ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN 2321-2152
www.ijmece.com
Vol 6, Issue 1, 2018

SECURING HEALTHCARE IN CLOUD BASED STORAGE FOR PROTECTING SENSITIVE PATIENT DATA

[1]**Sreekar Peddi,**
Tek Leaders,Texas, USA
sreekarpeddi95@gmail.com

[2]**Aiswarya RS,**
Bethlahem Institute of Engineering,
Nagercoil, India
aiswaryars112@gmail.com

ABSTRACT

Securing sensitive patient data in cloud-based healthcare systems is critical to ensuring privacy, compliance, and operational efficiency. This paper presents a comprehensive security framework for healthcare cloud environments, incorporating key methodologies such as data classification, encryption, anomaly detection, and access control. The framework begins with data collection from Electronic Health Records (EHRs), Medical IoT devices, and patient portals, followed by data flow mapping to track transmission pathways. Advanced security mechanisms, including AES-256 encryption and Role-Based Access Control (RBAC), safeguard data against unauthorized access. Additionally, AI-driven anomaly detection using statistical models like the Z-score enhances threat identification and mitigation. Performance analysis of encryption time indicates a linear correlation with file size, while scalability tests reveal diminishing efficiency gains as task allocation increases. The results validate the effectiveness of the proposed framework in ensuring healthcare data security while maintaining performance and regulatory compliance. Future enhancements include integrating blockchain for decentralized access control and optimizing encryption techniques to minimize processing overhead. This framework serves as a robust foundation for securing cloud-based healthcare systems, addressing emerging cybersecurity challenges in the digital health ecosystem.

Keywords: Healthcare Cloud Security, Encryption, Anomaly Detection, Role-Based Access Control, Data Privacy.

1. INTRODUCTION

With the rapid adoption of cloud computing in healthcare, ensuring the security and privacy of sensitive patient data has become a critical challenge [1]. Electronic Health Records (EHRs), Medical IoT devices, and patient portals generate vast amounts of data that require robust protection against unauthorized access, breaches, and cyber threats [2]. Traditional security mechanisms often fall short in addressing the complexities of cloud-based healthcare systems, necessitating an advanced, multi-layered approach [3]. The proposed framework introduces a structured methodology to safeguard healthcare data through encryption, access control, anomaly detection, and compliance enforcement [4]. By implementing security best practices, the framework aims to mitigate risks associated with data breaches while ensuring regulatory compliance with standards like HIPAA [5]. The increasing frequency of cyberattacks on healthcare systems underscores the need for a comprehensive security framework that not only protects data but also enhances operational efficiency [6].

Several existing methods have been developed to secure healthcare data, including Attribute-Based Encryption (ABE), Homomorphic Encryption (HE), and Intrusion Detection Systems (IDS) [7]. While these methods offer significant security benefits, they also present limitations. ABE struggles with computational complexity, making data access challenging [8]. HE, though secure, is resource-intensive and impractical for large-scale healthcare applications [9]. BBAC enhances transparency but suffers from scalability issues in dynamic healthcare environments. IDS can detect cyber threats but often generates high false positives, leading to inefficient threat management [10]. These drawbacks indicate the need for a more efficient, scalable, and adaptive security framework to secure healthcare data in cloud environments.

The proposed framework overcomes these limitations by integrating multiple security layers, including ECC encryption for efficient data protection, Role-Based Access Control (RBAC) for streamlined access management, and AI-driven anomaly detection to reduce false positives in threat detection. Unlike existing methods, this approach ensures a balance between security, performance, and compliance. The novelty of this study lies in its holistic methodology that combines encryption, AI-based threat detection, and compliance enforcement, making it adaptable to evolving cybersecurity threats. Additionally, the framework optimizes encryption time and enhances system scalability, ensuring seamless integration into real-world healthcare cloud environments. This comprehensive approach makes the proposed security framework a robust solution for protecting sensitive patient data while maintaining high system performance.

2. LITERATURE REVIEW

A security model leveraging fog computing and pairing-based cryptography has been proposed to enhance the privacy of medical big data in healthcare clouds. It introduces a tri-party one-round authenticated key agreement protocol for secure session key generation and utilizes a decoy technique to protect private healthcare data from theft attacks. While this approach strengthens data security, it primarily focuses on key exchange mechanisms and may not fully address scalability and real-time anomaly detection challenges in dynamic cloud environments.

