

**SECURE AND EFFICIENT DATA MANAGEMENT FOR HEALTHCARE IOT
DEVICES IN CLOUD-ENABLED SYSTEMS USING SERPENT ENCRYPTION**

Raj Kumar Gudivaka

Tecra Systems Private Limited, Telangana, India
rajkumargudivaka35@gmail.com

Rajya Lakshmi Gudivaka

Gudlavalleru Engineering, College, Gudlavalleru
rlakshmigudivaka@gmail.com

Karthick.M

Assistant Professor, Department, SNS College of Technology, Coimbatore, India.
magukarthik@gmail.com

http://doi.org/10.35409/IJBMER.2019.2099_1

ABSTRACT

The increasing adoption of Internet of Things (IoT) devices in healthcare has significantly improved patient monitoring and care management, enabling collection of critical health data. However, challenges remain in ensuring the secure transfer of sensitive data, managing computational overhead, and optimizing data transmission efficiency in cloud-enabled healthcare systems. This paper presents a framework that addresses these challenges by enhancing security and optimizing the transfer of healthcare data in IoT systems. The system begins with collecting data from healthcare IoT devices, such as wearable health monitors and patient monitoring systems. Then, the collected data is scaled using Robust Scaler, which helps in mitigating the influence of outliers, ensuring that the data is normalized while maintaining robustness. Categorical data is handled by Label Encoding, converting non-numeric categories into numeric labels. After preprocessing, the data undergoes encryption using the Serpent cipher, which provides secure encryption, ensuring that sensitive healthcare data is protected during storage or transfer. Finally, the processed and encrypted data is securely transferred to the cloud platform for storage and processing. Experimental results demonstrate that as key size increases from 128 bits to 256 bits, the Serpent encryption strength improves, reaching approximately 98%, while transmission latency rises from 50 ms for 1 MB of data to 3800 ms for 100 MB. This work by develops a secure, efficient, and scalable framework that ensures the privacy of healthcare data while minimizing latency in IoT cloud systems.

Keywords: Healthcare IoT, Data Security, Serpent Encryption, Cloud Computing and Secure Data Transfer.

1. INTRODUCTION

The integration of Internet of Things (IoT) devices in healthcare systems has revolutionized patient care by enabling monitoring of vital signs, leading to more proactive and personalized healthcare [1][2]. With the rise of cloud computing, healthcare data generated from IoT devices can be stored, processed, and analyzed on remote cloud platforms, offering a scalable solution for health management [3] [4]. However, as the volume of sensitive medical data increases, ensuring its secure transmission and storage has become a critical concern [5] [6]. Data privacy, integrity, and

accessibility are crucial to the success of IoT-enabled healthcare systems [7] [8]. The proposed framework addresses the growing need for secure and efficient data transfer techniques, aiming to improve the reliability and security of healthcare data while optimizing performance for cloud-based processing [9].

Existing methods for secure data transfer in healthcare IoT systems rely on various communication protocols and encryption techniques [10] [11]. Protocols like MQTT and CoAP are commonly used for low-latency communication in IoT devices, while encryption methods such as AES, RSA, and ECC provide security for data transmission [12] [13]. However, these methods have several limitations [14]. For instance, traditional encryption schemes like RSA are computationally intensive and inefficient on resource-constrained IoT devices [15]. Moreover, these methods often lack scalability to handle large datasets and are vulnerable to potential future quantum computing threats [16] [17]. Additionally, many existing systems do not effectively address the trade-off between security and performance, especially in healthcare applications where low latency and high throughput are critical [18] [19].

The proposed framework overcomes these drawbacks by leveraging Serpent encryption for stronger security and efficient data transfer, ensuring that healthcare IoT data remains encrypted and secure throughout its journey to the cloud. The framework incorporates data scaling and robust preprocessing methods, such as Robust Scaler and Label Encoding, to handle large datasets effectively. By optimizing data transfer with lightweight encryption and low-latency communication protocols, the framework ensures enhanced security, improved scalability, and reduced resource consumption, making it ideal for healthcare applications. The novelty of the proposed system lies in its combination of high security, computational efficiency, and the ability to handle large-scale data transfers in a secure and privacy-preserving manner.

The paper is organized as follows: Section 2 reviews related work and existing methods. Section 3 presents the proposed framework, including methodology and techniques used. Section 4 provides the results and analysis of the proposed framework. Finally, Section 5 concludes the paper.

2. LITERATURE SURVEY

The effectiveness of various computational models, including Genetic Algorithms (GA), Monte Carlo Methods (MCM), and Markov Models (MM), in cloud-based scientific computing [20]. The study focused on evaluating execution time, accuracy, and resource consumption to measure computational efficiency and scalability [21]. The vulnerability of traditional centralized security models to dynamic cyber threats [22]. The study introduced a decentralized framework combining Federated Learning (FL), K-Nearest Neighbors (KNN), Generative Adversarial Networks (GANs), and IOTA Tangle for secure cyber threat detection [23].

A federated learning framework optimized through split learning, integrating graph neural networks and hashgraph technology to enhance cybersecurity systems [24]. Their work aimed to strengthen defense mechanisms against malware detection and data protection challenges [25]. Natarajan developed a hybrid model combining Radial Basis Function Networks (RBFN), Genetic Algorithms (GA), and Particle Swarm Optimization (PSO) to improve healthcare disease diagnosis [26]. The study focused on optimizing RNNs and RBFNs for processing IoT device data using a PSO-GA framework, enhancing sensitivity and specificity for chronic sickness identification [27]. High-performance machine learning pipeline combining Recursive Feature Elimination (RFE),

Extreme Learning Machine (ELM), and Sparse Representation Classification (SRC) for feature selection and efficient data representation [28]. Their work emphasized the optimization of AI pipelines to enhance feature selection and model performance [29]. The rise in security concerns related to cloud-connected robotics, including command injection and DDoS attacks [30]. The study proposed a hybrid intrusion detection system combining Transformer, RNN, and GNN models to improve attack detection accuracy and response time [31].

