International Journal of Science Academic Research
Vol. 06, Issue 03, pp.9669-9675, March, 2025
Available online at http://www.scienceijsar.com

ISSN: 2582-6425

Research Article

SECURE CLOUD-BASED HEALTHCARE DATA MANAGEMENT FOR PRIVACY-PRESERVING STORAGE

***Ronald Ojino**

The Open University of Kenya, Kenya

Received 24th January 2025; **Accepted** 27th February 2025; **Published online** 31st March 2025

Abstract

With the rapid adoption of cloud computing, organizations increasingly rely on cloud storage for managing sensitive data, such as healthcare records. However, healthcare data management in cloud environments faces significant security challenges, including unauthorized access, data breaches and privacy risks. To address these challenges, this work presents to protect sensitive patient information in the cloud from unauthorized access, cyber threats, and data breaches while enabling secure retrieval and processing for healthcare applications. Healthcare data is gathered from multi-speciality hospitals. This data undergoes key generation using Hash-based Message Authentication Code-based Key Derivation Function to produce a secure cryptographic approach to derive encryption keys. Following this, end-to-end encryption using Advanced Encryption Standard in Galois/Counter Mode ensures confidentiality, protecting data from unauthorized access. The encrypted data is then stored in a secure cloud environment, where it remains protected from external threats. To facilitate controlled access, Zero Trust Architecture and access control mechanisms authenticate users and grant permissions based on strict security policies. When a verified user requests access, the system enforces fine-grained access control, ensuring that only authorized individuals retrieve decrypted information. Finally, the entire process ensures privacy-preserving data sharing, allowing healthcare professionals to securely access and share data without compromising security or compliance. Results demonstrate that key generation time increases from 0.5 ms (128-bit) to 6.0 ms (1024-bit), while security strength improves from 60% to 99.5% as the key size increases. Additionally, data upload performance analysis shows cloud transmission time dominates total upload time, reaching 30 seconds for 500 MB files. The proposed approach enhances security, scalability and efficiency, ensuring robust protection for cloud-stored healthcare data.

Keywords: Healthcare data, Zero Trust Architecture, Key Generation, Encryption and Cloud Storage.

INTRODUCTION

Cloud-enabled e-healthcare services have recently changed medical practice by providing virtual diagnosis, patient monitoring and smooth access to Electronic Health Records (EHRs)[1]. To store and manage healthcare data, cloud computing offers a very scalable solution, cost efficiency and high availability [2]. It would maximize the collaborative work of doctors, nurses, patients and even insurance providers all towards improving health care delivery [3]. Such an improvement can be attributed to integrating IoT-based medical devices, telemedicine and AI-driven analytics into patient care [4]. However, the increasing digitization of healthcare has exposed the system to greater safety and privacy threats with susceptible patient data that travel through the public network [5]. The defense of a strong, secured and privacy-preserving mechanism for healthcare data management could not be considered more important at any time than now [6]. In 2024, a hybrid cryptographic security algorithm was developed that combines AES, RSA, ECC, and homomorphic encryption to ensure secure, efficient mobile data transmission and storage in cloud environments. As presented by Chetlapalli et al. 2024 [7], the study emphasized the benefits of using multiple encryption algorithms in tandem to improve security without sacrificing performance, a concept that shaped the cryptographic techniques applied in the proposed cloud healthcare system. It follows, then, that secure data storage, transmission and access control are some of the major challenges modern e-healthcare services face [8]. The rising trend in cloud-based healthcare continues to be driven by several factors, including demand for remote healthcare services, increased telemedicine activities and frustration with the manual process of managing patient data. Moreover, the COVID-19 pandemic sped up this wave, necessitating digital options for the remote consultation and sharing of medical data[9]. Countries, including the US and those in Europe, put into effect regulations that impose tough security mandates to safeguard data, such as creating a HIPAA and GDPR environment, to whet the appetite of the health providers to adopt secure cloud solutions[10]. The overreliance on cloud services is a burden that exposes even healthcare data to things, such as unauthorized access, data breaches, insider threats and cyber attacks [11]. These weaknesses bring out the need for advanced security frameworks for data confidentiality, integrity and controlled access under the most effective cloud-based healthcare scenario [12]. Traditional security methods, such as password-based authentication, static encryption techniques and centralized key management, do not provide adequate security for modern cyber threats [13]. These conventional approaches can potentially lead to data breaches, identity theft and unauthorized modifications that compromise the privacy of patients[14]. Besides, role-based access control (RBAC) models often do not provide the flexibility needed in today's dynamic healthcare environments[15]. An additional drawback for RBAC is that with extremely static authorization policies, inconsistent data access policies may exist[16]. Static encryption keys also create vulnerabilities that can be exploited by attack methods that employ old cryptographic mechanisms [17]. The absence of end-to-end encryption and multi-layered security makes healthcare data susceptible to attack with man-in-the-middle (MITM), eavesdropping, or ransom ware threats. This warrants the necessity for an advanced, lightweight, scalable security framework to tackle these issues and improve data privacy for the cloud-based E-healthcare services. The

Corresponding Author:** ***Ronald Ojino,
The Open University of Kenya, Kenya

paper is structured as follows: Section 2 reviews existing solutions and their limitations. Section 3 details the methodology of the study. Section 4 presents theresults, followed by Section 5 concludes the paper.