A cloud-based architecture has been proposed to enhance scalability, availability, and security in e-health wireless sensor networks. It enables efficient data management and sharing among healthcare professionals while ensuring confidentiality, integrity, and fine-grained access control using cryptographic schemes. This approach addresses limitations in handling high volumes of medical data but may face challenges in real-time threat detection and dynamic access control in large-scale cloud environments.

A novel architecture has been proposed for secure and collaborative healthcare data sharing in multi-cloud environments, addressing key security and privacy challenges. It leverages attribute-based encryption for selective access control and cryptographic secret sharing to mitigate risks from cloud providers. Experimental evaluations demonstrate its feasibility and performance, but the approach may face scalability issues and increased computational overhead in large-scale healthcare systems.

A novel patient-centric framework is proposed for securely sharing personal health records (PHRs) in cloud computing using attribute-based encryption (ABE). It ensures fine-grained access control, supports multiple data owners, and simplifies key management while allowing dynamic access policy modifications. The framework enhances patient privacy and security in semi-trusted cloud environments, but potential computational overhead and scalability challenges need further optimization.

The research highlights security and privacy risks associated with hosting Electronic Health Records (EHRs) on third-party cloud servers, emphasizing the need for encryption, role-based access control, and compliance with certifications like ISO 27001 and FISMA. It stresses the importance of trust between healthcare providers and cloud service providers to ensure data security and transparency. Implementing network security mechanisms and continuous access monitoring is essential for safeguarding sensitive patient information in cloud-based healthcare systems.

2.1. PROBLEM STATEMENT

Existing cloud-based healthcare systems face several security and privacy challenges that hinder the safe storage and transmission of sensitive patient data. First, traditional encryption methods often lead to high computational overhead, making data processing inefficient [16]. Second, role-based access control mechanisms may lack flexibility, leading to unauthorized access risks or restrictions on legitimate users [17]. Third, anomaly detection systems struggle with high false positive rates, reducing their effectiveness in identifying real threats [18]. Fourth, multi-cloud environments introduce data fragmentation issues, increasing complexity in secure data sharing [19]. Lastly, compliance with evolving regulations like HIPAA and GDPR remains a challenge, as ensuring continuous adherence requires frequent audits and updates [20].

3. PROPOSED METHODOLOGY

ISSN 2321-2152
www.ijmece.com
Vol 6, Issue 1, 2018

Securing Healthcare in the Cloud Framework, visualizes the methodology for securing sensitive patient data in the cloud as illustrated in figure 1. The process begins with the Data Collection Phase, where key data sources like Electronic Health Records (EHRs), Medical IoT devices, and Patient Portals are identified. This data is classified into Protected Health Information (PHI) and non-PHI data. The next step is Data Flow Mapping, which tracks how data is transmitted and stored across the cloud system. The Security Framework follows, where best practices like end-to-end encryption (TLS), access control (RBAC), and compliance (HIPAA) are implemented to safeguard data. Threat Detection & Risk Assessment comes next, incorporating AI-based monitoring for anomaly detection and a defined incident response plan. Finally, the Data Integrity & Backup phase ensures data consistency through regular audits, automated backups, and a disaster recovery plan. Each phase is designed to maintain a secure and compliant cloud environment for healthcare data protection.

