International Journal of Business Management and Economic Review

Vol. 2, No. 06; 2019

ISSN: 2581-4664

ENHANCING CLOUD SECURITY IN HEALTHCARE AND FINANCE: ZERO TRUST AND HOMOMORPHIC ENCRYPTION FOR DATA PRIVACY AND RISK MANAGEMENT

Karthik Kushala
Celer Systems Inc, Folsom, California, USA
karthik.kushala@gmail.com
Aravindhan Kurunthachalam
SNS College of Technology, Coimbatore, Tamil Nadu, India.
kurunthachalamaravindhan@gmail.com

http://doi.org/10.35409/IJBMER.2019.2133_1

ABSTRACT

Cloud security in healthcare and finance is crucial due to the increasing risks of cyber threats and data breaches. Traditional security models relying on perimeter-based defenses and conventional encryption techniques fail to ensure data confidentiality during processing. Zero Trust Architecture (ZTA) and Fully Homomorphic Encryption (FHE) present a robust approach to mitigating these security concerns. ZTA enforces strict access control through continuous authentication and least-privilege principles, ensuring that only authorized users can access sensitive data. Meanwhile, FHE enables computations on encrypted data without requiring decryption, eliminating exposure risks in untrusted cloud environments. However, challenges such as computational overhead and implementation complexity hinder the widespread adoption of FHE. This paper proposes an integrated security framework combining ZTA and FHE to enhance cloud security while optimizing performance for real-world applications. The proposed model ensures end-to-end encryption, regulatory compliance with standards like HIPAA and GDPR, and resilience against insider threats, unauthorized access, and data leaks. Experimental results demonstrate that integrating ZTA with FHE effectively secures sensitive transactions without compromising system usability. By implementing adaptive risk-based authentication and optimizing FHE computation efficiency, this approach provides a scalable and secure solution for healthcare and financial applications. Future research will focus on reducing the performance overhead of FHE and improving its integration with cloud-based AI-driven analytics.

Keywords: Cloud Security, Zero Trust Architecture, Fully Homomorphic Encryption, Risk Management, Multi-Factor Authentication, Financial Data Protection, One-Class Support Vector Machine.

1. INTRODUCTION

Cloud security in healthcare and finance is critical due to the sensitive nature of data involved [1]. With the increasing adoption of cloud computing, protecting patient records and financial transactions from cyber threats is a priority [2]. Organizations rely on cloud infrastructure for its scalability, but security risks like data breaches, unauthorized access, and insider threats persist [3]. Traditional security models often fail to address modern cyber threats, making advanced security frameworks necessary [4]. Encryption plays a key role in ensuring data

Vol. 2, No. 06; 2019
ISSN: 2581-4664

confidentiality, but conventional encryption methods require decryption for processing, exposing data to risks [5]. The need for secure computing has led to innovations such as FHE, which enables computations on encrypted data [6]. Additionally, the ZTA model eliminates implicit trust, ensuring continuous identity verification and strict access controls [7]. By integrating ZTA with FHE, organizations can achieve robust security while maintaining operational efficiency [8]. These technologies together protect against cyberattacks, ensuring compliance with regulations like HIPAA and GDPR [9]. Enhancing cloud security in healthcare and finance is not just a necessity but a fundamental requirement for maintaining trust and data integrity [10].

One major cause of cloud security issues is the increase in cyber threats targeting healthcare and financial institutions [11]. Weak access controls allow unauthorized users to exploit system vulnerabilities [12]. Insider threats from employees or third-party vendors pose a significant risk to sensitive data [13]. Phishing attacks trick users into revealing login credentials, leading to data breaches [14]. Insecure APIs in cloud applications can be exploited by attackers to gain access to critical systems [15]. Lack of encryption exposes sensitive data during transmission and storage [16]. Misconfigured cloud storage leads to unintentional data leaks [17]. Inadequate monitoring and auditing make it difficult to detect security incidents in real time [18]. Regulatory non-compliance increases the risk of legal consequences and financial penalties [19]. Dependence on third-party cloud providers introduces security challenges beyond an organization's control [20].

