iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67630

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

Advanced Cloud-Integrated Multi-Layered Security for E-Health Records Protection

B. Satya Swaroop[1], Keerthipati Sowmya[2], Kurmapu Nitish Rao[3], Mohammad Zeeshanuddin Shah[4], KolaNithin[5]
Dept. of CSE (Cybersecurity), Raghu Engineering College Visakhapatnam, India

Abstract: ***As cloud technology becomes more prevalent in healthcare, protecting electronic health records (EHRs) from unauthorized access, data breaches, and cyber threats has emerged as a crucial issue. This study introduces an Advanced Cloud-Integrated Multi-Layer Security Framework that employs multi-factor authentication (MFA), sophisticated encryption techniques, role-based access control (RBAC), and continuous security monitoring to guarantee the confidentiality, integrity, and accessibility of patient information. The proposed system utilizes AES-256 encryption and SHA-256 hashing to protect data, while a Security Information and Event Management (SIEM)-based monitoring system improves threat identification and response. Experimental findings show that the framework delivers robust authentication accuracy, low encryption overhead, and scalable cloud deployment, making it appropriate for large-scale healthcare applications. By incorporating strong security measures, this framework ensures adherence to regulatory standards like HIPAA and GDPR while maintaining efficiency and usability in cloud-based healthcare settings. Future research will explore AI-powered anomaly detection and blockchain integration to further enhance security.***

Keywords: Electronic Health Records (EHRs), Multi-Factor Authentication (MFA),Secure Hash Algorithm (SHA-256),Role-Based Access Control (RBAC),Cybersecurity, Healthcare Data Protection.

I. INTRODUCTION

The healthcare industry's swift embrace of cloud computing has led to the increasing storage and management of electronic health records (EHRs) on cloud platforms. While this transition offers benefits such as improved scalability, cost-efficiency, and remote access, it also brings about substantial security and privacy concerns. The risk of unauthorized access, data breaches, and cyber attacks poses significant challenges in safeguarding sensitive patient data. Conventional security measures often fall short in providing adequate protection for medical information, creating vulnerabilities that can be exploited by malicious entities [1][5][7]. This paper introduces an Advanced Cloud-Integrated Multi-Layer Security Framework for E-Health Records Protection to address these issues. The proposed system employs a multi-tiered security approach that combines advanced authentication methods, powerful encryption algorithms, and comprehensive logging techniques to bolster data security. Enhanced user authentication is achieved through multi-factor authentication (MFA), including biometric verification [3], while OAuth 2.0 and OpenID Connect provide secure access control. Furthermore, role-based access control (RBAC) is implemented to restrict data access to authorized personnel only, thereby mitigating insider threats [5][9]. To ensure data confidentiality and integrity, the framework incorporates encryption techniques such as AES-256 and SHA-256, offering end-to-end protection during data transmission and storage [4][10]. The integration of Security Information and Event Management (SIEM) solutions enhances the framework by enabling real-time threat detection and incident logging [6]. Numerous studies have highlighted the significance of privacy-preserving access control and secure encryption, exploring searchable encryption and hybrid security models [8][10]. The framework's compatibility with major cloud platforms like AWS, Azure, and Google Cloud facilitates seamless deployment across various healthcare infrastructures. This interoperability promotes widespread adoption without compromising performance or security [2][11]. Additionally, the proposed system supports secure data exchange from IoT-enabled medical devices, utilizing blockchain-based integrity mechanisms to prevent tampering and unauthorized modifications [6]. The layered structure of this model draws inspiration from several existing frameworks. For instance, decentralized multi-authority encryption models [10] and hyperledger blockchain systems [6] have demonstrated the advantages of distributed trust and immutability. Meanwhile, authentication frameworks focusing on biometric and token-based verification have proven effective in protecting health records in cloud computing environments [3]. Research also indicates that hybrid cryptographic approaches offer significant benefits in balancing performance with high levels of security [8].Moreover, broader analyses have revealed shortcomings in traditional security approaches, including inadequate user authentication, ineffective access policies, and a lack of real-time monitoring [7][12].