LITERATURE SURVEY

With point cloud learning for new framework transforming architecture, it has now come up with several solutions regarding the specific issues of irregular and absence order characteristics due to the nature of the data obtained from point clouds [18]. PCT further condenses sequences of points into a permutation that could thus help farthest point sampling and nearest neighbor search in augmenting the capturing from local contexts [19]. Bobba et al. (2024) [20] introduce a dual approach combining SE-PSO-enhanced Sigmoid-LeCun Temporal Convolutional Networks for ransom ware detection and Attribute-Based K-Anonymity for data anonymization. Sparked by these insights, the proposed method merges dynamic detection strategies to secure healthcare data in cloud environments, enhancing both security and efficiency while minimizing false alarms. Another downside to PCT is that, while it gives poser to the state-of-art results in object shape classification and segmentation, it is computationally expensive and hence cannot be scaled to larger point cloud datasets. Interesting news is that changes have taken place so fast that from the original idea of an internetwork service that could be leased to ISPs; it gained its identity as a public utility, accepted by major corporations, large institutions and most government organizations [21]. Major milestones for this journey are the core papers by Google in 2003 and their following establishment of a commercial service via Amazon EC2 in 2006 [22]. Now, it is not only cost-saving purposes behind cloud computing, it has gained hype as a means of making money, too. The article goes further to examine the concept, the evolution, pros and cons, the value chain and some of the standardization initiatives made on their way.

This study elaborates on the application of cloud computing technology to organizations and illustrated in the case studies in order to appreciate the technological innovations and salient features of the technology [23]. Furthermore, it speaks on the kinds of challenges in security and intrusion detection systems facing the field now and what could be future research directions on challenges posed to cloud adoption in business environments [24]. Clouds have practically served and become generally accepted by industries, individuals and society in general since 2019. In all probability due to low cost and an on-demand consideration [25], security has become such a major problem as it has challenged all the three layers of security-the IaaS, PaaS and SaaS levels-all through the year 2020. This particular research attempts to furnish a synopsis of security in clouds within the previous 10 years. However, the research is inherently restricted by the climate of rapid technology advancement as related to clouds and challenges in addressing increasing security concerns over time [26]. A mass of data generated by IIoT cannot be handled by IIoT devices because of power and storage issues [27]. Self-organization and short-range IoT networking power a solution where cloud computing can be used for storing data outside some constraints of the device. This research is focused on hitches and algorithms that seamlessly integrate IoT with cloud computing focusing on the efficiency of cloud solutions and new forms of semi-structured storage[28].

The implementation of newly established algorithms, such as anomaly and cluster-based algorithms, is presented for analyzing streams of IoT events to detect possible undesired activities[29]. The training involved improving fraud detection based on supervised and unsupervised learning models using previous historical transaction data. Credibility was bolstered through adaptive retraining methods and automatic responses to fraud events[30]. Challenges found include bad quality data, computational complexity, and the highly dynamic shift in the fraud environment, which significantly affects the capability of detecting fraud. A service-oriented architecture was developed for the system to run on a Hadoop-managed server cluster, providing both processing power and data storage[31]. This system efficiently manages educational resources for remote learning within large datasets and high concurrency. Stress tests have proven that the platform can reliably support a multitude of simultaneous users and numerous data transactions during heavy loads.

The hybrid IoT-integrated framework, combining edge AI and cloud computing, has recently been proven to be an intelligent solution for processing health data. The research focuses on data sharing security, reduced latency, and improved process quality for decision-making purposes. Advanced AI models like Random Forest classifiers, Transformer Networks, and Temporal Convolutional Networks were used in this model. Distributed processing across the system was enabled through cloud computing, cloudlet, and edge layers. Real-time stream analytics is performed using Apache Flink, while secure information exchange is ensured through blockchain technology. However, some limitations of this work include high computation costs, integration issues, and bottlenecks in large-scale data processing. An approach was also suggested for narrowing down IoT security using critical node identification, invasive assessments, security measures, and performance impact analyses. One such approach involved quantification in assessing vital IoT system components after vulnerability assessments. An intrusion detection system was recommended, along with a variety of encryption tools, access control methodologies, and frequent security audits to assess the sensitivity of each method in overall IoT system security.

Problem Statement

Most existing systems perform well; however, dynamic and adaptive access control mechanisms are largely absent, thus leading to unauthorized access and possible insider threats[32]. In addition, poor key management practices, using stagnant or often reused cryptographic keys, give rise to brute-force and replay attacks on encryptions[33]. This set of challenges exposes sensitive health data to security threats comprising both confidentiality and integrity. The proposed work will solve these issues through strict access control, efficient key management and end-to-end encryption for secure cloud-based health data management.