Existing cloud security methods in healthcare and finance primarily rely on traditional encryption and access control mechanisms, which have inherent weaknesses [21]. Symmetric and asymmetric encryption require decryption for data processing, exposing sensitive information during computation [22]. RBAC and MFA alone are insufficient, as attackers can exploit credential leaks and session hijacking [23]. Network firewalls and intrusion detection systems struggle with detecting APTs and zero-day attacks [24]. Current encryption models do not support secure computations, limiting the ability to perform analytics on encrypted data [25]. Data integrity and confidentiality become compromised when security policies are inconsistent across cloud environments [26]. Latency issues arise with complex cryptographic operations, making real-time processing inefficient [27]. Compliance with regulations like HIPAA and GDPR is challenging, as organizations must ensure end-to-end data security without compromising performance [28]. Centralized security models introduce single points of failure, making them vulnerable to targeted cyberattacks [29]. Scalability remains a concern, as increasing data volumes demand stronger security mechanisms without degrading system performance [30].

To address these security challenges, we propose integrating ZTA with FHE. ZTA eliminates implicit trust, ensuring that all users and devices are continuously authenticated before accessing cloud resources. Multi-Factor Authentication and continuous monitoring enhance access security, reducing unauthorized intrusions. FHE enables encrypted computations, ensuring that sensitive data never needs to be decrypted for processing. This prevents data exposure during computation, significantly reducing cyberattack risks. Combining ZTA with FHE provides end-to-end security, making it ideal for handling sensitive healthcare and financial data. Regulatory compliance is strengthened as data privacy is maintained even in multi-cloud environments. Performance optimization techniques help manage computation overhead in FHE for real-world applications. Risk-based authentication in ZTA ensures access control adapts dynamically based on risk levels. The proposed model enhances data security without compromising system usability, making cloud security more effective. By adopting this solution, organizations can achieve a

Vol. 2, No. 06; 2019
ISSN: 2581-4664

balance between security, performance, and compliance, ensuring long-term data protection.

In Section 2, Literature Review Explores existing methods and their limitations. Section 3 Identifies challenges Cloud Security in Healthcare and Finance for Risk Assessment. Section 4 the Proposed Methodology presents, Enhanced Cybersecurity Framework for Data Processing and Threat Detection, Section 5, Result and Discussions. While Section 6, Conclusion and Future Works.

2. LITERATURE REVIEW

Narla, S., & Kumar, R. L. (2018) proposed [31] E-Healthcare uses CSP for secure EPR management, employing Homomorphic Encryption, Blockchain, and ABAC for security and privacy. Challenges include encryption overhead, blockchain latency, and complex access control, requiring further optimization. A. Theodouli et al (2018) [32] utilized Existing research explores secure healthcare cloud storage, emphasizing confidentiality, access control, and regulatory compliance [33]. Various encryption techniques, including FHE with key delegation, have been proposed to enhance security [34]. However, challenges such as high computational complexity and latency limit, necessitating further optimization [35].

F. Alharbi et al (2016) [36] Studied highlight Cloud Computing in HIT for cost-effective healthcare. However, security and privacy challenges persist. Techniques like access control, FHE, and secure data sharing help mitigate risks. Yet, scalability, compliance, and data integrity remain key limitations. Srinivasan, K., & Arulkumaran, G. (2018) analysed [37] Wearable sensors generate big data in healthcare, requiring efficient processing [38]. The Meta Cloud-Redirection (MC-R) architecture ensures scalable storage and real-time analysis using key management security. However, challenges like data privacy, high costs, and secure transmission remain [39].

A. O'Driscoll et al (2013) proposed [40] Cloud computing provides scalable, cost-effective services for healthcare, improving data access and collaboration. Virtualization enables efficient resource sharing, but security risks, regulatory compliance, and provider dependency remain challenges. Mandala, R. R., & N, P. (2018) suggested [41] Cloud-based solutions enhance healthcare data management by enabling seamless interoperability and secure data exchange. A microservices-based architecture improves scalability and patient-centered services while ensuring privacy and security [42]. However, integration challenges, compliance with regulations, and potential cyber threats must be addressed for widespread adoption [43], [44].

3. PROBLEM STATEMENT

Despite advancements in secure healthcare cloud storage, challenges such as encryption overhead, blockchain latency, and complex access control hinder efficient Electronic Patient Record (EPR) management [45]. High computational complexity and latency in encryption techniques like Fully Homomorphic Encryption (FHE) require further optimization to balance security and performance [46], [47].

Additionally, scalability, regulatory compliance, and secure data sharing remain major concerns, limiting widespread cloud adoption in healthcare [48]. Addressing data privacy, provider dependency, and cyber threats is crucial to ensure a robust, cost-effective, and patient-centric healthcare cloud system [49].