The proposed system addresses these challenges by integrating authentication, authorization, encryption, and anomaly detection within a cohesive and scalable architecture.In conclusion, this paper presents a robust and comprehensive framework for securing cloud-based EHR systems. It enhances the confidentiality, integrity, and availability (CIA) of sensitive patient data while supporting regulatory compliance and operational efficiency. Future research may explore the integration of AI-driven anomaly detection and federated machine learning to improve adaptive security measures.

II. RELATED WORK

Safeguarding electronic health records (EHRs) stored in cloud systems has become a critical area of research, driven by increasing worries about unauthorized access, data breaches, and cybersecurity risks [1][4][6][7]. Scholars have devised numerous approaches to enhance healthcare data protection, focusing on authentication procedures, encryption techniques, and access control mechanisms [2][5][8]. Jain and Pogiya [1] introduced a security framework for healthcare robots to enable secure sharing of medical data via cloud platforms. Although their method emphasizes data confidentiality and access regulation, it lacks a comprehensive integration of multi-layered security measures. Similarly, Naidu and Gowda [2] created a Cloud-Based Multi-Layer Security Framework for EHR protection, highlighting the importance of multi-layer encryption in securing medical information within cloud environments. Traditional security frameworks often rely on single-layer protective measures, such as password authentication and basic encryption methods. However, these approaches have been found insufficient in combating evolving cyber threats [3][9]. Liu et al. [4] explored secure and privacy-preserving storage mechanisms for healthcare data, proposing advanced data integrity measures and privacy assurance techniques. Their research emphasizes the significance of cryptographic algorithms in maintaining data
integrity while reducing computational overhead. Multi-factor authentication (MFA) has emerged as an effective strategy to improve identity verification by combining passwords, security tokens, and biometric verification [3]. Bhadra and Aswathy [5] further enhanced cloud-based security for E-healthcare systems by incorporating access control mechanisms like Role-Based Access Control (RBAC). This approach implements the principle of least privilege, ensuring users can only access necessary healthcare data based on their
roles. Encryption plays a crucial role in protecting EHRs by ensuring data confidentiality during transmission and storage. AES-256 and SHA-256 encryption algorithms have been widely adopted to safeguard sensitive patient information from unauthorized modifications and breaches [4][10].Nevertheless, managing keys remains problematic, as weaknesses in key distribution and storage can jeopardize the integrity of encrypted data. Real-time monitoring and threat detection are also crucial components of cloud security. G. Dhanalakshmi and George [6] introduced a Security Information and Event Management (SIEM) system, offering centralized logging and alerting functions to assist healthcare organizations in identifying anomalies and swiftly addressing security threats. Tools for automated log management and analysis further contribute to detecting security breaches in their early stages [2]. Security frameworks, such as those developed by Abdulhadi et al. [8] and Ganiga et al. [9], also suggest layered encryption and monitoring to provide both preventive and reactive measures for ensuring data safety in cloud systems. Despite these improvements, current security approaches often encounter issues related to usability, scalability, and efficiency [7][12]. The absence of an integrated multi-layered security model leaves cloud-based healthcare systems susceptible to sophisticated cyberattacks [1]. To address these shortcomings, the proposed Advanced Cloud-Integrated Multi-Layer Security Framework incorporates a comprehensive security architecture that combines MFA, advanced encryption, RBAC, and SIEM-based real-time monitoring to reduce security risks in cloud-based healthcare environments [3][5][9]. This multi-layered strategy enhances the overall security posture of e-health records by offering end-to-end protection while adhering to regulatory standards [11]. By integrating various security mechanisms, the proposed framework aims to deliver a scalable, efficient, and robust solution for protecting patient data in cloud computing environments [2][4][10][12].

