Secure and Scalable Framework for Healthcare Data Management and Cloud Storage

[1]Bhavya Kadiyala
Data Architect, CBMI at UTHSC, Memphis, TN, USA
kadiyalabhavyams@gmail.com

[2]G. Arulkumaran
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology
Associate Professor
chennai, india
arulkumarang.reva@gmail.com

ABSTRACT

The critical importance of enforcing effective security measures in health systems with the increasing cloud computing usage highlights the growing concern on protecting sensitive patient information. Complications in existing systems involve even higher computational costs of encryption incurred due to poor authentication mechanisms exposed to data breaches. This study aims to collect healthcare data from hospitals and patients, to ensure its confidentiality, and store the data securely in cloud storage for efficient and protected access. The data is collected from hospitals and patients, followed by detection of outliers for the subsequent elimination of discrepancies. The sensitive nature of the data will be secured by applying the Triple Data Encryption Standard (3DES) encryption, while OAuth will provide resourceful authentication. The encrypted data are stored for scalability access in cloud storage. The results indicate that in increasing data size, the time taken for an encryption also seems to increase from 10 seconds at 40 KB to 55 seconds at 120 KB and throughput, peaking at 0.5 req/s at the request rate of 0.6. The study improves data security, boosts system performance, and improves scalability in cloud-based healthcare systems, thus providing the best solution for problems that challenge the systems today.

Keywords: Cloud Storage, Data Encryption, Healthcare Data Security, OAuth Authentication, Scalable Healthcare Systems**.**

1. INTRODUCTION

The aforementioned increasing complications and scaling demands in healthcare systems have, therefore, necessitated the secure and efficient management of sensitive patient data [1]. Cloud computing is a popular solution because of its scalability, flexibility, and cost [2]. However, there exist serious challenges to the privacy and security of data entrusted to cloud-based healthcare systems [3]. Traditional encryption methods and authentication algorithms rarely suffice to guarantee that no unauthorized access is allowed and that confidentiality is granted for patient information [4]. With recent trends witnessing the healthcare domain adopting cloud technology, the necessity arising for robust security measures has been even more pronounced towards protection of patient privacy and upholding of regulatory compliance [5].

A number of methods are available, and most of them have been proposed to ensure security and authentication in cloud-based healthcare systems [6]. Many of these approaches are based on traditional encryption techniques: AES Advanced Encryption Standard, RSA Rivest–Shamir–Adleman, and Triple DES also known as 3DES, to encrypt patient data [7]. Other authentication protocols include OAuth which have been implemented into cloud services [8]. However, such methods and mechanisms often suffer from a high computational cost and poorly scale with an overall vulnerability to many types of cyberattacks including brute force and man-in-the-middle attacks [9]. Furthermore, they depend on a single-layer security mechanism that makes them vulnerable to breaches in case of a single point of failure [10].

2. LITERATURE SURVEY

The cloud computing today is used by governments, large organizations, and institutions, not really much different from the Jigsaw Mali. Historical portraits are the first work on this road map, proclaiming publications on Google in 2003, succeeded by the actual commercial launching of Amazons EC2 in 2006[11]. With cloud computing,

some industry is seeing, save dollars, and is providing revenue opportunities. Basic concepts, history, pros and cons, value chains, and standardization developments spanning several years [12].

After all, IIoT produces a large quantity of data that will not be maintained in the inside storage buffer available on devices with problems such as power scarcity and limited storage capacity [13]. Self-organization and short-range IoOT networking provide outsourcing to cloud computing data out of the bounds on the device. [14] This study discusses obstacles associated with merging IoT with cloud computing and then deliberates on the computing techniques, with an emphasis on Large and Complex Problems for Tools in Cloud Solutions that get formed as a result and trends in the data storage.

The research has focused on the instances of these technologies in organizations from perspective of innovations and other major aspects of these technologies [15]. For an inclusive approach, other topics included were cybersecurity and intrusion detection and prevention as future research directions concerning the challenges of cloud adoption in a business environment [16],[17].

PCT or Point Cloud Transformer proposes a promising novel framework for point cloud learning that has been constructed from the transformer architecture, will directly deal with their irregular and unordered nature to conquer the aforementioned limitations [18]. PCT operates in point sequences, is permutation invariant, and captures local context by means of far-point sampling and nearest-neighbor search. A point against this architecture is that it admittedly attains state-of-the-art results in shape classification and segmentation tasks-high cost of resources inefficient for larger point cloud datasets [20].