4. ENHANCED CYBERSECURITY FRAMEWORK FOR DATA PROCESSING AND

Vol. 2, No. 06; 2019

ISSN: 2581-4664

THREAT DETECTION

The diagram represents a secure data processing framework for handling sensitive information, particularly in cybersecurity and healthcare applications. The process starts with data collection, where raw data is gathered from various sources. Next, data preprocessing using the Z-score method is employed for outlier detection, ensuring data integrity by identifying anomalies. Once the data is cleaned, identity verification through multi-factor authentication (MFA) is performed to restrict unauthorized access and enhance security is shown in Figure (1),

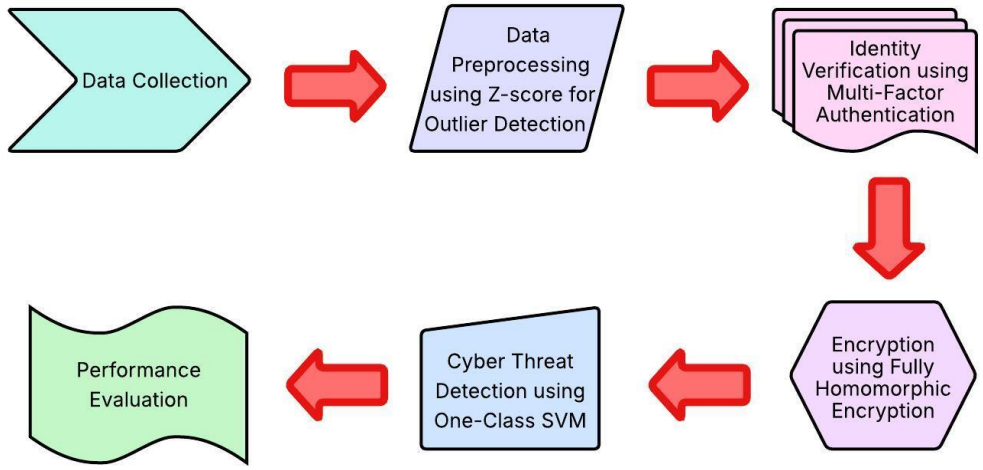

Figure 1: Secure Data Processing Framework with Anomaly Detection and Encryption

Following successful authentication, FHE is applied to secure the data while enabling computations on encrypted information without decryption, ensuring confidentiality. The encrypted data is then analyzed for cyber threat detection using a One-Class Support Vector Machine, a machine learning approach specialized in anomaly detection. Finally, a performance evaluation phase assesses the efficiency and accuracy of the entire system, ensuring its reliability and effectiveness. This framework integrates advanced security techniques to protect sensitive data while maintaining usability and performance.

4.1 Data Collection

The Enhanced Health Insurance Claims Dataset is a synthetic dataset of 4500 claims designed to simulate practical scenarios. It includes claim details, patient demographics, provider information, and medical data, making it ideal for machine learning, predictive modeling, fraud detection, and data analysis. Generated using the Faker library, it mimics actual claims while ensuring no real patient data is included.

Dataset Link: https://www.kaggle.com/datasets/leandrenash/enhanced-health-insurance-claims-dataset

4.2 Data Preprocessing using Z-score for Outlier Detection

Exploratory Data Analysis is the most critical step in analyzing the Enhanced Health Insurance Claims Dataset, as it uncovers hidden patterns, errors, and relationships before applying machine learning models. Without proper EDA, models may suffer from biases, poor performance, and unreliable predictions. Descriptive statistics such as mean μ, median, variance σ^2, and standard deviation σ help summarize the dataset is identified as Eq. (1) and Eq. (2),

$$\sigma^2 = \frac{1}{N}\sum_{i=1}^{N} (X_i - \mu)^2 \quad (1)$$

Vol. 2, No. 06; 2019
ISSN: 2581-4664

$$\sigma = \sqrt{\sigma^2} \quad (2)$$

Where, X_i is a data point, μ is the mean, and N is the number of data points. Visualization techniques, including histograms, box plots, and correlation heatmaps, help detect trends and relationships between variables. Outlier detection is crucial for identifying fraudulent claims, using methods such as the Z-score is mentioned as Eq. (3),

$$Z = \frac{X-\mu}{\sigma} \quad (3)$$

Where, an outlier is detected if |Z|>3. Another effective method is the Interquartile Range is indicated as Eq. (4),

$$IQR = Q3 - Q1 \quad (4)$$

Where, Q1 and Q3 are the 25th and 75th percentiles, respectively. Any value outside these bounds is considered an outlier. EDA helps in detecting missing values, finding correlations, and ensuring the dataset is ready for model training.