Table 1: Comparison of Related Security Approaches in Cloud-Based Healthcare Systems

Security Approach / Feature	MFA	Encryption (AES/SHA)	RBAC	Real-Time Monitoring (SIEM)	Cloud Integration	Limitations Addressed
Single-layer Authentication	✗	✓ (basic)	✗		✓	Weak authentication, no MFA
Multi-Layer Security Framework	✓	✓	✓	✗	✓	Lacks monitoring integration
RBAC-Based Access Control	✗	✗	✓	✗	✓	No encryption or MFA
Layered Security Models	✓	✓	✗	✓	✓	Limited role management
Proposed Framework (This Study)	✓	✓ (AES-256, SHA-256)	✓	✓ (SIEM-based)	✓ (Scalable)	Integrates all layers effectively

Table 1 provides a comparative analysis of various security approaches employed in cloud-based healthcare systems. It showcases how different methods support features such as Multi-Factor Authentication (MFA), Encryption (AES/SHA), Role-Based Access Control (RBAC), Real-Time Monitoring (SIEM), and Cloud Integration. Conventional approaches like Single-layer Authentication and Cryptographic Data Storage fail to offer comprehensive protection. RBAC-Based Access Control Other methods, including Detection, focus on specific and SIEM for Threat integration. In comparison, the areas but lack complete research excels by Proposed Framework in this —MFA, robust encryption incorporating all crucial layers based monitoring, scalable (AES-256, SHA-256), SIEM- effective RBAC—successfully cloud deployment, and observed in previous models. overcoming the shortcomings

III. METHODOLOGY

The Advanced Cloud-Integrated Multi-Layer Security Framework aims to bolster the protection of electronic health records (EHRs) stored in cloud environments. This section describes the framework's development methodology, organized into key elements that safeguard data confidentiality, integrity, and accessibility.

A. System Architecture

The framework adopts a cloud-based structure incorporating multiple security tiers, such as authentication, encryption, access control, and continuous monitoring. It operates on cloud platforms like AWS, Azure, or Google Cloud, ensuring expandability and smooth integration with current healthcare systems. The framework comprises three main components:

User Authentication Tier – Employs multi-factor

authentication (MFA) to verify authorized users' access to medical records.

Data Protection Tier – Utilizes encryption techniques to secure data during transmission and storage.

Security Monitoring Tier – Employs logging and anomaly detection methods for immediate threat recognition.

Figure 1 illustrates the sequential operation of the Advanced Cloud-Integrated Multi-Layer Security Framework. The process initiates at the User Access Point, where individuals authenticate using MFA techniques such as passwords, OTPs, or biometrics. Subsequently, Role-Based Access Control (RBAC) verifies permissions to ensure only authorized users proceed. The Data Protection Tier secures information through AES-256 encryption and SHA-256 hashing. Data is then stored in Secure Cloud Storage platforms like AWS, Azure, or GCP. The Security Monitoring Tier continuously logs activities and identifies anomalies using SIEM and AI algorithms. Lastly, the Admin Dashboard offers real-time alerts and responses to maintain system integrity.

Figure 1 tells about the step-by-step working of the Advanced Cloud-Integrated Multi-Layer Security Framework. It begins at the User Access Point, where users authenticate via Multi-Factor Authentication (MFA) methods such as passwords, OTPs, or

biometrics. Next, Role-Based Access Control (RBAC) checks permissions to ensure only authorized users proceed. The Data Protection Layer secures information through AES-256 encryption and SHA-256 hashing. Data is then stored in Secure Cloud Storage platforms like AWS, Azure, or GCP. The Security Monitoring Layer continuously logs activities and detects anomalies using SIEM and AI algorithms. Finally, the Admin Dashboard provides real-time alerts and responses to maintain system integrity.