Cloud computing has become a necessity for people and businesses in providing services for their consumption-and quite beyond that. This was the fairest and most beautiful thing about it when it did provide ease of access and lower costs for an on-demand provision [21]. Security is still in the to-be-determined category; perhaps, his will continue to evolve as three-layer security exposures play up: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Here, the current review intends scanning the decade-long scenario of the security in the clouds [22].

2.1. PROBLEM STATEMENT

Cloud-based healthcare security applications face a number of challenges such as reliance on computation-intensive encryption technique not scaling well with huge data [23]. Singular layer security mechanisms such as simple password authentication generally fail at more advanced types of cyberattacks [24]. In addition, the majority of solutions fail to integrate their encryption and authentication system and suffer from ensuring data availability and redundancy [25], which may potentially introduce vulnerabilities in cloud environments.

3. METHODOLOGY

Advanced methods for encryption, authentication, and cloud-based technologies are revolutionizing the security and management of sensitive health data is shown in figure 1. The data is collected from multiple sources, among them hospitals and patients, followed by detection of outliers for the subsequent elimination of discrepancies. The sensitive nature of the data will be secured by applying the Triple DES (3DES) encryption. however, Triple DES encryption is meant to secure the sensitive data, while OAuth will provide resourceful authentication. The encrypted data are stored for scalability access in cloud storage.

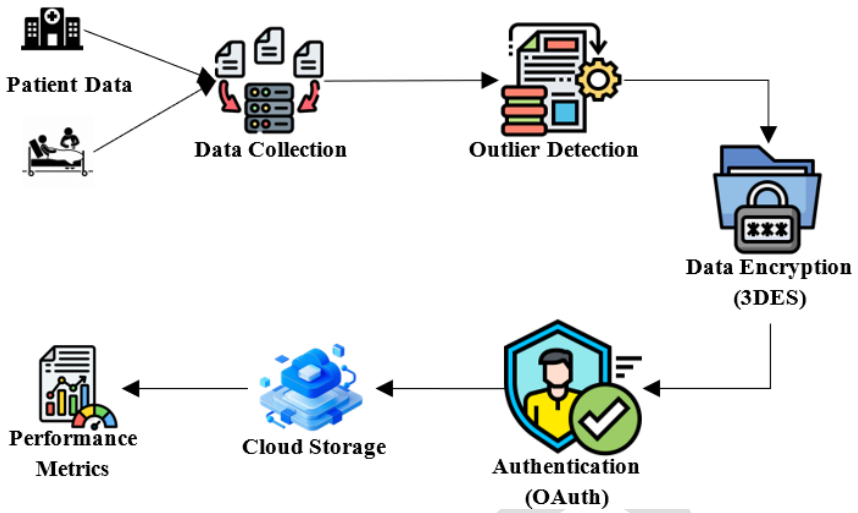

Figure 1: Secure Healthcare Data Management and Cloud Storage Framework

3.1. Data Collection

Data Collection refers to the collection of patient data from myriad sources such as hospitals and directly from the patients themselves. The data may include medical history, vital signs, lab results, and any other medical information. The collection process ensures accurate data retention, completion, and secure storage. Patient data collection employs Electronic Health Record Systems (EHR) enabled medical devices that continuously monitor and record patient health metrics. After collection, the data is sent through a secure system where it is processed, including testing for outliers and encryption to guarantee the confidentiality and integrity of the data before storage in the cloud. The data becomes the basis for deeper analyses and decision-making within the healthcare system.

3.2. Data Pre-processing

The collected patient data for further analysis and secure storage. The very first step is Outlier Detection where any data points which significantly deviate from the norm should be identified and removed with the purpose that only valid and reliable data be processed afterwards, which through that improves quality and accuracy in the data by eliminating errors or anomalies that could affect results. The next step is Data Encryption using Triple DES (3DES) to secure sensitive components of patient data. This would ensure that they remain confidential and protected from unauthorized access. Pre-processing, thus plays a pivotal role in justifying that the integrity and security when it comes to storing these patient data are done beforehand in the cloud for further analysis and retrieval.

