International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Ensuring Healthcare Data Security in Cloud Systems with IOT Device Integration and Encryption

[1*]Visrutatma Rao Vallu, [2]Winner Pulakhandam, [3]Archana Chaluvadi and [4]G. Arulkumaran

[1]Spectrosys, Woburn, Massachusetts, USA
[2]Personify Inc, Texas, USA
[3]Massachusetts Mutual Life Insurance Company, Massachusetts, USA
[4]Bule Hora University: Bule Hora, Oromia, ET,

Received 18 July 2022, Accepted 10 Aug 2022, Available online 15 Aug 2022, **Vol.12, No.4 (July/Aug 2022)**

Abstract

The integration of Internet of Things (IoT) devices in healthcare systems has significantly enhanced patient monitoring and data collection. However, existing solutions often fail to address critical issues such as scalability, high computational overhead, and inadequate security in resource-constrained environments like IoT devices. This paper proposes a framework designed to ensure the security of healthcare data in cloud systems by integrating IoT devices with advanced encryption techniques. The workflow begins with gathering healthcare data from IoT devices such as wearable health monitors and medical sensors. This collected data is then passed to the IoT Integration block, which ensures smooth communication between the IoT devices and the cloud platform. Following this, the data is encrypted using Blowfish encryption to ensure its confidentiality and security during both transmission and storage. The encrypted data is then sent to Cloud Storage, where it is securely stored in cloud databases. In parallel, Multi-Factor Authentication (MFA) is applied to verify the identity of users before granting access to sensitive data. The performance evaluation of the proposed framework reveals that the average encryption time for a dataset size of 10 arbitrary units is 0.27 seconds, while the maximum latency time is 0.37 seconds. These results demonstrate the efficiency and scalability of the framework, providing a secure and robust solution for managing healthcare data in IoT-enabled environments.

Keywords: *IoT (Internet of Things) Integration, Healthcare Data Security, Blowfish Encryption, Multi-Factor Authentication and Cloud Storage.*

1. Introduction

The increasing integration of Internet of Things (IoT) devices in healthcare systems has revolutionized data collection and monitoring, offering numerous benefits in patient care [1]. However, with the growing volume of sensitive healthcare data being transmitted and stored, ensuring the security and privacy of this data becomes a critical concern [2]. Healthcare data, especially when stored in cloud systems, needs to be protected from cyber threats such as unauthorized access, data breaches, and cyber-attacks [3]. The proposed framework aims to address these security challenges by integrating IoT devices with cloud systems, incorporating strong encryption mechanisms like Blowfish and secure authentication protocols, ensuring healthcare data is protected throughout its lifecycle [4].

Existing methods in healthcare data security primarily focus on encryption techniques, access control, and cloud storage security [5]. Techniques such as AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), and homomorphic encryption are commonly used for data protection [6]. While these methods provide a level of security, they often suffer from issues such as high computational overhead, limited scalability, and vulnerability to specific types of attacks [7]. Moreover, traditional authentication mechanisms like passwords and basic encryption are insufficient in protecting sensitive health data, leading to potential risks in terms of data privacy and unauthorized access [8].

The significance of using this framework lies in its ability to address the increasing security concerns surrounding healthcare data in cloud systems [9]. As healthcare data becomes more critical and widely shared across cloud platforms and IoT devices, safeguarding sensitive information from cyber threats is of utmost importance [10]. By ensuring secure transmission, storage, and access control, this

*Corresponding author's ORCID ID: :0000-0000-0000-0000
DOI: https://doi.org/10.14741/ijcet/v.12.4.10

framework aims to protect patient privacy, reduce the risks of data breaches, and mitigate potential misuse of healthcare data [11]. The integration of secure communication protocols and authentication methods enhances the reliability of healthcare systems, providing peace of mind for both patients and healthcare providers [12]. This approach is vital for fostering trust in digital health solutions, paving the way for more efficient, secure, and reliable healthcare services [13].

The proposed framework is significant in addressing the escalating security challenges faced by healthcare data in cloud environments [14]. As healthcare information increasingly circulates across interconnected cloud platforms and IoT devices, protecting this sensitive data from cyber threats becomes paramount [15]. By implementing robust mechanisms for secure data transmission, storage, and stringent access control, the framework ensures patient privacy is maintained and the risks of data breaches or misuse are minimized [16]. Furthermore, the integration of advanced communication protocols and strong authentication methods enhances the overall trustworthiness and reliability of healthcare systems [17], [18]. This comprehensive security approach not only safeguards critical health information but also fosters confidence among patients and providers, thereby promoting wider adoption of digital health technologies and enabling more secure, efficient, and dependable healthcare services [19].