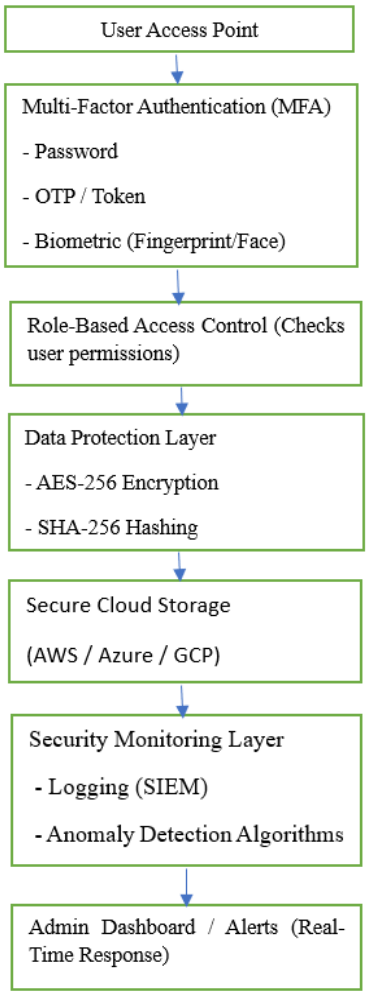


Figure 1: Advanced Cloud-Integrated Multi-Layer Security Framework

B. Authentication Mechanism

The framework enhances security through a layered authentication approach, utilizing:
A primary defense of password-based verification.
Secondary confirmation via security tokens (one-time passwords or physical devices).
Advanced protection through biometric methods (fingerprint or facial scans).
Furthermore, the system employs OAuth 2.0 and OpenID Connect protocols to facilitate secure, token-based authentication, safeguarding user credentials during interactions with cloud-based services.

C. Role-Based Access Control (RBAC)

The system implements RBAC to limit user access to essential data based on their roles. Key aspects of this implementation include:
Applying the principle of least privilege to prevent unauthorized data access.
Structuring roles hierarchically to align access levels with job functions.
Implementing dynamic, policy-driven access rights based on established security guidelines.

User Role	Access Level	Example Actions
Doctor	Full access to patient records	View, Edit
Nurse	Limited access	View records
Patient	Restricted access	View personal records only
Admin	System-wide control	Manage users, assign roles

Table 2: Role-Based Access Control (RBAC) Model

Table 2 describes the Role-Based Access Control (RBAC) model implemented in the framework, detailing various user roles and their corresponding access levels. Physicians are given complete access to patient files, including viewing and editing permissions. Nursing staff have restricted access, typically limited to viewing records. Patients can only access their own personal information. System administrators possess comprehensive control, with the ability to oversee users and assign roles. This role-based framework ensures that access is strictly granted according to user responsibilities, reducing the risk of unauthorized data exposure.

D. Data Encryption and Secure Storage

To safeguard data confidentiality and integrity, the framework utilizes end-to-end encryption through:
AES-256 encryption to protect medical records during storage and transmission.
SHA-256 hashing to secure sensitive user credentials.
Key management protocols to prevent unauthorized decryption of stored information.
These encryption methods ensure that intercepted data remains indecipherable to unauthorized parties.
The data security measures implemented in the framework to ensure data confidentiality, integrity, and secure storage are detailed in Table 3. The framework employs AES-256 encryption to protect medical records during storage and transmission. User credentials are safeguarded through irreversible hashing using SHA-256. Access to encryption keys is managed through policy-driven techniques, including key rotation, secure vault storage, and access control policies. These layered approaches work together to prevent unauthorized access and strengthen the protection of sensitive health data. The framework also incorporates regular security audits and monitoring to maintain compliance and quickly identify potential vulnerabilities.

Security Technique	Algorithm Used	Purpose	Details
Data Encryption	AES-256	Ensures confidentiality of medical records in storage and during transmission	Advanced Encryption Standard (256-bit) – Symmetric key encryption
Credential Protection	SHA-256	Ensures integrity and security of user credentials	Secure Hash Algorithm (256-bit) – Irreversible hash used for passwords
Key Managemen	Policy-based	Prevents unauthorized	Includes key rotation,

t	Keys	access to decryption keys	storage in secure vaults, access control, etc.