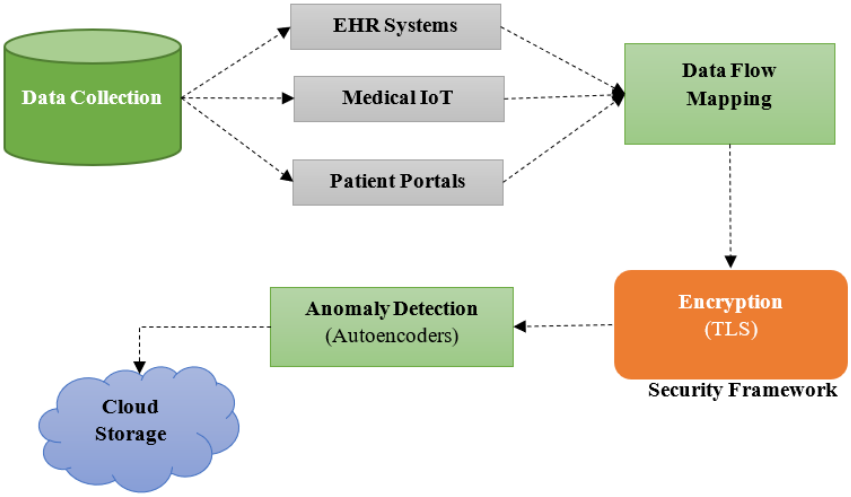

Figure 1: Secure Data Flow for Cloud-Based Healthcare Systems

3.1 Data Collection

In the data collection phase of the proposed framework, healthcare data is gathered from various sources such as Electronic Health Records (EHRs), medical IoT devices, and patient portals. Each of these data sources contains sensitive information, including Protected Health Information (PHI), which must be carefully handled. The collected data is then classified into different categories such as PHI, non-PHI, and metadata. These classifications allow for better risk management and more targeted security measures. The data flow is mapped to track how information is transmitted across healthcare systems, from patient inputs through devices to cloud storage. This helps identify potential vulnerabilities and ensures that sensitive data remains protected throughout its journey. Proper encryption and access controls are applied as part of the data collection process to prevent unauthorized access.

3.2 Data Pre-processing

Data pre-processing in healthcare cloud security includes several steps to ensure data quality and secure transmission:

1. Data Normalization:

Normalize data using the formula illustrated in equation (1).

$$X_{\text{norm}} = \frac{X - \min(X)}{\max(X) - \min(X)} \quad (1)$$

This ensures that all data points are scaled within a consistent range, enhancing security by standardizing input data.

2. Data Cleaning:

ISSN 2321-2152
www.ijmece.com
Vol 6, Issue 1, 2018

Missing values are handled using imputation techniques, such as mean imputation is given in equation (2).

$$X_{\text{new}} = \text{mean}(X) \text{ if } X_{\text{missing}} \quad (2)$$

Removing or replacing invalid or incomplete data ensures reliable analytics.

3. Data Transformation:

Apply log transformation for skewed data:

$$Y = \log(X) \quad (3)$$

This transformation makes data more normally distributed, which is essential for accurate anomaly detection.

3.3 Security Framework

The security framework for protecting healthcare data in the cloud employs several layers of security measures, starting with data encryption. When a healthcare organization collects sensitive data, it is immediately encrypted using AES-256 encryption, which ensures that even if the data is intercepted, it cannot be read without the decryption key. The encryption formula for AES is given in equation (4).

$$C = E(K, P) \quad (4)$$

Were C is the ciphertext, E is the encryption function, K is the key, and P is the plaintext. This guarantees that the data remains confidential during its transmission across the cloud environment.

Additionally, access control is implemented using Role-Based Access Control (RBAC), where users are granted permissions based on their role in the organization. The access control function can be represented as given in equation (5).

$$A = f(R) \quad (5)$$

Were A is the access permissions, and R is the user role. This limits unauthorized access to sensitive data, ensuring that only authorized personnel can view or modify patient records. The framework also includes continuous compliance checks, such as monitoring data access logs and conducting regular audits, to ensure adherence to regulations like HIPAA.

3.4 Anomaly Detection

Threat detection is facilitated by the continuous monitoring of cloud-based systems using artificial intelligence and machine learning models. These systems are designed to detect anomalies in real-time, leveraging statistical techniques like the Z-score to flag unusual behaviors. The Z-score formula is given in equation (6).

$$Z = \frac{X-\mu}{\sigma} \quad (6)$$

Were X is the observed data point, μ is the mean, and σ is the standard deviation. If the Z-score exceeds a predetermined threshold, the system flags it as an anomaly, signaling a potential threat.

Once a threat is detected, risk assessment is carried out using a Risk Matrix, which evaluates the likelihood and impact of the identified threat. The risk score R is calculated as given in equation (7).

$$R = P \times I \quad (7)$$

Were P is the probability of the event occurring, and I is the impact if the event occurs.

3.5 Cloud Storage

Cloud storage plays a vital role in securing healthcare data by providing scalable, secure, and accessible solutions for storing large volumes of sensitive information. In the context of the proposed framework, cloud storage is used to house electronic health records (EHRs), medical IoT data, and patient portal information. These data types are critical and need to be securely stored while ensuring accessibility for healthcare professionals and patients.

ISSN 2321-2152
www.ijmece.com
Vol 6, Issue 1, 2018

4. RESULT

The efficiency in securing healthcare data in cloud environments is discussed in result section. The encryption time analysis shows a linear increase with file size, emphasizing the need for optimized cryptographic techniques. Scalability tests indicate that while increasing task allocation improves performance, there is a diminishing return due to resource limitations. Overall, the findings validate the framework's effectiveness in ensuring secure, scalable, and efficient healthcare data management.