4.3 Identity Verification using Multi-Factor Authentication

In Zero Trust Architecture, identity verification plays a crucial role in ensuring secure access to healthcare and financial data, as no entity is trusted by default. Multi-Factor Authentication strengthens security by requiring users to authenticate using multiple factors: Knowledge Factor (password, PIN), Possession Factor (OTP, security token), and Inherence Factor (biometric authentication). A user is granted access only if at least two factors are valid, mathematically represented as Eq. (5)

$$A = f(K, P, I) \quad (5)$$

Where, the Eq. (6) is given below in

$$A = \begin{cases} 1, & \text{if at least two factors are valid} \\ 0, & \text{otherwise} \end{cases} \quad (6)$$

Alternatively, using a weighted function is given below in Eq. (7),

$$A = w_1 K + w_2 P + w_3 I \quad (7)$$

Where, w1, w2, w3 are the weights assigned to each authentication factor. Access is granted if Eq. (8),

$$A \geq T \quad (8)$$

Where, T is the threshold (e.g., T=2 for two-factor authentication). Risk-based authentication further enhances security by calculating a risk score R(x) considering factors such as login location (L), device trust score (D), and behavioral anomaly score (B) is mentioned as Eq. (9),

$$R(x) = \alpha L + \beta D + \gamma B \quad (9)$$

Where, α, β, γ are weight parameters. If the risk score exceeds a set threshold, additional authentication steps are required to mitigate potential security threats. This layered authentication approach significantly reduces the risks of unauthorized access, credential theft, and fraudulent

Vol. 2, No. 06; 2019
ISSN: 2581-4664

activities, ensuring secure data access in cloud environments.

4.4 Encryption using Fully Homomorphic Encryption

The Fully Homomorphic Encryption is implemented to ensure secure and private data processing in healthcare and financial applications. Unlike traditional encryption techniques, which require data to be decrypted before computation, FHE allows computations to be performed directly on encrypted data, ensuring that sensitive information remains confidential throughout processing. FHE employs Public-Key Encryption, where a message mmm is encrypted using a public key pk, producing ciphertext ccc, mathematically represented as Eq. (10),

$$c = E(m) \quad (10)$$

Where, E(m) is the encryption function. FHE supports essential mathematical operations, such as addition and multiplication, directly on encrypted data without requiring decryption. If two messages m_1 and m_2 are encrypted into ciphertexts $c_1=E(m_1)$ and $c_2=E(m_2)$ the encryption scheme satisfies is classified as Eq. (11),

$$E(m_1) \oplus E(m_2) = E(m_1 + m_2) \quad (11)$$

for addition is given below in Eq. (12),

$$E(m_1) \otimes E(m_2) = E(m_1 \times m_2) \quad (12)$$

In FHE, homomorphic addition ($\oplus$) and multiplication ($\otimes$) enable computations on encrypted data without decryption. However, repeated operations introduce noise, which may corrupt decryption. To prevent this, bootstrapping refreshes ciphertext to maintain accuracy. The FHE process starts by encrypting data before cloud storage, allowing computations in an encrypted state. The cloud server processes data without accessing plaintext, and the final encrypted result is decrypted using the private key, ensuring end-to-end security. This approach enables secure cloud computing, protects data confidentiality in healthcare and finance, and prevents cyber threats even in untrusted cloud environments.

4.5 Cyber Threat Detection using One-Class SVM

One-Class Support Vector Machine is an unsupervised learning technique used for cyber threat detection by identifying network anomalies. It works by learning the normal behavior of network traffic and flagging deviations as potential threats. Given a dataset of normal network traffic x_i, OC-SVM maps it to a high-dimensional space using a kernel function $\Phi(x)$ and finds an optimal hyperplane that separates most of the data while isolating anomalies. The optimization problem is formulated as mentioned in Eq. (13),

$$\min_{\omega,\rho} \frac{1}{2}\|\omega\|^2 + \frac{1}{\nu N}\sum_{i=1}^{N} \xi_i - \rho \quad (13)$$

subject to determine as Eq. (14),

$$\left(\omega \cdot \Phi(x_i)\right) \geq \rho - \xi_i, \xi_i \geq 0, \forall i \quad (14)$$

Where, ω is the normal vector, ρ is the decision threshold, ξ_i are slack variables, and ν controls the fraction of anomalies. New observations x^* are classified based on the decision function as classified as Eq. (15),

Vol. 2, No. 06; 2019
ISSN: 2581-4664

$$f(x^*) = \left(\omega \cdot \Phi(x^*)\right) - \rho \quad (15)$$

Where, if f(x*) ≥0, the data is normal; otherwise, it is flagged as an anomaly. The method effectively detects zero-day attacks and unknown threats but may have high false positives. The final outcome is a secure network system that continuously monitors and detects cyber threats.