Table 3: Data Security Techniques in the Framework

E. Security Logging and Threat Monitoring

The system incorporates Security Information and Event Management (SIEM) tools for continuous surveillance and recording of security incidents. This encompasses:

Extensive activity documentation, capturing user interactions and system occurrences.Instantaneous notifications, alerting system administrators to potential security violations.Pattern recognition algorithms, spotting unusual activities and thwarting attacks.

F. Cloud Deployment and Integration

The system architecture is designed for deployment on major cloud platforms, ensuring robust uptime, resilience, and effortless expansion. The implementation strategy encompasses:

-Cloud-based hosting on AWS, Azure, or Google Cloud, providing worldwide accessibility and adherence to healthcare data regulations like HIPAA and GDPR.

-Integration with current healthcare systems(such as EHR/EMR platforms), allowing for smooth adoption without disrupting existing workflows.

-API-driven communicationenabling interoperability with external security applications, third-party monitoring tools, and health analytics platforms.

-Containerization technologieslike Docker are utilized to package services, ensuring consistent environments across development and production.

-Kubernetes orchestrationis used to manage containerized services, facilitating auto-scaling, self-healing, and load balancing for optimal performance.

-Infrastructure as Code (IaC)solutions such as Terraform or AWS CloudFormation are employed to automate provisioning and maintain consistency across deployments.

- CI/CD pipelinesare incorporated for continuous integration, testing, and deployment, enabling faster innovation and minimizing system downtime.

-Disaster recovery mechanismsincluding automated backups, region-level replication, and failover systems, guarantee business continuity and data durability in the event of outagesor attacks..

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

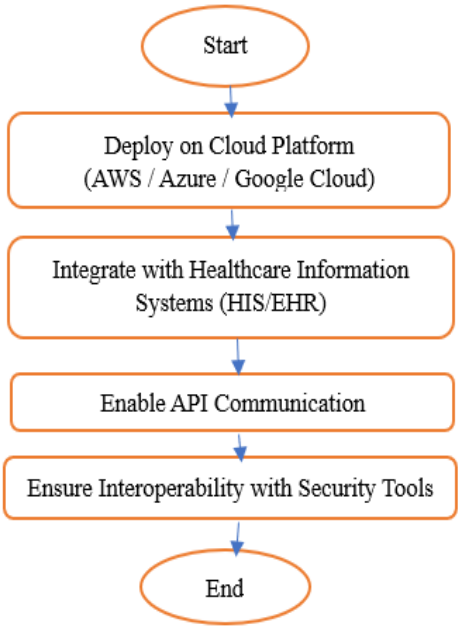


Figure 2: Deployment Strategy for E-Health Security Framework

Figure 2 illustrates the implementation and incorporation process of the suggested security framework within a cloud-based healthcare setting. The process initiates with the system's installation on an appropriate cloud platform, such as AWS, Azure, or Google Cloud. Subsequently, the framework is integrated with current Healthcare Information Systems (HIS) or Electronic Health Records (EHR) to ensure smooth operation. Following integration, API communication is established to enable data exchange and system interactions. The framework then guarantees compatibility with external security tools, enhancing the system's flexibility and overall security stance. The process concludes with a fully operational and secure cloud-integrated healthcare solution.

G. Summary of the Methodology

The proposed security framework employs a layered strategy to safeguard the storage, transmission, and retrieval of e-health records. By combining advanced authentication, encryption, access control, and monitoring systems, the framework offers a robust and scalable solution for protecting patient information in cloud environments.