3.3. Data Encryption using Triple DES

Data encryption using Triple DES (3DES) is needed to secure sensitive patient data from unauthorized access during storage and transmission. Triple DES is a symmetric key encryption algorithm whereby the standard DES algorithm is applied three times for every data block, thus enhancing security compared to ordinary DES. After pre-processing of the patient data, 3DES would be used to encrypt them in such a way as to maintain data confidentiality and discourage data breach. It encrypts the data using a long key through multiple paths, which enhance security and render it tough for the adversary to decrypt the data blocks without the key. After encryption, they are stored in the cloud so that they can remain protected, being accessed only by authorized users. The equation (1) for Triple DES encryption is given below.

$$C = E_K3\big(D_K2(E_K1(P))\big) \tag{1}$$

Were, P is the plaintext data, C is the ciphertext, E_K1 and E_K3 represent encryption with key $K1$ and $K3$, D_K2 represents decryption with key $K2$, $K1, K2$, and $K3$ are the three secret keys used.

3.4. Authentication using OAuth

OAuth-based authentication allows a secure and efficient means of verifying the identity of medical practitioners or users who are accessing sensitive health data. OAuth is a token-based authorization framework that allows users to give third-party services access to their resources without sharing their credentials. In this application scenario, the user logs in through the OAuth provider, which returns an access token used for the purpose of

authentication.
The OAuth flow can be described by the following steps:

- Authorization Request: The user is redirected to the authorization server to grant permission.
- Authorization Grant: Upon successful login, the user grants authorization, and an authorization code is sent.
- Access Token Request: The authorization code is sent to the OAuth server to request an access token.
- Access Token Response: The server responds with an access token that is used to access protected resources.

The general OAuth equation can be summarized as:

$$\text{Access Token} = f(\text{Authorization Grant, Client Credentials}) \quad (2)$$

Were, Authorization Grant is a temporary credential provided by the user, Client Credentials are the client ID and secret used by the application, The Access Token is then used to authenticate and authorize the user to access protected healthcare data.

3.5. Cloud Storage

- With cloud storage, patient data is encrypted and stored largely in a secure, scalable, and centralized place. The great accessibility of data also makes it easy to manage data across all healthcare systems.
- Cloud storage can be integrated with OAuth-based authentication to impose strict access to stored patient data. Proper authenticated users would thus be able to access or modify the stored patient data, ensuring that patient-level security and privacy are upheld.
- Patients' data is replicated over multiple sites, which is a characteristic of cloud storage. In this way, data may be consistently recovered even in cases of hardware failure or system downtime.
- The cloud storage system is well capable of scaling dynamically to hold the patient data that continue growing constantly. It really means that the healthcare system can grow without involving in extensive infrastructure upgrading.
- Cloud storage ensures a secure method of retrieving data via encrypted communication channels whereby patient data is protected both at the time of storage and when accessing only authorized personnel when needed can bring forth the information.

4. RESULT

Increased security and efficiency in cloud healthcare systems are demonstrated in the results of the proposed framework. Integration of Triple DES encryption and use of OAuth authentication assures secure access control and strong data protection. It also provides scalability, offering cloud storage that is transforming hematology in terms of cloud storage and patients' private data, while scalability, reliability, and non-stop management are also some of the ways in which this approach offers a solution concerning the existing performance and security challenges.

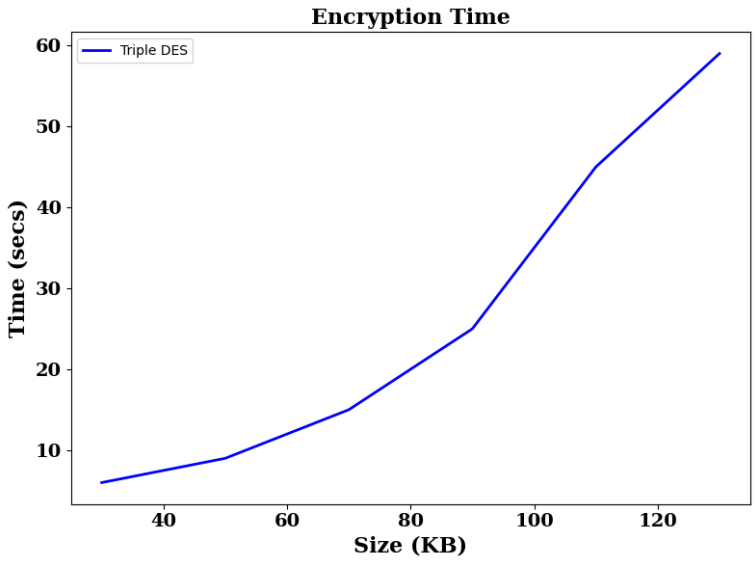

Figure 2: Triple DES Encryption Time

Figure 2 shows elapsed time on encrypting the Triple Data Encryption Standard as the data size increases about 20-30 seconds for every 500 kb to 4gb raise in size. At approximately 40 kb, it takes 10 seconds to encrypt, while it goes higher to about 55 seconds on 120 kb. Such behaviour clearly shows the computational cost of Triple Data Encryption Standard, as higher data size requires greater processing time, considering it is meant for large data systems that require that processing. The graph shows scalability and probably some performance limitations on the application of Triple Data Encryption Standard in practice.