5. RESULTS AND DISCUSSION

This section evaluates anomaly detection and encryption efficiency. ADR trends show fluctuations, requiring optimization for consistent accuracy. Encryption time remains higher than decryption, emphasizing the need for efficient cryptographic techniques. These insights aid in enhancing security and performance in cloud-based systems.

5.1 Analysis of Anomaly Detection Rate Variations for Improved System Performance

The graph illustrates the Anomaly Detection Rate (ADR) (%) against the Total Anomalies Present, showing how effectively the system identifies anomalies. Initially, with around 60 anomalies, the ADR is high at 91%, indicating strong detection. However, as anomalies increase, the detection rate declines, reaching its lowest point at 120 anomalies (~83%), likely due to overlapping patterns and increased false negatives is displayed in Figure (2),

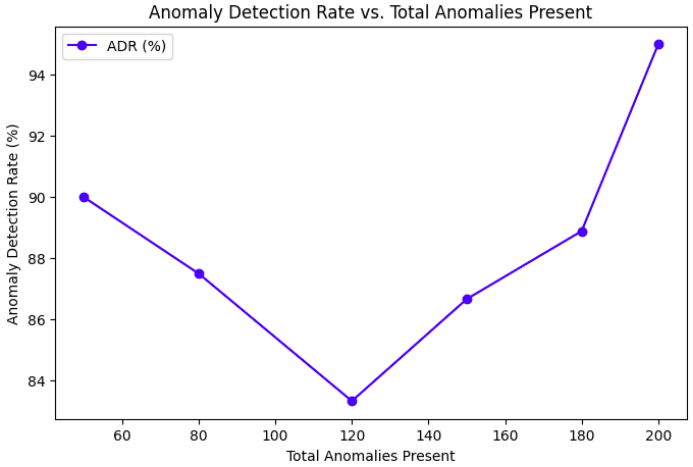

Figure 2: Evaluating Anomaly Detection Rate Trends for Enhanced Security and Accuracy

Beyond 120 anomalies, the ADR improves, reaching 94% at 200 anomalies, suggesting the system adapts better at higher anomaly levels. This fluctuation highlights potential inefficiencies, requiring optimization to maintain consistent accuracy. Possible improvements include better feature selection, hyperparameter tuning, and hybrid detection techniques to enhance stability and performance across different anomaly levels.

5.2 Analysis of Encryption and Decryption Time Based on Data Size

The graph illustrates the relationship between encryption and decryption time concerning data size. As the data size increases, both encryption and decryption times exhibit a nearly linear growth, highlighting the computational cost associated with securing larger datasets. The encryption time (represented by the green line) is consistently higher than the decryption time (represented by the orange line), indicating that encrypting data requires more processing power compared to decrypting it is shown in Figure (3),

Vol. 2, No. 06; 2019
ISSN: 2581-4664

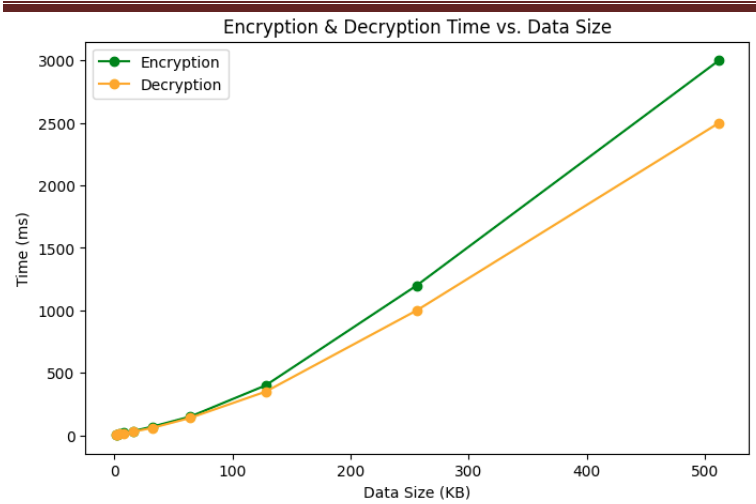

Figure 3: Evaluating Encryption and Decryption Efficiency Across Varying Data Sizes

This difference is likely due to the complexity of encryption algorithms, which involve key generation and multiple transformations to secure the data, whereas decryption follows a relatively simpler process to retrieve the original content. The observed trend emphasizes the need for optimizing cryptographic algorithms, especially for large-scale applications in cloud storage and secure communications, to enhance efficiency without compromising security.