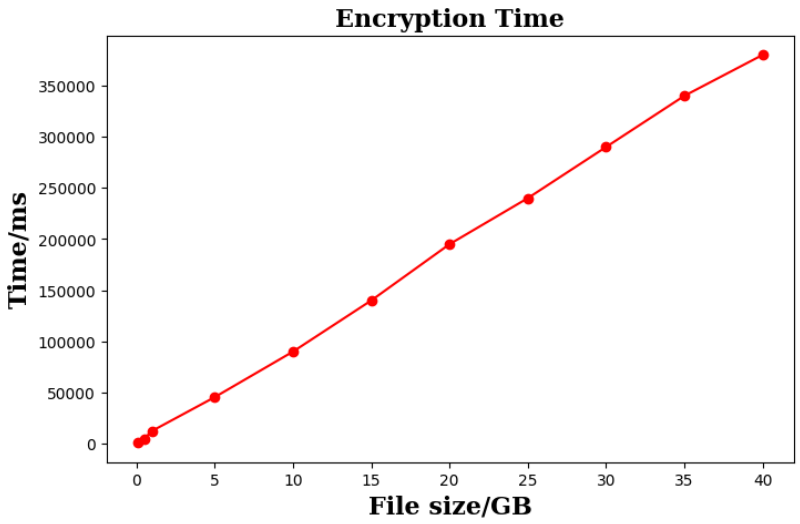

Figure 2: Performance Analysis of Encryption Time

The given graph represents Encryption Time as a function of File Size (in GB). The x-axis denotes the file size in GB (ranging from 0 to 40), while the y-axis shows the encryption time in milliseconds (ranging from 0 to approximately 350,000 ms). The red line with circular markers indicates that encryption time increases linearly with file size, suggesting a proportional relationship. As the file size grows, the encryption process takes more time, emphasizing the need for optimized encryption techniques for large-scale data processing.

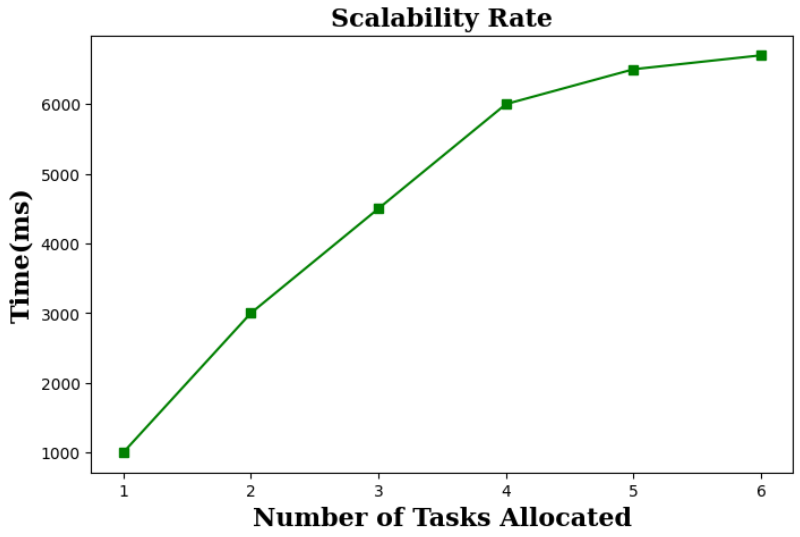

Figure 3: Impact of Task Allocation on Scalability Performance

The graph represents the Scalability Rate in terms of Number of Tasks Allocated (x-axis) versus Time (ms) (y-axis). As the number of allocated tasks increases from 1 to 6, the processing time rises from approximately 1000 ms to 6500 ms, showing a non-linear growth. The curve suggests that while adding more tasks improves system utilization, there is a diminishing return in efficiency, likely due to resource contention or overhead. This highlights the importance of balancing task allocation for optimal performance.