The paper is organized as follows: Section 2 provides a literature review of related works and challenges [20]. Section 3 explains the proposed methodology [21]. Section 4 presents experimental results [22], and Section 5 concludes with findings and future research directions [23].

2. Literature Survey

The increasing reliance on cloud computing frameworks in healthcare systems, emphasizing the need for robust encryption techniques to secure sensitive health data [24]. The study highlighted that traditional security measures were insufficient in addressing the vulnerabilities posed by the rapid adoption of IoT devices in healthcare [25]. Integrating advanced encryption algorithms and secure communication protocols was necessary to ensure comprehensive data protection in cloud-based healthcare systems [26]. The research stressed the importance of enhancing cloud security to keep pace with evolving technological challenges [27]. It proposed a more holistic approach to safeguard sensitive health data across all stages of data transmission and storage [28]. This study laid the foundation for understanding the gaps in existing cloud security measures [29].

The challenges of integrating IoT devices with cloud computing in healthcare, particularly focusing on data privacy and integrity [30]. The paper noted that while encryption methods like AES and RSA were widely adopted, they suffered from high computational complexity, which hindered their effectiveness in resource-constrained IoT environments [31]. More efficient encryption techniques were needed to improve security without compromising performance [32]. The study suggested that lightweight security mechanisms could address these limitations [33]. It recommended exploring alternative encryption solutions that could optimize performance for IoT devices in healthcare systems [34]. This highlighted the need for security solutions tailored to IoT-specific challenges [35].

The performance of various encryption algorithms in IoT-based healthcare systems, emphasizing the limitations of traditional methods like RSA and AES [36]. The research found that these algorithms were not well-suited for resource-constrained IoT devices due to their high computational cost [37]. Jadon proposed alternative encryption methods, such as Blowfish, which offered faster encryption and lower resource consumption while maintaining a high level of security [38]. The study demonstrated that optimized encryption techniques could provide sufficient security without overburdening IoT devices [39]. It encouraged further exploration of lightweight encryption algorithms that could be effectively implemented in healthcare IoT environments [40]. The findings were instrumental in identifying more suitable encryption methods for IoT-based healthcare systems [41].

The importance of secure authentication mechanisms for IoT-based healthcare systems [42]. The paper pointed out that conventional authentication methods were inadequate for securing access to sensitive healthcare data, especially when dealing with a large number of devices [43]. The use of Multi-Factor Authentication (MFA) as a more robust solution to enhance security [44]. The study demonstrated that combining MFA with secure encryption techniques would significantly strengthen the overall security of healthcare cloud systems [45]. It highlighted the need for more advanced authentication protocols to protect sensitive data from unauthorized access [46].

The challenges of ensuring data security in healthcare systems, particularly regarding the integration of IoT devices with cloud environments [47]. The research stressed the importance of end-to-end encryption and strong access control mechanisms to protect patient data [48]. Findings reinforced the need for reliable data transmission protocols and robust encryption algorithms in healthcare systems [49]. The study emphasized that combining effective encryption with secure authentication was essential to mitigate the risks of data breaches and unauthorized access [50]. It also suggested that healthcare systems should prioritize the adoption of advanced security frameworks to maintain the integrity and confidentiality of patient information [51]. This research highlighted the growing demand for comprehensive security solutions in healthcare IoT systems [52].

2.1 Problem Statement

Although significant progress has been made in securing healthcare data through IoT integration, several challenges remain unresolved [53]. These challenges include scalability issues and high computational overhead. Scalability problems arise when handling an increasing number of IoT devices and vast amounts of healthcare data, which strain the system's ability to efficiently manage and process information [54]. High computational overhead, particularly with traditional encryption methods like AES and RSA, puts a heavy load on IoT devices, leading to slower processing and delayed data analysis [55]. The work is proposed to overcome these challenges by incorporating lightweight encryption techniques and developing a scalable cloud infrastructure to optimize both performance and security in healthcare data management [56]. Despite advances in securing healthcare data via IoT integration, key challenges such as scalability and high computational overhead persist [57]. Managing a growing number of IoT devices and large volumes of data often overwhelms system resources, impacting efficient processing [58]. Traditional encryption algorithms like AES and RSA impose significant computational demands on resource-constrained IoT devices, causing slower performance and delays in data analysis [59]. To address these issues, the proposed work focuses on implementing lightweight encryption methods alongside a scalable cloud infrastructure [60]. aiming to enhance both security and system efficiency in healthcare data management [61].