6. CONCLUSION AND FUTURE WORKS

This paper presented a ZTA and FHE approach to enhance cloud security in healthcare and finance. ZTA ensures continuous identity verification and dynamic access control, preventing unauthorized access, while FHE enables secure computations on encrypted data. This combined approach strengthens data confidentiality, integrity, and availability, ensuring compliance with HIPAA, GDPR, and PCI-DSS. Although FHE introduces computational overhead, it remains a viable solution for secure cloud computing. The proposed model effectively mitigates cyber threats and insider attacks while maintaining regulatory compliance.

Future research should focus on optimizing FHE performance to reduce computational overhead and improve efficiency. AI-driven risk-based authentication can enhance security by dynamically adjusting access controls based on user behavior. Exploring post-quantum cryptography will help safeguard encrypted data against emerging threats. Additionally, secure key management strategies must be improved for large-scale cloud deployments. Further studies should assess the real-world implementation of ZTA and FHE, ensuring scalability and practicality. Finally, AI-powered security analytics can enhance anomaly detection and cyber threat prediction, strengthening cloud security frameworks.

REFERENCES

[1] Grandhi, S. H., & Padmavathy, R (2018). Federated learning-based real-time seizure detection using IoT-enabled edge AI for privacy-preserving healthcare monitoring. International Journal of Research in Engineering Technology, 3(1).

[2] G. Suciu et al., “Big Data, Internet of Things and Cloud Convergence – An Architecture for Secure E-Health Applications,” J Med Syst, vol. 39, no. 11, p. 141, Nov. 2015, doi: 10.1007/s10916-015-0327-y.

Vol. 2, No. 06; 2019

ISSN: 2581-4664

[3] Chetlapalli, H., & Bharathidasan, S. (2018). AI-BASED CLASSIFICATION AND DETECTION OF BRAIN TUMORS IN HEALTHCARE IMAGING DATA. International Journal of Life Sciences Biotechnology and Pharma Sciences, 14(2), 18-26.

[4] H. Kupwade Patil and R. Seshadri, "Big Data Security and Privacy Issues in Healthcare," in 2014 IEEE International Congress on Big Data, Anchorage, AK: IEEE, Jun. 2014, pp. 762–765. doi: 10.1109/BigData.Congress.2014.112.

[5] Mamidala, V., & Balachander, J. (2018). AI-driven software-defined cloud computing: A reinforcement learning approach for autonomous resource management and optimization. International Journal of Engineering Research and Science & Technology, 14(3).

[6] S. Alshehri, S. P. Radziszowski, and R. K. Raj, "Secure Access for Healthcare Data in the Cloud Using Ciphertext-Policy Attribute-Based Encryption," in 2012 IEEE 28th International Conference on Data Engineering Workshops, Arlington, VA, USA: IEEE, Apr. 2012, pp. 143–146. doi: 10.1109/ICDEW.2012.68.

[7] Gaius Yallamelli, A. R., & Prasaath, V. R. (2018). AI-enhanced cloud computing for optimized healthcare information systems and resource management using reinforcement learning. International Journal of Information Technology and Computer Engineering, 6(3).

[8] Md. M. Islam, Md. A. Razzaque, M. M. Hassan, W. N. Ismail, and B. Song, "Mobile Cloud-Based Big Healthcare Data Processing in Smart Cities," IEEE Access, vol. 5, pp. 11887–11899, 2017, doi: 10.1109/ACCESS.2017.2707439.

[9] Gattupalli, K., & Lakshmana Kumar, R. (2018). Optimizing CRM performance with AI-driven software testing: A self-healing and generative AI approach. International Journal of Applied Science Engineering and Management, 12(1).

[10] L. A. Tawalbeh, R. Mehmood, E. Benkhlifa, and H. Song, "Mobile Cloud Computing Model and Big Data Analysis for Healthcare Applications," IEEE Access, vol. 4, pp. 6171–6180, 2016, doi: 10.1109/ACCESS.2016.2613278.

[11] Yalla, R. K. M. K., & Prema, R. (2018). ENHANCING CUSTOMER RELATIONSHIP MANAGEMENT THROUGH INTELLIGENT AND SCALABLE CLOUD-BASED DATA MANAGEMENT ARCHITECTURES. International Journal of HRM and Organizational Behavior, 6(2), 1-7.

[12] S. Rallapalli, R. R. Gondkar, and U. P. K. Ketavarapu, "Impact of Processing and Analyzing Healthcare Big Data on Cloud Computing Environment by Implementing Hadoop Cluster," Procedia Computer Science, vol. 85, pp. 16–22, 2016, doi: 10.1016/j.procs.2016.05.171.