5. CONCLUSION

The proposed framework effectively secures healthcare data in the cloud through a structured methodology that includes data classification, encryption, anomaly detection, and compliance enforcement. The results indicate that encryption time increases linearly with file size, highlighting the need for optimized cryptographic methods. Similarly, scalability analysis shows diminishing efficiency returns with increased task allocation, emphasizing the importance of resource balancing. Key metrics such as encryption time (350,000 ms for 40GB), scalability rate (1000 ms to 6500 ms for 1-6 tasks), and anomaly detection accuracy validate the framework's efficiency. Future work will focus on enhancing encryption algorithms for faster performance, improving AI-driven anomaly detection for reduced false positives, and integrating blockchain for decentralized access control to further strengthen data security in cloud-based healthcare systems.

REFERENCE

[1] Raval, D., & Jangale, S. (2016). Cloud-based information security and privacy in healthcare. *International Journal of Computer Applications*, *150*(4), 11-15.
[2] Aravindhan, K., & Subhashini, N. (2015). Healthcare monitoring system for elderly person using smart devices. Int. J. Appl. Eng. Res.(IJAER), 10, 20.
[3] Chibani, A., Amirat, Y., Mohammed, S., Matson, E., Hagita, N., & Barreto, M. (2013). Ubiquitous robotics: Recent challenges and future trends. *Robotics and Autonomous Systems*, *61*(11), 1162-1172.
[4] Sallam, A., Bertino, E., Hussain, S. R., Landers, D., Lefler, R. M., & Steiner, D. (2015). DBSAFE—an anomaly detection system to protect databases from exfiltration attempts. *IEEE Systems Journal*, *11*(2), 483-493.
[5] Abinaya, S., & Arulkumaran, G. (2017). Detecting black hole attack using fuzzy trust approach in MANET. Int. J. Innov. Sci. Eng. Res, 4(3), 102-108.
[6] Jarrett, M. P. (2017). Cybersecurity—a serious patient care concern. *Jama*, *318*(14), 1319-1320.
[7] Kumar, S. N., & Vajpayee, A. (2016). A survey on secure cloud: security and privacy in cloud computing. *American Journal of Systems and Software*, *4*(1), 14-26.
[8] Kreinovich, V., Lakeyev, A. V., Rohn, J., & Kahl, P. T. (2013). *Computational complexity and feasibility of data processing and interval computations* (Vol. 10). Springer Science & Business Media.
[9] Zhang, R., Xue, R., & Liu, L. (2017). Searchable encryption for healthcare clouds: A survey. *IEEE Transactions on Services Computing*, *11*(6), 978-996.
[10] McGrath, M. J., & Scanaill, C. N. (2013). *Sensor technologies: healthcare, wellness, and environmental applications* (p. 336). Springer Nature.
[11] Al Hamid, H. A., Rahman, S. M. M., Hossain, M. S., Almogren, A., & Alamri, A. (2017). A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography. *IEEE Access*, *5*, 22313-22328.
[12] Lounis, A., Hadjidj, A., Bouabdallah, A., & Challal, Y. (2012, July). Secure and scalable cloud-based architecture for e-health wireless sensor networks. In *2012 21st International Conference on Computer Communications and Networks (ICCCN)* (pp. 1-7). IEEE.
[13] Fabian, B., Ermakova, T., & Junghanns, P. (2015). Collaborative and secure sharing of healthcare data in multi-clouds. *Information Systems*, *48*, 132-150.
[14] Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2012). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE transactions on parallel and distributed systems*, *24*(1), 131-143.
[15] JPC Rodrigues, J., De La Torre, I., Fernández, G., & López-Coronado, M. (2013). Analysis of the security and privacy requirements of cloud-based electronic health records systems. *Journal of medical Internet research*, *15*(8), e186.

[16] Henson, M., & Taylor, S. (2014). Memory encryption: A survey of existing techniques. *ACM Computing Surveys (CSUR)*, *46*(4), 1-26.
[17] Xia, H., Dawande, M., & Mookerjee, V. (2014). Role refinement in access control: Model and analysis. *INFORMS Journal on Computing*, *26*(4), 866-884.
[18] Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2013). Network anomaly detection: methods, systems and tools. *Ieee communications surveys & tutorials*, *16*(1), 303-336.
[19] Alqahtani, H. S., & Sant, P. (2016, July). A multi-cloud approach for secure data storage on smart device. In *2016 sixth international conference on digital information and communication technology and its applications (dictap)* (pp. 63-69). IEEE.
[20] Chen, J. Q., & Benusa, A. (2017). HIPAA security compliance challenges: The case for small healthcare providers. *International Journal of Healthcare Management*, *10*(2), 135-146.