3. Methodologies

The methodology begins with gathering healthcare data from IoT devices such as wearable health monitors and medical sensors. This collected data is then passed to the IoT Integration block, which ensures smooth communication between the IoT devices and the cloud platform. Following this, the data is encrypted using Blowfish encryption to ensure its confidentiality and security during both transmission and storage.

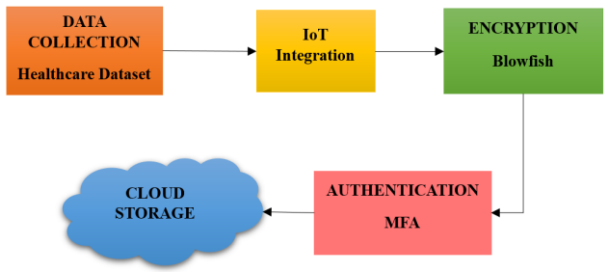

Figure 1: Block Diagram of Healthcare Data Security Framework

The encrypted data is then sent to Cloud Storage, where it is securely stored in cloud databases. In parallel, Authentication is applied to verify the identity of users before granting access to the sensitive data. This multi-layered approach ensures both data protection and regulated access, safeguarding healthcare information throughout its lifecycle. This process is visualized in Figure 1.

3.1 Data Collection

Gathering data from IoT devices, such as wearable health monitors and medical sensors, is a key component of the proposed framework. These devices track vital health parameters, including heart rate, blood pressure, oxygen levels, and body temperature. The collected data is transmitted to a centralized cloud platform for processing and storage. The data collection process ensures that accurate and up-to-date health information is gathered consistently. This enables healthcare professionals to access reliable patient information for analysis and decision-making.

3.2 IoT Integration

Following data collection, IoT integration involves connecting the collected data from wearable health monitors and medical sensors to the cloud platform for centralized processing. The IoT devices are seamlessly integrated with the cloud infrastructure, enabling continuous data transmission. Secure communication protocols, are used to ensure that data is transmitted safely between the devices and the cloud. This integration allows for efficient data flow, reducing latency and ensuring that healthcare professionals can access the data from any location. It ensures scalability, as more IoT devices can be added without disrupting the overall system. This connection enhances the overall healthcare system's ability to manage and analyze patient data effectively.

3.3 Encryption

After IoT integration, encryption ensures that the collected healthcare data is securely protected during transmission and storage. Sensitive data, such as patient health metrics, is encrypted using the Blowfish encryption algorithm, providing strong security while maintaining low computational overhead. This encryption ensures that even if data is intercepted during transmission, it remains unreadable to unauthorized parties. The encrypted data is stored securely in cloud databases, preventing potential breaches. The encryption process is seamless and transparent to users, ensuring data confidentiality without compromising system performance. By using encryption, the system safeguards patient privacy and meets regulatory standards for data protection.

Round Function Formula is expressed as equation (1),

$$R_{i+1} = L_i \oplus F(R_i, P_i) \quad (1)$$

In each round of the Blowfish encryption algorithm, the right half of the data (R) from the previous round is processed by the function F, which takes the current right half R_i and the current subkey P_i as inputs. The function F performs a series of substitutions and permutations using the S-boxes and P-array. The result of this function is then XORed with the left half L_i of the data from the current round to generate the new right half R_{i+1}.

Final XOR Formula is represented as equation (2),

$$\text{Ciphertext} = L_{16} \| R_{16} \quad (2)$$

After 16 rounds of processing, the final left half L_{16} and the final right half R_{16} are concatenated to form the complete 64-bit ciphertext. The symbol "parallel" (|) represents the concatenation of the two 32 -bit halves to produce the 64 -bit encrypted result. This final ciphertext is the encrypted version of the original plaintext data.