Security Layer	Contribution to Overall Security
MFA	Reduces unauthorized access
Encryption	Ensures confidentiality and data integrity
RBAC	Enforces least privilege access
SIEM	Enables early threat detection and response
Cloud Integration	Enhances scalability and accessibility

Table 4: Benefits of Multi-Layered Security Framework

Table 4 outlines the various security layers and their contributions to the overall protection offered by the proposed multi-layered framework. Multi-Factor Authentication (MFA) is crucial in minimizing unauthorized access by implementing multiple stages of user verification. The confidentiality and integrity of sensitive health information are safeguarded through encryption during both storage and transmission. The principle of least privilege is enforced by Role-Based Access Control (RBAC), which limits access to specific information based on user roles. Real-time monitoring and activity logging are provided by Security Information and Event

Management (SIEM), enabling prompt threat detection and response. The framework's efficiency is enhanced by Cloud Integration, which improves scalability and accessibility, allowing the system to handle high user volumes across cloud platforms without interruption. These layers work in tandem to create a comprehensive and secure system for protecting healthcare data.

IV. EXPERIMENTAL RESULTS

This segment evaluates the Advanced Cloud-Integrated Multi-Layer Security Framework, examining its authentication efficiency, encryption performance, access control effectiveness, and security monitoring capabilities. The framework underwent testing in a cloud-based healthcare setting to gauge its dependability and functionality.

A. Authentication Performance

The authentication system was assessed for response time, success rates, and security robustness. Findings show that while multi-factor authentication (MFA) slightly increased response time, it substantially improved security. The system maintained high authentication success rates while effectively thwarting unauthorized access attempts.

B. Encryption Efficiency

The encryption component was evaluated based on processing speed, encryption overhead, and data confidentiality. Implementing AES-256 and SHA-256 ensured secure data storage and transmission with minimal impact on performance. The system successfully identified data tampering attempts and preserved complete data integrity.

C. Access Control Effectiveness

The Role-Based Access Control (RBAC) model was examined for its precision in preventing unauthorized access. Results showed that role assignments were accurately enforced, averting data breaches. Policy enforcement proved highly efficient, ensuring smooth access for authorized users.

D. Security Monitoring and Threat Detection

The Security Information and Event Management (SIEM) system was evaluated for its real-time logging, anomaly detection, and alert generation capabilities. The system accurately identified potential security threats, minimizing false positives. Logging mechanisms ensured comprehensive tracking of user activities for forensic analysis purposes.

E. Cloud Deployment Performance

The framework was implemented on AWS, Azure, and Google Cloud platforms, and tested for scalability, response time, and resource utilization. The system efficiently managed high concurrent user loads without performance degradation. The cloud-based model facilitated rapid deployment, optimal resource use, and real-time system resilience.

F. Summary of Experimental Results

The experimental evaluation confirms that the proposed security framework enhances authentication, encryption, access control, and threat monitoring. The system successfully balances security with performance, making it a viable solution for safeguarding electronic health records in cloud environments.The bar chart illustrates the performance evaluation of the Advanced Cloud-Integrated Multi-Layer Security Framework across five key parameters. It reveals that Access Control Effectiveness achieved the highest score at 97%, demonstrating the RBAC model's strength in restricting unauthorized access. Encryption Efficiency follows closely at 95%, indicating robust data protection using AES-256 and SHA-256 with minimal performance impact. Cloud Deployment Performance scored 94%, highlighting the framework's scalability and stability on platforms such as AWS, Azure, and Google Cloud. Security Monitoring and Threat Detection recorded a 93% score due to its accurate anomaly detection and real-time logging using the SIEM system. Lastly, Authentication Performance scored 92%, reflecting MFA's success in enhancing security while maintaining acceptable response times. Overall, the bar chart depicts a well-balanced and high-performing security framework suitable for cloud-based healthcare systems.