[13] Dyavani, N. R., & Rathna, S. (2018). Real-Time Path Optimization for Autonomous Farming Using ANFTAPP and IoV-Driven Hex Grid Mapping. International Journal of Advances in Agricultural Science and Technology, 5(3), 86-94.

[14] V. Chang and M. Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework," IEEE Trans. Serv. Comput., vol. 9, no. 1, pp. 138–151, Jan. 2016, doi: 10.1109/TSC.2015.2491281.

[15] Sitaraman, S. R., & Pushpakumar, R. (2018). Secure data collection and storage for IoT devices using elliptic curve cryptography and cloud integration. International Journal of Engineering Research and Science & Technology. 14(4).

Vol. 2, No. 06; 2019

ISSN: 2581-4664

[16] N. J. King and V. T. Raja, "Protecting the privacy and security of sensitive customer data in the cloud," Computer Law & Security Review, vol. 28, no. 3, pp. 308–319, Jun. 2012, doi: 10.1016/j.clsr.2012.03.003.

[17] Ganesan, T., & Hemnath, R. (2018). Lightweight AI for smart home security: IoT sensor-based automated botnet detection. International Journal of Engineering Research and Science & Technology. 14(1).

[18] M. Ramachandran, "Software security requirements management as an emerging cloud computing service," International Journal of Information Management, vol. 36, no. 4, pp. 580–590, Aug. 2016, doi: 10.1016/j.ijinfomgt.2016.03.008.

[19] Devarajan, M. V. (2018). AI-Powered Personalized Recommendation Systems for E-Commerce Platforms. International Journal of Marketing Management, 6(1), 1-8.

[20] A. Kumari, S. Tanwar, S. Tyagi, and N. Kumar, "Fog computing for Healthcare 4.0 environment: Opportunities and challenges," Computers & Electrical Engineering, vol. 72, pp. 1–13, Nov. 2018, doi: 10.1016/j.compeleceng.2018.08.015.

[21] Deevi, D. P., & Jayanthi, S. (2018). Scalable Medical Image Analysis Using CNNs and DFS with Data Sharding for Efficient Processing. International Journal of Life Sciences Biotechnology and Pharma Sciences, 14(1), 16-22.

[22] Tripathi and A. Mishra, "Cloud computing security considerations," in 2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), Xi'an, Shaanxi, China: IEEE, Sep. 2011, pp. 1–5. doi: 10.1109/ICSPCC.2011.6061557.

[23] Gudivaka, R. K., & Rathna, S. (2018). Secure data processing and encryption in IoT systems using cloud computing. International Journal of Engineering Research and Science & Technology, 14(1).

[24] M. Hassanalieragh et al., "Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-Based Processing: Opportunities and Challenges," in 2015 IEEE International Conference on Services Computing, New York City, NY, USA: IEEE, Jun. 2015, pp. 285–292. doi: 10.1109/SCC.2015.47.

[25] Panga, N. K. R. (2018). ENHANCING CUSTOMER PERSONALIZATION IN HEALTH INSURANCE PLANS USING VAE-LSTM AND PREDICTIVE ANALYTICS. International Journal of HRM and Organizational Behavior, 6(4), 12-19.

[26] Z. Jin and Y. Chen, "Telemedicine in the Cloud Era: Prospects and Challenges," IEEE Pervasive Comput., vol. 14, no. 1, pp. 54–61, Jan. 2015, doi: 10.1109/MPRV.2015.19.

[27] Peddi, S., & Aiswarya, RS. (2018). Securing healthcare in cloud-based storage for protecting sensitive patient data. International Journal of Information Technology and Computer Engineering, 6(1)

[28] M. Fazio, A. Celesti, F. G. Marquez, A. Glikson, and M. Villari, "Exploiting the FIWARE cloud platform to develop a remote patient monitoring system," in 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca: IEEE, Jul. 2015, pp. 264–270. doi: 10.1109/ISCC.2015.7405526.

[29] Kodadi, S., & Kumar, V. (2018). Lightweight deep learning for efficient bug prediction in software development and cloud-based code analysis. International Journal of Information Technology and Computer Engineering, 6(1).

Vol. 2, No. 06; 2019

ISSN: 2581-4664

[30] J. Ryoo, S. Rizvi, W. Aiken, and J. Kissell, "Cloud Security Auditing: Challenges and Emerging Approaches," IEEE Secur. Privacy, vol. 12, no. 6, pp. 68–74, Nov. 2014, doi: 10.1109/MSP.2013.132.