METHODOLOGIES

This process initiates with data collection within different health facilities where the patient data which includes medical history and test results is aggregated. The cryptographic key is generated using HKDF (HMAC-based Key Derivation Function), thereby ensuring efficient key management. The collected data are encrypted using the Advanced Encryption Standard-Galois/Counter Mode to ensure confidentiality and

integrity during the communication process. The encrypted data are stored securely in the cloud to ensure it is protected from unauthorized access. In case of users requesting access, authentication through Identity Based Access Control in Zero Trust Architecture is performed, making sure that only duly authenticated users can step further. Post-authentication, the access control policies will check for authorization so that only legitimate users shall be enabled to retrieve relevant data[34]. Once authorized, the decryption key derived from HKDF can effectively allow patient's data access, ensuring that patient information remains secure while permitting authorized healthcare personnel to use the data judiciously. The overall architecture is illustrated in Figure 1.

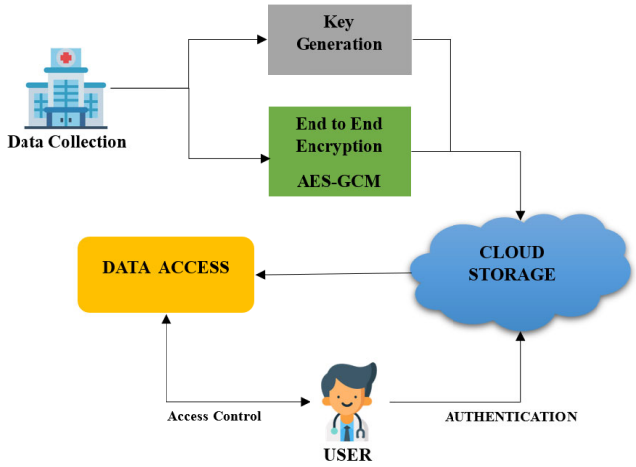

Figure 1. Secure Cloud-Based Healthcare Data Management Architecture

Data Collection

In cloud-based E-health care services, hospital patient Electronic Health Records (EHR) are collected from various sources such as hospitals, wearable devices and remote monitoring systems. All collected data are arranged and categorized for secure infrastructure in the cloud to ensure availability and efficient management. Cloud storage provides access in real time, and scalability and allows for collaboration by healthcare providers from a remote place. Redundant storage and backup prevent data loss and provide disaster recovery in case of failures. Advanced techniques for indexing and retrieval help in optimizing performance for quick and efficient accessing. The regulatory compliance in the field of health assures data protection while remaining available for authorized use.

Key Management using HKDF

After the data collection from healthcare facilities, the key management is performed using the HKDF, which ensures the safe management of keys. The HKDF has been given to produce strong cryptographic keys based on a shared secret, which provides more security and prevents key reuse[35]. A master key is derived and expanded into several session keys, with each used for encrypting different pieces of data[36]. This dynamically generated key enhancement method adds to confidentiality and counter measures against different cryptographic attacks. Derived keys are subject to periodic updates, making them less vulnerable to brute-force or replay attacks [37]. Those securely managed keys are then used to encrypt the collected healthcare data in preparation for transmission and storage. HealthFog, a state-of-the-art hybrid system that merges IoT, fog nodes, and cloud computing for fast and accurate disease detection, achieving a 94.5% accuracy rate and 0.08-second latency. Sparked by this pioneering work, the designed system adapts similar hybrid models to elevate healthcare data management security and performance in the cloud, as presented by Kethu at al. (2024)[38].

HKDF works in two stages:

Extract Phase - Converts the master key into a fixed-length pseudorandom key.
Expand Phase - Generates multiple cryptographic keys from the extracted key.

Extract Phase is represented as equation (1),

$$PRK = HMAC(\text{salt}, K_{master}) \quad (1)$$

Where, PRK = Pseudorandom key (intermediate key), HMAC = Hash-based Message Authentication Code, salt = Random value ensuring uniqueness, K_{master} = Master key used for key derivation. This step ensures that even if the initial key material has low entropy, HMAC strengthens it into a secure pseudorandom key[39]. The salt prevents predictability, making it harder for attackers to guess future keys.

Expand Phase is expressed as equation (2),

$$K_{session} = HMAC(PRK, \text{info} \parallel \text{counter}) \quad (2)$$

Where, $K_{seassion}$ = Derived session key used for encryption, info = Context-specific information, counter = Iteration value to generate multiple keys. This step generates a secure session key specific to each transaction, ensuring that old keys cannot be reused[40]. The info parameter ensures that each application (e.g., encryption, authentication) gets a unique key.

The full HKDF key derivation function is expressed as equation (3),

$$K_{session} = HKDF(K_{input}, \text{salt}, \text{info}, L) \quad (3)$$

Where, $K_{session}$ = Final session key used for AES-GCM encryption,K_{input} = Initial key material, salt = Random salt value, info = Application-specific data, L = Desired key length
If an attacker compromises a session key, they cannot derive past or future keys. Every encryption session has a different key, reducing vulnerability to cryptographic attacks. Enhances security for cloud-based EHRs ensures only authorized users can generate valid keys.