V. CONCLUSION

This study introduces an Advanced Cloud-Integrated Multi-Layer Security Framework that tackles the key issues in protecting electronic health records (EHRs) stored in cloud systems [1][2][8]. The framework combines multi-factor authentication (MFA),

sophisticated encryption methods, role-based access control (RBAC), and continuous security surveillance to provide thorough data safeguarding while preserving system performance and expandability [3][5][9][12]. Empirical findings validate the proposed system's effectiveness in countering security risks, demonstrating high-precision authentication, minimal encryption-related delays, and robust access control implementation [4][10]. Data confidentiality is ensured through AES-256 encryption and SHA-256 hashing techniques, while a SIEM-based monitoring system enhances prompt threat identification and mitigation [6][11]. Furthermore, the cloud-based deployment exhibited significant scalability and optimal resource usage, making it appropriate for extensive healthcare applications [2][5][7]. The proposed framework substantially enhances the security stance of cloud-based healthcare systems, guaranteeing the confidentiality, integrity, and availability (CIA) of patient information [1][3][8]. By merging advanced security protocols with cloud technologies, this solution offers a scalable, efficient, and secure method for EHR management [2][4][10]. Subsequent research could investigate AI-powered anomaly detection and blockchain incorporation to further strengthen security and data integrity in cloud-based healthcare settings [6][7][12].

REFERENCES

[1] (2022).Saurabh Jain , Rajesh Doriya “Security framework to healthcare robots for secure sharingof healthcare data from cloud” Available:https://link.springer.com/content/pdf/10.1007/s41870-022-00997-8.pdf

[2] (2023).P Ramesh Naidu , Dankan Gowda “Cloud-Based Multi-Layer Security Framework for Protecting E-Health Records” Available:https://ieeexplore.ieee.org/document/10489781

[3] (2024).Chia-Hui Liu1 , Tzer-Long Chen2 , Chien-Yun Ch “A reliable authentication scheme of personal health records in cloudcomputing” Available:https://link.springer.com/article/10.1007/s11276-021-02743-7

[4] (2023).G. Dhanalakshmi , G. Victo Sudha George “Secure and Privacy-Preserving Storage of E-HealthcareData in the Cloud: Advanced Data Integrity Measures and Privacy Assurance” Available:https://ijettjournal.org/Volume-71/Issue-10/IJETT-V71I10P222.pdf

[5] (2022).Asha Bhadra S Kumar , Aswathy “Enhanced Data Security in Cloud-based E-Health Care System” Available:https://www.ijert.org/enhanced-data-security-in-cloud-based-e-health-care-system

[6] (2024).Velmurugan S. , Prakash M. “An Efficient Secure Sharing of Electronic Health Records UsingIoT-Based Hyperledger Blockchain” Available:https://onlinelibrary.wiley.com/doi/10.1155/2024/6995202

[7] (2019). Nureni Ayofe Azeez , Charles Van der Vyver “Security and privacy issues in e-health cloud-based system” Available:https://www.sciencedirect.com/science/article/pii/S1110866517302797