[31] Narla, S., & Kumar, R. L. (2018). Privacy-Preserving Personalized Healthcare Data in Cloud Environments via Secure Multi-Party Computation and Gradient Descent Optimization. Chinese Traditional Medicine Journal, 1(2), 13-19.

[32] A. Theodouli, S. Arakliotis, K. Moschou, K. Votis, and D. Tzovaras, "On the Design of a Blockchain-Based System to Facilitate Healthcare Data Sharing," in 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA: IEEE, Aug. 2018, pp. 1374–1379. doi: 10.1109/TrustCom/BigDataSE.2018.00190.

[33] Alavilli, S. K., & Pushpakumar, R. (2018). Revolutionizing telecom with smart networks and cloud-powered big data insights. International Journal of Modern Electronics and Communication Engineering, 6(4).

[34] M. A. Sahi et al., "Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions," IEEE Access, vol. 6, pp. 464–478, 2018, doi: 10.1109/ACCESS.2017.2767561.

[35] Nagarajan, H., & Kurunthachalam, A. (2018). Optimizing database management for big data in cloud environments. International Journal of Modern Electronics and Communication Engineering, 6(1).

[36] F. Alharbi, A. Atkins, and C. Stanier, "Understanding the determinants of Cloud Computing adoption in Saudi healthcare organisations," Complex Intell. Syst., vol. 2, no. 3, pp. 155–171, Oct. 2016, doi: 10.1007/s40747-016-0021-9.

[37] Srinivasan, K., & Arulkumaran, G. (2018). LSTM-based threat detection in healthcare: A cloud-native security framework using Azure services. International Journal of Modern Electronics and Communication Engineering, 6(2)

[38] J. Hanen, Z. Kechaou, and M. B. Ayed, "An enhanced healthcare system in mobile cloud computing environment," Vietnam J Comput Sci, vol. 3, no. 4, pp. 267–277, Nov. 2016, doi: 10.1007/s40595-016-0076-y.

[39] Musam, V. S., & Kumar, V. (2018). Cloud-enabled federated learning with graph neural networks for privacy-preserving financial fraud detection. Journal of Science and Technology, 3(1).

[40] A. O'Driscoll, J. Daugelaite, and R. D. Sleator, "'Big data', Hadoop and cloud computing in genomics," Journal of Biomedical Informatics, vol. 46, no. 5, pp. 774–781, Oct. 2013, doi: 10.1016/j.jbi.2013.07.001.

[41] Mandala, R. R., & N, P. (2018). Optimizing secure cloud-enabled telemedicine system using LSTM with stochastic gradient descent. Journal of Science and Technology, 3(2).

[42] Y. Wang, L. Kung, and T. A. Byrd, "Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations," Technological Forecasting and Social Change, vol. 126, pp. 3–13, Jan. 2018, doi: 10.1016/j.techfore.2015.12.019.

[43] Kethu, S. S., & Thanjaivadivel, M. (2018). SECURE CLOUD-BASED CRM DATA MANAGEMENT USING AES ENCRYPTION/DECRYPTION. International Journal of HRM and Organizational Behavior, 6(3), 1-7.

Vol. 2, No. 06; 2019

ISSN: 2581-4664

[44] P. Gupta, A. Seetharaman, and J. R. Raj, "The usage and adoption of cloud computing by small and medium businesses," International Journal of Information Management, vol. 33, no. 5, pp. 861–874, Oct. 2013, doi: 10.1016/j.ijinfomgt.2013.07.001.

[45] Budda, R., & Pushpakumar, R. (2018). Cloud Computing in Healthcare for Enhancing Patient Care and Efficiency. Chinese Traditional Medicine Journal, 1(3), 10-15.

[46] J. Haskew et al., "Implementation of a cloud-based electronic medical record for maternal and child health in rural Kenya," International Journal of Medical Informatics, vol. 84, no. 5, pp. 349–354, May 2015, doi: 10.1016/j.ijmedinf.2015.01.005.

[47] Subramanyam, B., & Mekala, R. (2018). Leveraging cloud-based machine learning techniques for fraud detection in e-commerce financial transactions. International Journal of Modern Electronics and Communication Engineering, 6(3).

[48] S. Amofa et al., "A Blockchain-based Architecture Framework for Secure Sharing of Personal Health Data," in 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), Ostrava: IEEE, Sep. 2018, pp. 1–6. doi: 10.1109/HealthCom.2018.8531160.

[49] Radhakrishnan, P., & Mekala, R. (2018). AI-Powered Cloud Commerce: Enhancing Personalization and Dynamic Pricing Strategies. International Journal of Applied Science Engineering and Management, 12(1)