3.4 Authentication

The encrypted data is protected by Multi-Factor Authentication (MFA) to further secure access to sensitive healthcare information. MFA requires users to provide multiple forms of verification before accessing the encrypted data, ensuring that only authorized individuals can retrieve the information. Typically, this involves a combination of something the user knows (e.g., a password), something the user has (e.g., a mobile device or authentication token), and something the user is (e.g., biometric data). By requiring these multiple verification steps, MFA reduces the risk of unauthorized access, even if one form of authentication is compromised. This additional layer of security ensures that only trusted healthcare professionals can interact with the encrypted data. MFA significantly strengthens the protection of healthcare data from potential breaches.

3.5 Cloud Storage

After successful authentication through Multi-Factor Authentication (MFA), the encrypted data is securely stored in the cloud. The cloud storage system ensures that the data remains protected using advanced security measures such as encrypted databases and secure data centers. Access to this stored data is restricted based on user roles, ensuring that only authorized personnel can retrieve or modify the information. The cloud platform also provides scalability, allowing for the storage of large volumes of healthcare data while maintaining security and compliance with regulations. Continuous monitoring is performed to detect any unusual access patterns or potential security breaches. This secure cloud storage enables reliable data availability while safeguarding patient privacy and confidentiality.

4. Results

The results of the proposed framework are evaluated based on encryption time and latency time as the data size increases. The analysis reveals how encryption time and latency scale with data volume, providing insights into the efficiency and performance of Blowfish encryption. These results highlight the scalability of the encryption process in IoT environments and the need for optimization techniques as data size grows.

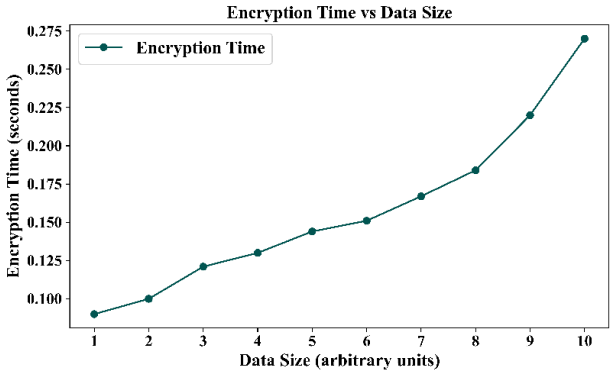

Figure 2: Encryption time for Blowfish

Figure 2 illustrates the relationship between encryption time and data size for Blowfish encryption. As the data size increases from 1 to 10 arbitrary units, the encryption time steadily increases, starting at 0.09 seconds and rising to 0.27 seconds. This demonstrates that Blowfish encryption time is proportional to the data size, with a consistent rise as the data volume increases. This trend is typical for symmetric encryption algorithms like Blowfish, where larger data requires more processing time. The results highlight the scalability of Blowfish encryption, and suggest that it is efficient for small to medium-sized datasets but may require optimization techniques for larger datasets in IoT environments.

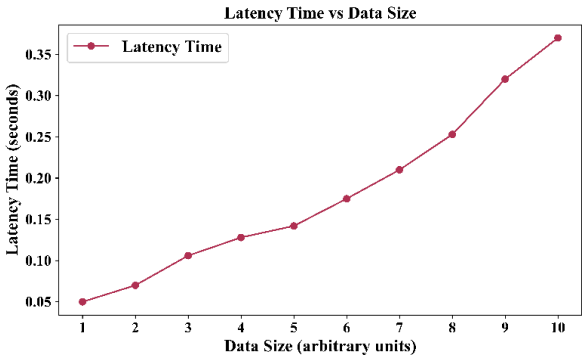

Figure 3: Latency time

Figure 2 illustrates the relationship between latency time and data size for Blowfish encryption. As the data size increases from 1 to 10 arbitrary units, the latency time rises from 0.05 seconds to 0.37 seconds. This

demonstrates that latency time scales with data size, indicating that larger datasets require more time to be processed. The graph reflects how the system's processing and transmission time increase as the volume of data grows. It highlights that Blowfish encryption, while efficient, results in higher latency as the data size increases, necessitating optimization techniques for handling larger datasets effectively.