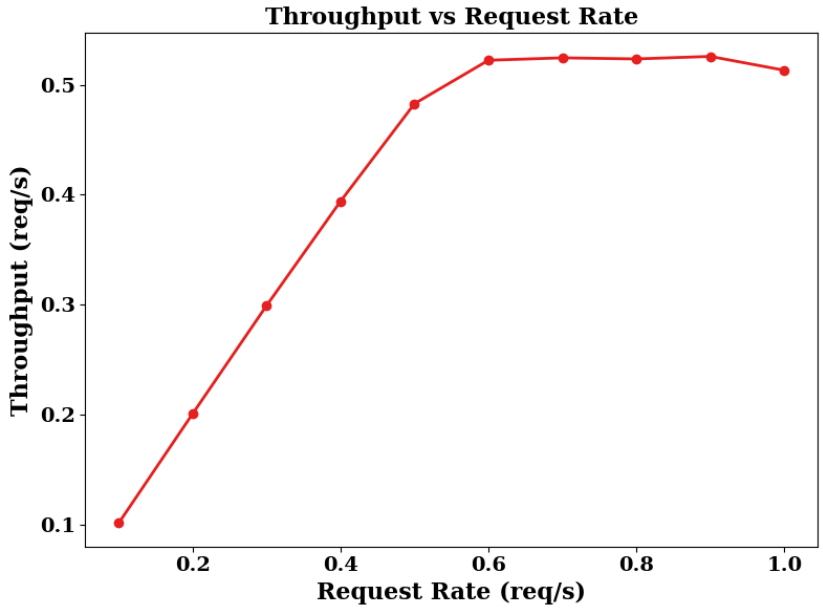

Figure 3: Throughput vs. Request Rate in Cloud-based Healthcare Systems

Figure 3 represents the relationship between throughput and request rate with interconnecting the data points. With an increase in the request rate, the throughput is maximum at around a request rate of 0.6 requests per second, where throughput is approximately 0.5 requests per second. Beyond this point, for request rates above 0.6, the throughput levelled off, implying no significant increase in throughput with an increased request rate. For instance, at a lower request rate of 0.1, throughput is approximately 0.1 requests per second, showing an increase as the request rate increases until reaching saturation at higher request rates. This behaviour, therefore, indicates the optimal request rate for maximum throughput just before pushing the system's limits.

5. CONCLUSION

The proposed framework features the enhanced security and management of sensitive healthcare data in cloud-based systems with Triple DES encryption and OAuth authentication. The use of Triple DES means more time is required for encryption with more data, as shown in Figure 2, while encryption time goes from about 10 seconds at 40 KB to 55 seconds at 120 KB, which is its cost of computation. On the other hand, according to Figure 3, throughput peaks at an even 0.5 req/s at a request rate of 0.6, which is then maintained, showing the performance limits of the system. The presented methodology thus guarantees strong data protection and access control, and the cloud storage availability for scalable and reliable data management. In the future, supporting blockchain integration for immutable storage of data and enabling real-time access could enforce further security and performance of the framework in large-scale healthcare systems.