End-to-End Encryption

Once the cryptographic keys have been generated securely, they are employed for End-to-End Encryption (E2EE) using AES-GCM. AES-GCM preserves confidentiality and integrity by keeping the collected information secret right from its storage or transmission[41]. With AES-GCM, the actual encryption involves taking the plaintext and processing it with AES together with a secret key and a randomly generated nonce (IV) to generate the cipher text and an accompanying

authentication tag, which is used later for integrity verification. For decryption, the recipient will use the same key and nonce to obtain original data and check its authenticity by the tag. AES-GCM provides authenticated encryption that can protect from manipulation, replay attacks, and unauthorized access. Efficient, secure, and great for healthcare data transmission and secure storage within a cloud environment.

AES-GCM encrypts the plaintext P using a secret key K and a nonce (IV) N, producing ciphertext C and an authentication tagT and it's represented as equation (4),

$$C, T = AES - GCM - Encrypt(K, N, P, A) \quad (4)$$

Where, C = Encrypted ciphertext, T = Authentication tag, K = Secret key derived from HKDF, N = Nonce (Initialization Vector), P = Plaintext data, A = Additional authenticated data (AAD) for integrity verification

Decryption retrieves the original plaintext P using the same secret key K, nonce N, and authentication tag T. If the integrity check fails, decryption is rejected. Also, it's represented as equation (5),

$$P = AES - GCM - Decrypt(K, N, C, A, T) \quad (5)$$

AES-GCM uses a Galois Counter Mode (GCM), an encryption mode that combines authentication so that data will be kept confidential and protected from modification. The nonce N ensures the uniqueness of encryption each time performed to guard against replay attacks. The authentication tag T indicates that the integrity of the data is guaranteed and verifies that the ciphertext has not been modified. The additional authenticated data (AAD) A is optional metadata. Its processing ensures that headers or specific user identifiers are authenticated along with the encrypted message. If T does not match at decryption time, the data will be considered compromised and decryption will not take place. This approach guarantees that healthcare data remains secure during transmission and storage, protecting against eavesdropping, unauthorized modifications, and replay attacks.

Cloud Storage

After the AES-GCM encryption, the data is secured and stored in the cloud to ensure access and secrecy. The data, encrypted along with its corresponding authentication tag, would be uploaded to prevent any unauthorized access. Indeed, the incredible architecture of the cloud allows for extensive scalability in the storage of data and also helps in managing large volumes of sensitive healthcare data. Access control models implement authentication as well as authorization policies that provide an avenue for verified users to access and decrypt data[42]. The secure transport layer will also facilitate the secure transfer of data between the cloud and authorized entities. Therefore, this guarantees integrity, confidentiality and compliance towards security standards at whole.

Authentication

Only those users who are authorized can be permitted to access the encrypted data stored in the cloud. To access the information, the user must authenticate themselves through one of the identity-based authentication mechanisms such as ZTA for access requests[43]. Requiring multi-factor authentication (MFA) and dynamic verification ensures that unauthorized individuals gain entry. Once authentication is successful, the system opens it up for usage of the data as per the access control policies strictly defined. It safeguards from unauthorized misuse and data leakage and is strengthened through secure session management, which prevents reuse or misassignment of authentication credentials.

Secure Access & Data Sharing

After a successful verification, the verified access control mechanism will ensure that only an authorized individual has the privilege of accessing or processing an encrypted data object. Role and policy-based access control RBAC/PBAC prevents user access according to roles. For instance, doctors, nurses and insurance providers should have access only to the data relevant to their practice. To further this secrecy, the secure computation enabled by multiparty computation has permitted a number of users to carry out computations by working on encrypted data without reducing it, thus preserving the medical information integrity while enabling secure collaborative analysis. Only the end result would be available, hence avoiding exposure of the data during processing. That means keeping most sensitive medical information private while enabling safe collaborative medical decision making legalized and compliant with laws.

Access control and secure data sharing are enforced using RBAC and Secure Multi-Party Computation (SMPC). The mathematical representation ensures that only authorized users can access or compute on encrypted data without revealing sensitive information

Access to data is granted based on user roles is represented as equation (6),

$$Access(U, R) = \begin{cases} 1, & \text{if } U \in R_{anthorized} \\ 0, & \text{otherwise} \end{cases} \quad (6)$$

Where,U = User requesting access, $R_{authorixed}$ = Set of authorized roles (e.g., Doctor, Nurse, Insurance Provider), Access $(U, R) - 1 \rightarrow$ Access granted, Access $(U, R) - 0 \rightarrow$ Access denied. Only verified users matching the authorized role set can access data. Unauthorized users are denied access, ensuring data confidentiality [44].

SMPC enables multiple parties to compute on encrypted data without decrypting it. Given N participants, each party P_i holds a secret share $S_i$is expressed as equation (7),

$$S - S_1 + S_2 + \cdots + S_N \ (modp) \quad (7)$$

Where, S = Original encrypted data, S_i = Secret share assigned to participant i, N = Number of computing parties, p = Large prime modulus for secure computations.

Computing a function $f(S)$ securely is represented as equation (8),

$$f(S) - f(S_1) + f(S_2) + \cdots + f(S_N) \ (modp) \quad (8)$$

Each party P_i only sees its own share S_i, never the full data S. The function $f(S)$ is computed without revealing individual inputs, ensuring privacy. Only the final computed result is

revealed, maintaining data confidentiality [45]. Access control ensures that only authorized users can access encrypted data using RBAC, where access is granted based on predefined roles. SMPC enables multiple users to perform computations on encrypted data without decrypting it, ensuring privacy and secure collaboration.

RESULTS

This section evaluates the performance of key generation and data upload processes. It analyzes the computational overhead of HKDF-based key derivation, the impact of encryption on upload time and the security strength. The findings highlight trade-offs between security, efficiency, and cloud transmission performance.

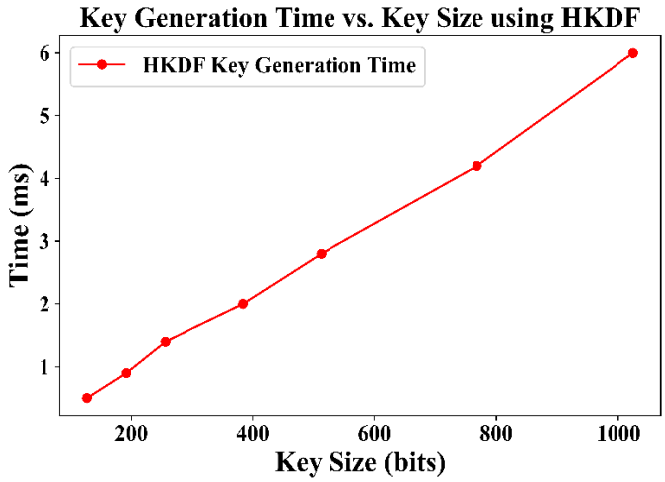

Figure 2. Key generation time vs Key size

In Figure 2, the correlation between the key size in bits and qualification time shown HKDF in milliseconds is set forth. With the key size increasing from 128-1024 bits, the generation time is observed ever-increasing in the range of 0.5-6.0 ms, thus the computational overhead for the acquisition of longer keys. The recorded times thus turn out to be 0.9 ms for a 192-bit key, 1.4 ms for 256 bits, 2.0 ms for 384, 2.8 for 512 bits, while 4.2 and 6.0 ms for 768 and 1024-bit keys respectively. Hence, this almost linear trend indicates that HKDF possesses a very good scaling property. It thus shows the trade-off between security and performance since bigger key sizes mean stronger protection but take longer to generate. Thus, an optimum key size should be selected for the expected compromise between security and efficiency [46].

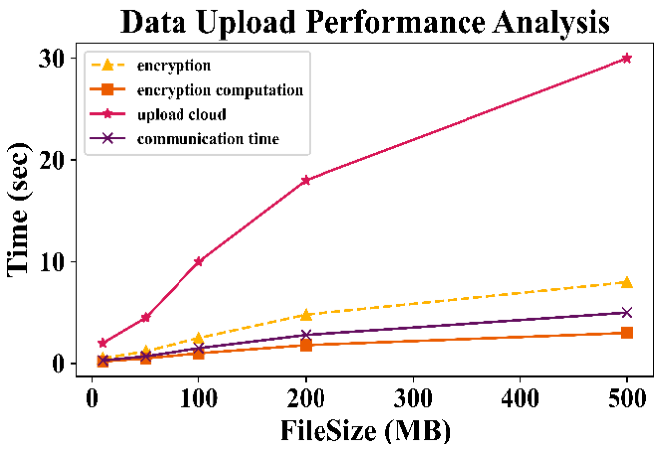

Figure 3. Data Upload Performance Analysis

In Figure 3, the data upload performance analysis showing the file size (in MB) and different components of time is reported. It is from 10 MB to 500 MB; the encryption time increases from 0.5 seconds to 8.0 seconds, and the encryption computation time increases from 0.2 seconds to 3.0 seconds, signifying a gradual increase of processing overhead as the file increases in size[47]. The upload cloud time grows steeply, from 2.0 sec to 30.0 sec, indicating cloud transmission contributes significantly to the overall upload time. In the same vein, the time for communication increases from 0.3 seconds to 5.0 seconds, but slower than that for cloud upload. This portrays the idea that as file sizes grow, encryption still crashes negligibly, but delays in networks and through the cloud dominate the overall upload performance[48].

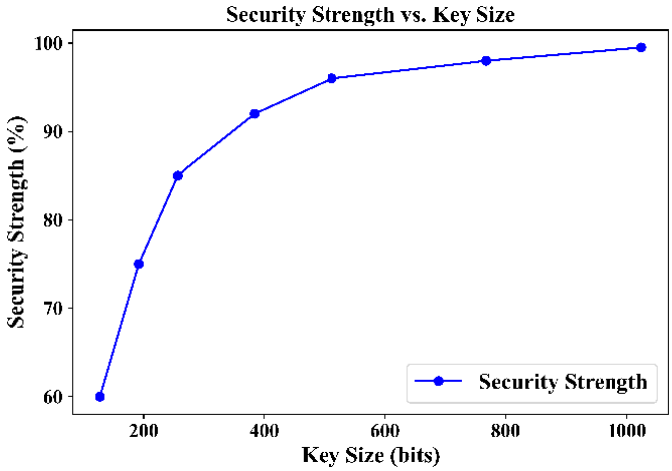

Figure 4. Security Strength

Figure 4 illustrates the association between key size in bits and security strength in percentages. The major change noticed is the increase of security strength from 60% to 99.5% as key size increases from 128 to 1024 bits. The increase is steep at first as 192-bit and 256-bit keys reach 75% and 85% as compared to say 384 bits which reaches 92% and 512 bits which reaches 96%. It shows shrinking returns continued improvement obtained with bigger key sizes. The peak or highest security strength of 99.5% is observed at the 1024-bit mark, thus it is proven that larger key sizes do yield stronger-encrypted standards, yet very little strength gain is observed beyond a specific threshold. Warning that higher costs are involved since little improvement occurs beyond a certain size, these results better explained the trade-off of security and cost in terms of computing processing because a higher key increases protection and consequently cost is likely to occur as well.

Conclusion

This paper describes a secure cloud-based healthcare data management system that can be used to ensure secure storage, controlled access and privacy-preserving data sharing in cloud-based healthcare systems. The proposed uses AES-GCM for securing data, HKDF for efficient key generation, ZTA for authentication and SMPC for privacy-preserving data sharing. Thus, the proposed system addresses security and privacy challenges. Also, performance evaluation shows that the time taken to generate keys will range from 0.5 ms for 128-bit keys to 6.0 ms for 1024-bit keys keeping up efficiency scaling property. Time taken for encryption remains computationally feasible between 0.5 sec for 10 MB of files to 8.0 sec for 500

MB files, and that time spent uploading to the cloud increases from 2.0 sec to 30.0 sec. Security strength evaluation confirms that increasing the key size enhances security, with security strength rising from 60% (128-bit) to 99.5% (1024-bit), reinforcing the system's resilience. This shows that network plays a role in the transmission of data in the system. However, there is a trade-off between the two. The balance is achieved with the least overhead in encryption while ensuring control of access and data protection. This, therefore, means that data is preserved from being accessed by unauthorized parties through adaptive authentication[49]. It also accounts for privacy-preserving collaborative processing. This makes it compliant with healthcare law. This, therefore, measures in the scalable and safe solution towards adopting healthcare applications. Future work will be concerned with the implementation of blockchain technology to provide decentralized and tamper-proof access control such that it guarantees transparency and immutability to healthcare data access.

REFERENCES

1. Shakil, K. A., Zareen, F. J., Alam, M., & Jabin, S. (2020). BAM Health Cloud: A biometric authentication and data management system for healthcare data in cloud. *Journal of King Saud University-Computer and Information Sciences,* 32(1), 57-64.
2. Sharma, D. K., Chakravarthi, D. S., Shaikh, A. A., Ahmed, A. A. A., Jaiswal, S., & Naved, M. (2023). The aspect of vast data management problem in healthcare sector and implementation of cloud computing technique. *Materials Today: Proceedings,* 80, 3805-3810.
3. Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2022). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. *Neural Computing and Applications,* 1-16.
4. Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M., & Abid, M. (2021). HealthBlock: A secure blockchain-based healthcare data management system. *Computer Networks,* 200, 108500.
5. Sengupta, S., & Bhunia, S. S. (2020). Secure data management in cloudlet assisted IoT enabled e-health framework in smart city. *IEEE Sensors Journal,* 20(16), 9581-9588.
6. Nazir, S., Khan, S., Khan, H. U., Ali, S., Garcia-Magarino, I., Atan, R. B., & Nawaz, M. (2020). A comprehensive analysis of healthcare big data management, analytics and scientific programming. *IEEE Access,* 8, 95714-95733.
7. H. Chetlapalli, D. P. Deevi, N. S. Allur, and T. Perumal, "Comprehensive Strategies For Mobile Data Security In Cloud Computing Using Advanced Cryptographic Techniques," *Int. J. Eng. Sci. Res.,* vol. 14, no. 2, 2024.
8. Gupta, N. S., & Kumar, P. (2023). Perspective of artificial intelligence in healthcare data management: A journey towards precision medicine. *Computers in biology and medicine,* 162, 107051.
9. Aceto, G., Persico, V., & Pescapé, A. (2020). Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0. *Journal of Industrial Information Integration,* 18, 100129.
10. Azbeg, K., Ouchetto, O., & Andaloussi, S. J. (2022). BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security. *Egyptian informatics journal,* 23(2), 329-343.
11. Tahir, A., Chen, F., Khan, H. U., Ming, Z., Ahmad, A., Nazir, S., & Shafiq, M. (2020). A systematic review on cloud storage mechanisms concerning e-healthcare systems. Sensors, 20(18), 5392.
12. Almalawi, A., Khan, A. I., Alsolami, F., Abushark, Y. B., & Alfakeeh, A. S. (2023). Managing security of healthcare data for a modern healthcare system. Sensors, 23(7), 3612.
13. Pustokhin, D. A., Pustokhina, I. V., & Shankar, K. (2020). Challenges and future work directions in healthcare data management using blockchain technology. In Applications of Blockchain in Healthcare (pp. 253-267). Singapore: Springer Singapore.
14. Zhang, G., Yang, Z., & Liu, W. (2022). Blockchain-based privacy preserving e-health system for healthcare data in cloud. *Computer Networks,* 203, 108586.
15. Shi, M., Jiang, R., Hu, X., & Shang, J. (2020). A privacy protection method for health care big data management based on risk access control. *Health care management science,* 23, 427-442.
16. Abbas, A., Alroobaea, R., Krichen, M., Rubaiee, S., Vimal, S., & Almansour, F. M. (2024). Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. *Personal and ubiquitous computing,* 28(1), 59-72.
17. Li, C., Dong, M., Li, J., Xu, G., Chen, X. B., Liu, W., & Ota, K. (2022). Efficient medical big data management with keyword-searchable encryption in healthchain. *IEEE Systems Journal*, 16(4), 5521-5532.
18. Stergiou, C. L., Plageras, A. P., Memos, V. A., Koidou, M. P., &Psannis, K. E. (2023). Secure monitoring system for IoT healthcare data in the cloud. *Applied Sciences,* 14(1), 120.
19. Kumar, P. M., Hong, C. S., Afghah, F., Manogaran, G., Yu, K., Hua, Q., & Gao, J. (2021). Clouds proportionate medical data stream analytics for internet of things-based healthcare systems. *IEEE Journal of Biomedical and Health Informatics*, 26(3), 973-982.
20. J. Bobba, R. L. Bolla, E. F. Abiodun, and S. Amin, "Attribute-based k-anonymity and se-psoenhanced sigmoid-lecun-tcn for mitigating ransom ware attack with api protection for cloud applications," *Int. J. Adv. Res. Inf. Technol. Manag. Sci.,* vol. 1, no. 01, Art. no. 01, Dec. 2024.
21. Wang, Z., Luo, N., & Zhou, P. (2020). GuardHealth: Blockchain empowered secure data management and Graph Convolutional Network enabled anomaly detection in smart healthcare. *Journal of Parallel and Distributed Computing,* 142, 1-12.
22. Arul, R., Al-Otaibi, Y. D., Alnumay, W. S., Tariq, U., Shoaib, U., & Piran, M. J. (2021). Multi-modal secure healthcare data dissemination framework using blockchain in IoMT. Personal and Ubiquitous Computing, 1-13.
23. Pandey, A. K., Khan, A. I., Abushark, Y. B., Alam, M. M., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Key issues in healthcare data integrity: Analysis and recommendations. *IEEE Access,* 8, 40612-40628.
24. Singh, S., Rathore, S., Alfarraj, O., Tolba, A., & Yoon, B. (2022). A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Generation Computer Systems,* 129, 380-388.
25. Jayabalan, J., & Jeyanthi, N. (2022). Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. *Journal of Parallel and distributed computing,* 164, 152-167.
26. Putzier, M., Khakzad, T., Dreischarf, M., Thun, S., Trautwein, F., & Taheri, N. (2024). Implementation of