Conclusions

This paper aims to ensure the security of healthcare data in cloud systems by integrating IoT devices with advanced encryption techniques. The proposed framework enhances the protection of patient information while ensuring efficient and secure data access and transmission. The performance evaluation of the framework shows that the average encryption time for a dataset size of 10 arbitrary units is 0.27 seconds, and the maximum latency time is 0.37 seconds. These results indicate the framework's scalability and efficiency, providing a secure method to manage large healthcare datasets while maintaining high levels of security. The implementation of Blowfish encryption and Multi-Factor Authentication (MFA) ensures both data confidentiality and access control, addressing critical challenges in healthcare data security within IoT environments. Looking ahead, the integration of this framework could be expanded to include more advanced encryption algorithms for comparison, as well as real-time data monitoring capabilities to further optimize its performance. Additionally, further research could explore the Incorporation of AI-based anomaly detection systems to identify and mitigate potential security threats for adaptive security. The continued development of this framework could help establish more efficient and robust solutions for managing and securing sensitive healthcare data.

References

[1] Vallu, V. R., & Rathna, S. (2020). Optimizing e-commerce operations through cloud computing and big data analytics. International Research Journal of Education and Technology, 03(06).

[2] Shabbir, M., Shabbir, A., Iwendi, C., Javed, A. R., Rizwan, M., Herencsar, N., & Lin, J. C. W. (2021). Enhancing security of health information using modular encryption standard in mobile cloud computing. IEEE Access, 9, 8820-8834.

[3] Jayaprakasam, B. S., & Padmavathy, R. (2020). Autoencoder-based cloud framework for digital banking: A deep learning approach to fraud detection, risk analysis, and data security. International Research Journal of Education and Technology, 03(12).

[4] Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. Future generation computer systems, 78, 964-975.

[5] Mandala, R. R., & Kumar, V. K. R. (2020). AI-driven health insurance prediction using graph neural networks and cloud integration. International Research Journal of Education and Technology, 03(10).

[6] Sivan, R., & Zukarnain, Z. A. (2021). Security and privacy in cloud-based e-health system. Symmetry, 13(5), 742.

[7] Ubagaram, C., & Kurunthachalam, A. (2020). Bayesian-enhanced LSTM-GRU hybrid model for cloud-based stroke detection and early intervention. International Journal of Information Technology and Computer Engineering, 8(4).

[8] Masood, I., Wang, Y., Daud, A., Aljohani, N. R., & Dawood, H. (2018). Towards Smart Healthcare: Patient Data Privacy and Security in Sensor-Cloud Infrastructure. Wireless Communications and Mobile Computing, 2018(1), 2143897.

[9] Ganesan, S., & Hemnath, R. (2020). Blockchain-enhanced cloud and big data systems for trustworthy clinical decision-making. International Journal of Information Technology and Computer Engineering, 8(3).

[10] Kumarage, H., Khalil, I., Alabdulatif, A., Tari, Z., & Yi, X. (2016). Secure data analytics for cloud-integrated internet of things applications. IEEE Cloud Computing, 3(2), 46-56.

[11] Musam, V. S., & Purandhar, N. (2020). Enhancing agile software testing: A hybrid approach with TDD and AI-driven self-healing tests. International Journal of Information Technology and Computer Engineering, 8(2).

[12] Mehrtak, M., SeyedAlinaghi, S., MohsseniPour, M., Noori, T., Karimi, A., Shamsabadi, A., ... & Dadras, O. (2021). Security challenges and solutions using healthcare cloud computing. Journal of medicine and life, 14(4), 448.

[13] Musham, N. K., & Bharathidasan, S. (2020). Lightweight deep learning for efficient test case prioritization in software testing using MobileNet & TinyBERT. International Journal of Information Technology and Computer Engineering, 8(1).

[14] Azeez, N. A., & Van der Vyver, C. (2019). Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. Egyptian Informatics Journal, 20(2), 97-108.

[15] Allur, N. S., & Hemnath, R. (2018). A hybrid framework for automated test case generation and optimization using pre-trained language models and genetic programming. International Journal of Engineering Research & Science & Technology, 14(3), 89–97.

[16] Sajid, A., & Abbas, H. (2016). Data privacy in cloud-assisted healthcare systems: state of the art and future challenges. Journal of medical systems, 40(6), 155.

[17] 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).

[18] Karunarathne, S. M., Saxena, N., & Khan, M. K. (2021). Security and privacy in IoT smart healthcare. IEEE Internet Computing, 25(4), 37-48.