REFERENCES

[1] Wu, L., Xue, L., Li, C., Lv, X., Chen, Z., Jiang, B., ... & Xie, Z. (2017). A knowledge-driven geospatially enabled framework for geological big data. *ISPRS International Journal of Geo-Information*, *6*(6), 166.
[2] Aydin, G., Hallac, I. R., & Karakus, B. (2015). Architecture and implementation of a scalable sensor data storage and analysis system using cloud computing and big data technologies. Journal of Sensors, 2015(1), 834217.
[3] Adjei, J. K. (2015). Explaining the role of trust in cloud computing services. *info*, *17*(1), 54-67.
[4] Zhao, R., Yan, R., Wang, J., & Mao, K. (2017). Learning to monitor machine health with convolutional bi-directional LSTM networks. *Sensors*, *17*(2), 273.
[5] Man, C. D., Micheletto, F., Lv, D., Breton, M., Kovatchev, B., & Cobelli, C. (2014). The UVA/PADOVA type 1 diabetes simulator: new features. *Journal of diabetes science and technology*, *8*(1), 26-34.
[6] 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.
[7] Patil, P., Narayankar, P., Narayan, D. G., & Meena, S. M. (2016). A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. *Procedia Computer Science*, *78*, 617-624.
[8] Sendor, J., Lehmann, Y., Serme, G., & de Oliveira, A. S. (2014, March). Platform-level support for authorization in cloud services with OAuth 2. In *2014 IEEE International Conference on Cloud Engineering* (pp. 458-465). IEEE.
[9] Iqbal, S., Kiah, M. L. M., Dhaghighi, B., Hussain, M., Khan, S., Khan, M. K., & Choo, K. K. R. (2016). On cloud security attacks: A taxonomy and intrusion detection and prevention as a service. *Journal of Network and Computer Applications*, *74*, 98-120.
[10] Konstantinou, C., Maniatakos, M., Saqib, F., Hu, S., Plusquellic, J., & Jin, Y. (2015, May). Cyber-physical systems: A security perspective. In *2015 20th IEEE European Test Symposium (ETS)* (pp. 1-8). IEEE.
[11] Kröger, F. (2016). Automated driving in its social, historical and cultural contexts. In *Autonomous driving: Technical, legal and social aspects* (pp. 41-68). Berlin, Heidelberg: Springer Berlin Heidelberg.
[12] Van Holt, T., Weisman, W., Johnson, J. C., Käll, S., Whalen, J., Spear, B., & Sousa, P. (2016). A social wellbeing in fisheries tool (SWIFT) to help improve fisheries performance. *Sustainability*, *8*(8), 667.
[13] Bader, A., Ghazzai, H., Kadri, A., & Alouini, M. S. (2016). Front-end intelligence for large-scale application-oriented internet-of-things. *IEEE Access*, *4*, 3257-3272.
[14] Chen, X., Xing, L., Qiu, T., & Li, Z. (2017). An auction-based spectrum leasing mechanism for mobile macro-femtocell networks of IoT. *Sensors*, *17*(2), 380.
[15] Edquist, C. (2013). CHAPTER ONE Systems of innovation approaches—Their emergence and characteristics. In *Systems of innovation* (pp. 1-35). Routledge.
[16] Patel, A., Taghavi, M., Bakhtiyari, K., & Júnior, J. C. (2013). An intrusion detection and prevention system in cloud computing: A systematic review. *Journal of network and computer applications*, *36*(1), 25-41.
[17] Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M., & Inácio, P. R. (2014). Security issues in cloud environments: a survey. *International journal of information security*, *13*, 113-170.
[18] Krallinger, M., Rabal, O., Lourenco, A., Oyarzabal, J., & Valencia, A. (2017). Information retrieval and text mining technologies for chemistry. *Chemical reviews*, *117*(12), 7673-7761.

[19] Wu, D., Pigou, L., Kindermans, P. J., Le, N. D. H., Shao, L., Dambre, J., & Odobez, J. M. (2016). Deep dynamic neural networks for multimodal gesture segmentation and recognition. *IEEE transactions on pattern analysis and machine intelligence*, *38*(8), 1583-1597.
[20] Aazam, M., & Huh, E. N. (2015, March). Fog computing micro datacenter based dynamic resource estimation and pricing model for IoT. In *2015 IEEE 29th international conference on advanced information networking and applications* (pp. 687-694). IEEE.
[21] Ward, J. S., & Barker, A. (2014). Observing the clouds: a survey and taxonomy of cloud monitoring. *Journal of Cloud Computing*, *3*, 1-30.
[22] Griebel, L., Prokosch, H. U., Köpcke, F., Toddenroth, D., Christoph, J., Leb, I., ... & Sedlmayr, M. (2015). A scoping review of cloud computing in healthcare. *BMC medical informatics and decision making*, *15*, 1-16.
[23] Anwar, S., Mohamad Zain, J., Zolkipli, M. F., Inayat, Z., Khan, S., Anthony, B., & Chang, V. (2017). From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions. *algorithms*, *10*(2), 39.
[24] Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information sciences*, *305*, 357-383.
[25] Tang, J., Cui, Y., Li, Q., Ren, K., Liu, J., & Buyya, R. (2016). Ensuring security and privacy preservation for cloud data services. *ACM Computing Surveys (CSUR)*, *49*(1), 1-39.