cloud computing in the German healthcare system. npj digital medicine, 7(1), 12.
27. Gohar, A. N., Abdelmawgoud, S. A., & Farhan, M. S. (2022). A patient-centric healthcare framework reference architecture for better semantic interoperability based on blockchain, cloud, and IoT. *IEEE access,* 10, 92137-92157.
28. Amponsah, A. A., Adekoya, A. F., &Weyori, B. A. (2022). Improving the financial security of national health insurance using cloud-based blockchain technology application. *International Journal of Information Management Data Insights,* 2(1), 100081.
29. Farid, F., Elkhodr, M., Sabrina, F., Ahamed, F., & Gide, E. (2021). A smart biometric identity management framework for personalised IoT and cloud computing-based healthcare services. Sensors, 21(2), 552.
30. Panwar, A., Bhatnagar, V., Khari, M., Salehi, A. W., & Gupta, G. (2022). A Blockchain Framework to Secure Personal Health Record (PHR) in IBM Cloud-Based Data Lake. *Computational Intelligence and Neuroscience,* 2022(1), 3045107.
31. Ramachandra, M. N., Srinivasa Rao, M., Lai, W. C., Parameshachari, B. D., Ananda Babu, J., & Hemalatha, K. L. (2022). An efficient and secure big data storage in cloud environment by using triple data encryption standard. *Big Data and Cognitive Computing,* 6(4), 101.
32. Narayanan, U., Paul, V., & Joseph, S. (2022). A novel system architecture for secure authentication and data sharing in cloud enabled Big Data Environment. *Journal of King Saud University-Computer and Information Sciences*, 34(6), 3121-3135.
33. Stauffer, J., & Zhang, Q. (2024). s2Cloud: a novel cloud-based precision health system for smart and secure IoT big data harnessing. Discover Internet of Things, 4(1), 3.
34. Mubarakali, A. (2020). Healthcare services monitoring in cloud using secure and robust healthcare-based BLOCKCHAIN (SRHB) approach. Mobile Networks and Applications, 25(4), 1330-1337.
35. Singh, G., Jeyaraj, R., Sharma, A., & Paul, A. (2023). A Novel Data Management Scheme in Cloud for Micromachines. *Electronics*, 12(18), 3807.
36. Kuttiyappan, M., Appadurai, J. P., Kavin, B. P., Selvaraj, J., Gan, H. S., & Lai, W. C. (2024). Big Data Privacy Protection and Security Provisions of the Healthcare SecPri-BGMPOP Method in a Cloud Environment. *Mathematics*, 12(13), 1969.
37. Yang, Z., Liang, B., & Ji, W. (2021). An intelligent end–edge–cloud architecture for visual IoT-assisted healthcare systems. *IEEE internet of things journal,* 8(23), 16779-16786.
38. S. S. Kethu, S. Narla, D. T. Valivarthi, S. Peddi, D. R. Natarajan, and A. Kurunthachalam, "HealthFog: A Comprehensive Cloud and Fog-Based System for Early Diagnosis of Infectious and Heart Diseases Leveraging IoT and Deep Learning," *Int. J. Appl. Sci. Eng. Manag.,* vol. 18, no. 2, 2024.
39. Margheri, A., Masi, M., Miladi, A., Sassone, V., & Rosenzweig, J. (2020). Decentralised provenance for healthcare data. *International Journal of Medical Informatics,* 141, 104197.
40. Dhiman, G., Juneja, S., Mohafez, H., El-Bayoumy, I., Sharma, L. K., Hadizadeh, M., & Khandaker, M. U. (2022). Federated learning approach to protect healthcare data over big data scenario. *Sustainability*, 14(5), 2500.
41. Ali, S., Hafeez, Y., Jhanjhi, N. Z., Humayun, M., Imran, M., Nayyar, A., & Ra, I. H. (2020). Towards pattern-based change verification framework for cloud-enabled healthcare component-based. Ieee Access, 8, 148007-148020.
42. Yoosuf, M. S. (2021). Lightweight fog-centric auditing scheme to verify integrity of IoT healthcare data in the cloud environment. Concurrency and Computation: Practice and Experience, 33(24), e6450.
43. Saini, A., Zhu, Q., Singh, N., Xiang, Y., Gao, L., & Zhang, Y. (2020). A smart-contract-based access control framework for cloud smart healthcare system. *IEEE Internet of Things Journal,* 8(7), 5914-5925.
44. Ghayvat, H., Pandya, S., Bhattacharya, P., Zuhair, M., Rashid, M., Hakak, S., & Dev, K. (2021). CP-BDHCA: Blockchain-based Confidentiality-Privacy preserving Big Data scheme for healthcare clouds and applications. *IEEE Journal of Biomedical and Health Informatics,* 26(5), 1937-1948.
45. Puri, V., Kataria, A., & Sharma, V. (2024). Artificial intelligence-powered decentralized framework for Internet of Things in Healthcare 4.0. Transactions on Emerging Telecommunications Technologies, 35(4), e4245.
46. Praveen, S. P., Murali Krishna, T. B., Anuradha, C. H., Mandalapu, S. R., Sarala, P., & Sindhura, S. (2022). A robust framework for handling health care information based on machine learning and big data engineering techniques. *International Journal of Healthcare Management,* 1-18.
47. Sarosh, P., Parah, S. A., Bhat, G. M., & Muhammad, K. (2021). A security management framework for big data in smart healthcare. *Big Data Research,* 25, 100225.
48. Xu, Y., Bhuiyan, M. Z. A., Wang, T., Zhou, X., & Singh, A. K. (2022). C-fdrl: Context-aware privacy-preserving offloading through federated deep reinforcement learning in cloud-enabled IoT. *IEEE Transactions on Industrial Informatics,* 19(2), 1155-1164.
49. Jeong, Y. S., Kim, D. R., & Shin, S. S. (2021). Efficient data management techniques based on hierarchical IoT privacy using block chains in cloud environments. *The Journal of Supercomputing*, 77, 9810-9826.

****