[19] Gudivaka, R. L., & Mekala, R. (2018). Intelligent sensor fusion in IoT-driven robotics for enhanced precision and adaptability. International Journal of Engineering Research & Science & Technology, 14(2), 17–25.

[20] Darwish, A., Hassanien, A. E., Elhoseny, M., Sangaiah, A. K., & Muhammad, K. (2019). The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems. Journal of Ambient Intelligence and Humanized Computing, 10, 4151-4166.

[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] Jayaram, R., & Prabakaran, S. (2021). Onboard disease prediction and rehabilitation monitoring on secure edge-cloud integrated privacy preserving healthcare system. Egyptian Informatics Journal, 22(4), 401-410.

[23] Gollavilli, V. S. B., & Thanjaivadivel, M. (2018). Cloud-enabled pedestrian safety and risk prediction in VANETs using hybrid CNN-LSTM models. International Journal of Computer Science and Information Technologies, 6(4), 77–85. ISSN 2347–3657.

[24] Hemalatha, P., Balaji, S., Chandru, E., Kumar, P. P., & Saravanan, D. (2021). Monitoring and securing the healthcare data harnessing IOT and blockchain technology. Turkish Journal of Computer and Mathematics Education, 12(2), 2554-2561.

[25] Parthasarathy, K., & Prasaath, V. R. (2018). Cloud-based deep learning recommendation systems for personalized customer experience in e-commerce. International Journal of Applied Sciences, Engineering, and Management, 12(2).

[26] Uke, N., Pise, P., Mahajan, H. B., Harale, S., & Uke, S. (2021). Healthcare 4.0 enabled lightweight security provisions for medical data processing. Turkish Journal of Computer and Mathematics Education, 12(11), 165-173.

[27] Dondapati, K. (2018). Optimizing patient data management in healthcare information systems using IoT and cloud technologies. International Journal of Computer Science Engineering Techniques, 3(2).

[28] Lo'ai, A. T., & Saldamli, G. (2021). Reconsidering big data security and privacy in cloud and mobile cloud systems. Journal of King Saud University-Computer and Information Sciences, 33(7), 810-819.

[29] 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).

[30] Wang, K., Chen, C. M., Tie, Z., Shojafar, M., Kumar, S., & Kumari, S. (2021). Forward privacy preservation in IoT-enabled healthcare systems. IEEE transactions on industrial informatics, 18(3), 1991-1999.

[31] Kadiyala, B., & Arulkumaran, G. (2018). Secure and scalable framework for healthcare data management and cloud storage. International Journal of Engineering & Science Research, 8(4), 1–8.

[32] Nepal, S., Ranjan, R., & Choo, K. K. R. (2015). Trustworthy processing of healthcare big data in hybrid clouds. IEEE Cloud Computing, 2(2), 78-84.

[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] Siam, A. I., Abou Elazm, A., El-Bahnasawy, N. A., El Banby, G., Abd El-Samie, F. E., & Abd El-Samie, F. E. (2019). Smart health monitoring system based on IoT and cloud computing. Menoufia journal of electronic engineering research, 28(1), 37-42.

[35] Natarajan, D. R., & Kurunthachalam, A. (2018). Efficient Remote Patient Monitoring Using Multi-Parameter Devices and Cloud with Priority-Based Data Transmission Optimization. Indo-American Journal of Life Sciences and Biotechnology, 15(3), 112-121.

[36] 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.

[37] 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).

[38] Das, J. (2020). Leveraging Cloud Computing for Medical AI: Scalable Infrastructure and Data Security for Advanced Healthcare Solutions. International journal of research and analytical reviews, 7, 504-514.

[39] Chauhan, G. S., & Palanisamy, P. (2018). Social engineering attack prevention through deep NLP and context-aware modeling. Indo-American Journal of Life Sciences and Biotechnology, 15(1).

[40] Nawaz, A., Peña Queralta, J., Guan, J., Awais, M., Gia, T. N., Bashir, A. K., ... & Westerlund, T. (2020). Edge computing to secure iot data ownership and trade with the ethereum blockchain. Sensors, 20(14), 3965.

[41] Vasamsetty, C., & Rathna, S. (2018). Securing digital frontiers: A hybrid LSTM-Transformer approach for AI-driven information security frameworks. International Journal of Computer Science and Information Technologies, 6(1), 46–54. ISSN 2347–3657.

[42] Tuli, S., Tuli, S., Wander, G., Wander, P., Gill, S. S., Dustdar, S., ... & Rana, O. (2020). Next generation technologies for smart healthcare: Challenges, vision, model, trends and future directions. Internet technology letters, 3(2), e145.

[43] Jadon, R., & RS, A. (2018). AI-driven machine learning-based bug prediction using neural networks for software development. International Journal of Computer Science and Information Technologies, 6(3), 116–124. ISSN 2347–3657.

[44] Nookala, G., Gade, K. R., Dulam, N., & Thumburu, S. K. R. (2019). End-to-End Encryption in Enterprise Data Systems: Trends and Implementation Challenges. Innovative Computer Sciences Journal, 5(1).

[45] 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).

[46] Pyrkova, A., & Temirbekova, Z. (2020). Compare encryption performance across devices to ensure the security of the IOT. Indonesian Journal of Electrical Engineering and Computer Science, 20(2), 894-902.

[47] Nippatla, R. P., & Palanisamy, P. (2018). Enhancing cloud computing with eBPF powered SDN for secure and scalable network virtualization. Indo-American Journal of Life Sciences and Biotechnology, 15(2).

[48] Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2016). Threats to networking cloud and edge datacenters in the Internet of Things. IEEE Cloud Computing, 3(3), 64-71.

[49] Gollapalli, V. S. T., & Arulkumaran, G. (2018). Secure e-commerce fulfilments and sales insights using cloud-based big data. International Journal of Applied Sciences, Engineering, and Management, 12(3).

[50] Yu, K., Tan, L., Yang, C., Choo, K. K. R., Bashir, A. K., Rodrigues, J. J., & Sato, T. (2021). A blockchain-based shamir's threshold cryptography scheme for data protection in industrial internet of things settings. IEEE Internet of Things Journal, 9(11), 8154-8167.

[51] Garikipati, V., & Palanisamy, P. (2018). Quantum-resistant cyber defence in nation-state warfare: Mitigating threats with post-quantum cryptography. Indo-American Journal of Life Sciences and Biotechnology, 15(3).

[52] Bakar, N. A. A., Ramli, W. M. W., & Hassan, N. H. (2019). The internet of things in healthcare: an overview, challenges and model plan for security risks management process. Indonesian Journal of Electrical Engineering and Computer Science (IJEECS), 15(1), 414-420.

[53] 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)

[54] Dondapati, K. (2018). Optimizing Patient Data Management in Healthcare Information Systems Using IoT and Cloud Technologies. Hospital, 3(2).

[55] Kushala, K., & Rathna, S. (2018). Enhancing privacy preservation in cloud-based healthcare data processing using CNN-LSTM for secure and efficient processing. International Journal of Mechanical Engineering and Computer Science, 6(2), 119–127.

[56] Chinnasamy, P., Deepalakshmi, P., Dutta, A. K., You, J., & Joshi, G. P. (2021). Ciphertext-policy attribute-based encryption for cloud storage: Toward data privacy and authentication in AI-enabled IoT system. Mathematics, 10(1), 68.

[57] Alagarsundaram, P., & Arulkumaran, G. (2018). Enhancing Healthcare Cloud Security with a Comprehensive Analysis for Authentication. Indo-American Journal of Life Sciences and Biotechnology, 15(1), 17-23.

[58] Smithamol, M. B., & Rajeswari, S. (2017). Hybrid solution for privacy-preserving access control for healthcare data. Advances in Electrical and Computer Engineering, 17(2), 31-38.

[59] Bhadana, D., & Kurunthachalam, A. (2020). Geo-cognitive smart farming: An IoT-driven adaptive zoning and optimization framework for genotype-aware precision agriculture. International Journal in Commerce, IT and Social Sciences, 7(4).

[60] Srinivasu, P. N., Bhoi, A. K., Nayak, S. R., Bhutta, M. R., & Woźniak, M. (2021). Blockchain technology for secured healthcare data communication among the non-terminal nodes in IoT architecture in 5G network. Electronics, 10(12), 1437.

[61] Ramar, V. A., & Rathna, S. (2018). Implementing Generative Adversarial Networks and Cloud Services for Identifying Breast Cancer in Healthcare Systems. Indo-American Journal of Life Sciences and Biotechnology, 15(2), 10-18.