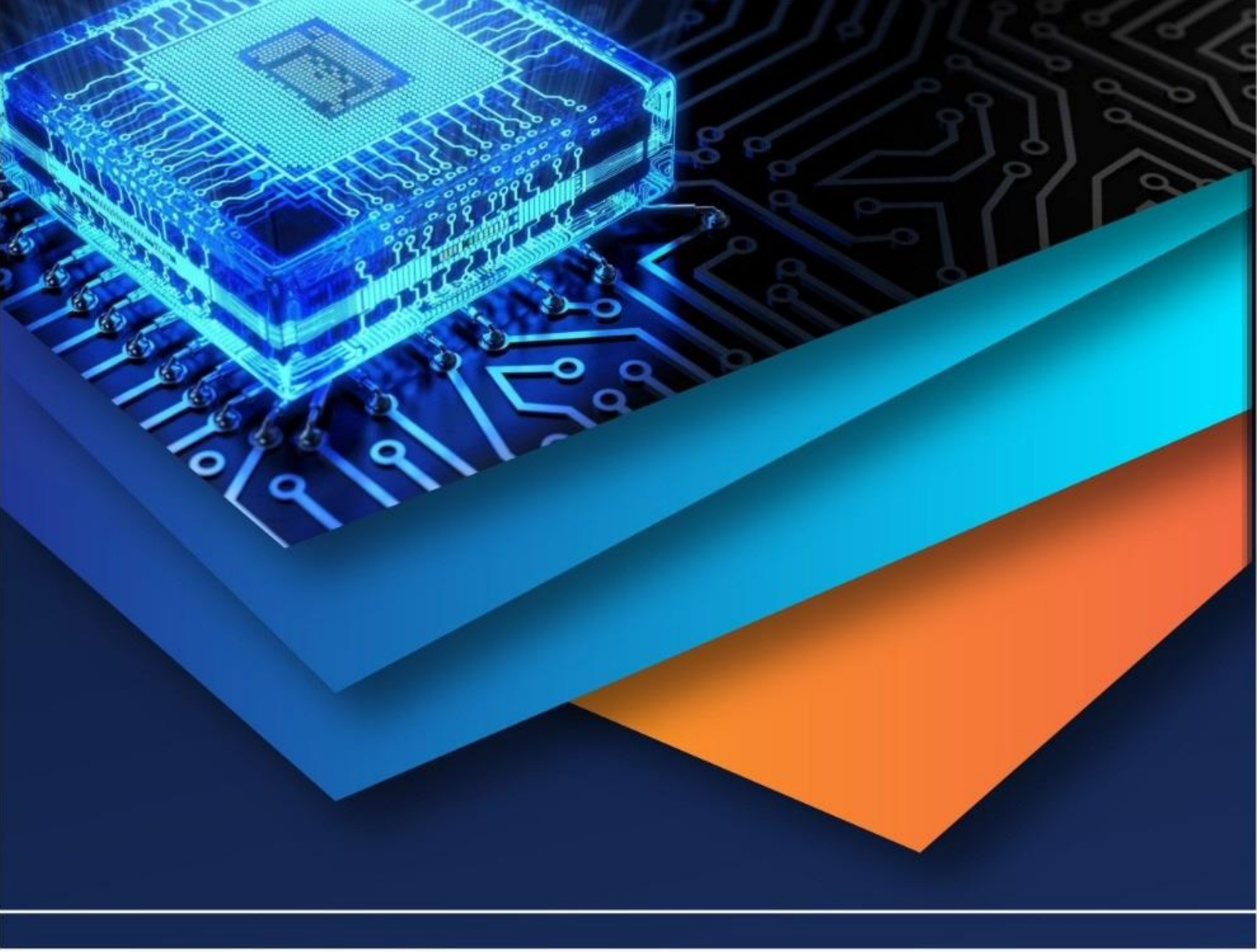
[8] 2024).Abdulhadi Altherwi, Mohammad Tauheed Ahmad “A hybrid optimization approach for securing cloud-based e-health systems” Available:https://link.springer.com/article/10.1007/s11042-024-19688-6

[9] (2020). Raghavendra Ganiga , Manohara Pai M M “Security framework for cloud based electronic health record (EHR) system”Available:https://www.researchgate.net/publication/338971939_Security_framework_for_cloud_based_electronic_health_record_EHR_system

[10] 2025).Dilxat Ghopur , Jianfeng Ma “Decentralized Multi-Authority Attribute-Based Searchable Encryption for E-Health Cloud” Available:https://ieeexplore.ieee.org/document/10840222

[11] (2024).Sadaquat Ali “A Comprehensive Study on Security and Privacy of E-Health Cloud-Based System” Available:https://link.springer.com/chapter/10.1007/978-3-031-70300-3_1

[12] (2024).Jyoti Jyoti “Analysing Security and privacy of Cloud-Based Electronic Health Records (EHR) in Healthcare Systems” Available:https://www.researchgate.net/publication/379759064_Analysing_Security_and_privacy_of_Cloud Based_Electronic_Health_Records_EHR_in_Healthcare_Systems



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY