. For example, doctors can view and edit patient records; nurses can view patient records; and administrators can manage all users in the system [18].

The authentication module validates the credentials of the user and retrieves the role of the user from the database [17].

The authorization module of the system checks whether or not the user is permitted to access the requested resource [8]. If not permitted, the user is denied access and this attempt will be recorded in the logs.

Additionally, an access logging module maintains a log of all access attempts to the database to create an audit trail of user activity [22]. This feature allows the healthcare administrator to track usage of the system and also helps to identify possible misuse of the system.

III. RESULTS DISCUSSION AND EXPECTED IMPACT

Integrating encryption technology and implementing Role-Based Access Control (RBAC) techniques into a healthcare cloud environment has concretely established how to improve the security of healthcare clouds using a layered security model [8]; therefore, even if one of the mechanisms used for securing data fails, the integrity of the data is still maintained through the other layers of protection [5].

The encryption control layer of the layered security model ensures that no other individuals except authorized users can interpret confidential information related to patients [7]. The access control layer only allows access to specific users who are permitted to use system resources [18].

Integrity control mechanisms, which are generally referred to as identity management mechanisms, are used to verify user identity before allowing them access control to the system [17]. Furthermore, identity management mechanisms enhance the security of the system by providing authentication before allowing users' access and utilization of the resources of the system [22].

The comparison between the traditional cloud system, existing models and proposed system is shown in Table 1.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar2029

Table 1 Comparison of Proposed System with Existing Healthcare Cloud Security Approaches

Approach	Encryption	Access Control	Identity Management	Security Level
Traditional Cloud Systems	Basic Encryption	Limited Access	Not Defined	Medium
Existing Models	AES / RSA	RBAC / ABAC	Partial	High
Proposed System	AES + RSA	RBAC	IAM Integration	Very High

The comparison clearly indicates that the proposed system provides enhanced security by integrating multiple layers, including encryption, role-based access control, and identity management. This layered approach ensures stronger protection compared to traditional and existing models.

The proposed model improves accountability through the activity logging and monitoring mechanisms [22]; therefore, the healthcare administration can review who performed what activity within the system log and identify who may be trying to hack the system or inappropriately utilize system resources.

In summary, the proposed model provides a practical and scalable approach for securing healthcare data in cloud computing environments [21].

IV. CONCLUSION

Healthcare organizations can greatly benefit from cloud computing due to its ability to create an infrastructure for scalable storage and improved management of medical data [9]. However, the migration of existing healthcare systems to a cloud platform poses significant security risks associated with data privacy and, therefore, potential for unauthorized access to sensitive healthcare data [5].

The research conducted examined a secure framework for the protection of healthcare data stored in cloud-based systems through the integration of encryption techniques with access control methods [7]. The proposed multilayered architecture utilizes a mix of encryption algorithms, role-based access control polices, and identity management systems to create an end to end secure environment for protecting confidential healthcare records [18].

The results of a prototype implementation demonstrated the ability to integrate an authentication, authorization, and activity logging process in order to avoid any unauthorized access to patient records [17]. The results also supported the conclusion that integrating structured access control policies with encryption is an effective means to secure healthcare information in a cloud infrastructure [21].

Future opportunities for research may include the evaluation of advanced security technologies (ex. blockchain-based identification management, homomorphic encryption, artificial intelligence-based intrusion detection systems, etc.) that would further enhance the overall security of cloud-based healthcare systems [27].

➢ *Funding*

The authors received no financial support for the research, authorship, and/or publication of this article.

➢ *Ethics and Consent to Participate*

- Not applicable.

REFERENCES

[1]. S. Dorairaj and P. Ramasamy, “Privacy-preserving healthcare data storage in cloud computing environments,” IEEE International Conference on Cloud Computing, 2020.
[2]. P. Khatiwada, H. Bhusal, A. Chatterjee, and M. W. Gerdess, “A proposed access control-based privacy preservation model to share healthcare data in cloud,” arXiv, 2020.
[3]. D. Singh and P. Kaur, “Secure data sharing in healthcare cloud using hybrid encryption techniques,” International Journal of Computer Applications, 2021.
[4]. V. Sharma and R. Gupta, “A secure framework for privacy preservation in cloud-based healthcare systems,” Journal of Information Security and Applications, 2021.
[5]. M. Mehrtak et al., “Security challenges and solutions in healthcare cloud computing environments,” Journal of Medical Internet Research, 2021.
[6]. M. Penelova, “Access control models and their applications in information systems,” Cybernetics and Information Technologies, 2021.
[7]. Z. Man, J. Li, X. Di, R. Zhang, X. Li, and X. Sun, “Research on cloud data encryption algorithm based on neural networks,” Information Sciences, 2022.
[8]. S. Nanda and R. Mishra, “Secure cloud data sharing using attribute-based access control,” Future Generation Computer Systems, 2022.
[9]. J. Alonso et al., “Understanding the challenges and architectural models of multi-cloud applications,” Journal of Cloud Computing, 2023.
[10]. D. Shivaramakrishna and M. Nagaratna, “A hybrid cryptographic framework for secure cloud storage using AES-OTP and RSA,” Alexandria Engineering Journal, 2023.
[11]. H. Huang, “Research on the application of data encryption technology in computer network communication security,” Applied Science and Innovative Research, 2024.
[12]. V. Rivaldi, N. H. Johari, R. Setiawan, and R. Y. Rumagit, “Comparative simulation of homomorphic encryption techniques in edge-cloud computing,” Procedia Computer Science, 2024.
[13]. A. Sapkal, L. Heisnam, and S. Kusi, “Evolution of cloud computing technologies and adoption trends,” IRJET, 2024.
[14]. G. Kapil, N. Kumar, and A. Mourya, “Attribute-based encryption models for healthcare big data protection,” IEEE Access, 2024.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar2029

[15]. R. Basani and P. Ganesan, "Secure healthcare data processing using AES encryption and cloud segregation," International Journal of Engineering and Management, 2024.
[16]. A. Zhao, "Application of data encryption technology in cloud computing environments," International Conference on Computing and Data Science Proceedings, 2025.
[17]. P. Jain, "Identity and access management in the cloud," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2025.
[18]. A. K. Akuthota, "Role-based access control in modern cloud security governance," International Journal of Scientific Research in Computer Science and Engineering, 2025.
[19]. P. Selvi et al., "Hybrid ECC-AES encryption framework for secure healthcare cloud applications," Scientific Reports, 2025.
[20]. G. Kapil, N. Kumar, A. Mourya, and V. Kumar, "Securing big healthcare data using attribute-based encryption in cloud environments," The Journal of Supercomputing, 2025.
[21]. S. Kumar et al., "Efficient access request management for healthcare data in cloud computing systems," Expert Systems with Applications, 2025.
[22]. R. Ojino, "Secure healthcare data management using zero trust architecture in cloud storage," International Journal of Advanced Research in Computer Science, 2025.
[23]. D. Rose, "Attribute dependent multi-factor authentication for secure cloud data access," Australian Computer Journal, 2025.
[24]. U. R. Saxena, "Reinforced reliable cloud computing through identity-based encryption and homomorphic cryptography," Computers, 2025.
[25]. A. Amanna and I. Shinde, "Securing generative AI in healthcare using zero-trust cloud architecture," arXiv, 2025.
[26]. H. X. Son et al., "SLIE: A secure lightweight identity-based encryption scheme for healthcare IoT services," arXiv, 2025.
[27]. M. N. Alruwaill, S. P. Mohanty, and E. Kougianos, "hChain 4.0: Secure blockchain framework for electronic health records," arXiv, 2025.
[28]. V. Gollapalli and A. Kurunthachalam, "Secure healthcare data storage and access control using AES and ECC encryption," Journal of Cloud Security, 2025.
[29]. S. Ali et al., "Security and privacy challenges in multi-cloud computing environments," Computers & Security, 2025.
[30]. S. Dorairaj and P. Ramasamy, "Privacy-preserving healthcare data sharing in distributed cloud systems," IEEE Cloud Computing, 2025.