Scalability and security in cloud-based healthcare applications, emphasizing the importance of data processing for improving patient care [32]. Machine learning models for data security and privacy, suggesting encryption techniques for ensuring secure transmission in healthcare IoT environments [33]. Narla further expanded this concept by exploring lightweight cryptographic protocols for data transmission, which minimize latency while ensuring high security in IoT applications [34].

Decentralized approach for securing data in IoT environments, which is relevant to improving security and privacy in healthcare IoT systems [35]. Cloud storage and communication efficiency, directly supporting the optimization of data transfer in cloud-enabled healthcare systems [36]. Federated learning's role in enhancing system scalability and preserving privacy in distributed healthcare IoT systems, offering insights into how decentralized learning models can be integrated to reduce computational overhead while ensuring privacy [37].

Need for effective data compression and encryption to handle large volumes of data in IoT systems [38]. Integrating advanced machine learning techniques like Federated Learning and K-Nearest Neighbors for anomaly detection, aiming to improve security in IoT environments [39]. Deevi furthered this by proposing secure and optimized data processing frameworks for cloud-based healthcare systems, which complement the proposed framework by emphasizing secure data transfer and encryption techniques for effective healthcare IoT management [40].

Recent advancements in secure healthcare data management have focused on integrating advanced cryptographic techniques with intelligent data processing to address the growing challenges of privacy, scalability, and real-time access in cloud-enabled IoT environments [41]. Emerging methods such as Serpent encryption, known for its lightweight structure and high resistance to cryptographic attacks, offer an efficient alternative to traditional encryption algorithms for securing healthcare data in resource-constrained IoT devices [42]. In parallel, adaptive machine learning models are increasingly being utilized to monitor and analyze healthcare data streams, enabling early detection of anomalies without compromising patient privacy [43]. Furthermore, research has shown that combining decentralized learning approaches, such as federated and split learning, with edge computing can significantly reduce latency and enhance data security at the device level [44]. These methods not only maintain compliance with healthcare regulations like HIPAA and GDPR but also empower real-time clinical decision-making [45].

2.1 Problem Statement

Although significant progress has been made in healthcare IoT systems, several challenges still persist, particularly in the areas of Data Security and Privacy Concerns and Computational Overhead [46]. Ensuring the security of sensitive healthcare data during transmission and storage remains difficult, especially in decentralized cloud environments [47]. Additionally, many existing solutions impose high computational overhead, making data processing on resource-constrained IoT devices a challenge [48] [49]. The proposed work aims to address these issues by developing

a secure, efficient framework using Serpent encryption and lightweight data transfer techniques, optimizing both security and computational efficiency healthcare IoT applications [50].

3.METHODOLOGIES

The workflow begins with the data collection from healthcare IoT devices, such as wearable health monitors and patient monitoring systems, which gather vital signs and patient-specific data. In the data preprocessing step, the collected data is scaled using Robust Scaler, which helps in mitigating the influence of outliers, ensuring that the data is normalized while maintaining robustness. Categorical data is handled by Label Encoding, converting non-numeric categories into numeric labels. After preprocessing, the data undergoes encryption using the Serpent cipher, which provides secure encryption, ensuring that sensitive healthcare data is protected during storage or transfer. Finally, the processed and encrypted data is securely transferred to the cloud platform for further analysis, storage, or processing. This workflow ensures that healthcare IoT data is securely handled from collection to cloud processing, safeguarding patient privacy throughout the process. This Process is illustrated in Figure 1.

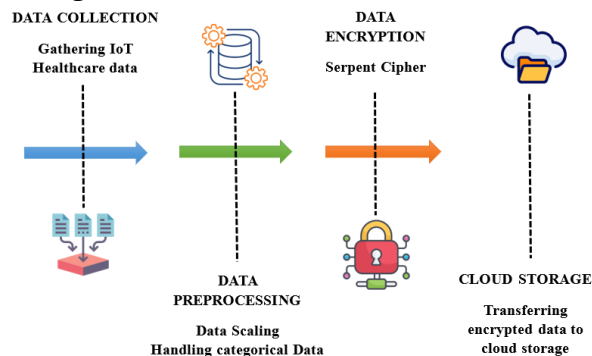


Figure 1: Workflow of Secure Healthcare IoT Data Transfer and Storage

3.1 Data Collection

Data collection in the proposed framework involves gathering healthcare data from IoT devices like wearable health monitors and patient monitoring systems. These devices track vital signs such as heart rate, blood pressure, glucose levels, and other patient-specific metrics. The data is continuously transmitted to a cloud platform for analysis. Additionally, patient-specific information like demographics and medical history is collected. This comprehensive data enables accurate health monitoring and early detection of potential issues.

3.2 Data Preprocessing

Data preprocessing involves cleaning and transforming raw data into a format suitable for analysis by handling missing values, normalizing features, and encoding categorical variables. This step ensures the data is consistent, accurate, and ready for modeling.

3.2.1 Data Scaling

After data collection, Robust Scaler is used to normalize the healthcare data, minimizing the effect of outliers. It scales the data to a consistent range, ensuring that all features are comparable. This step helps maintain the integrity of the data and ensures no feature dominates the model due to differing scales.

3.2.2 Handling Categorical Data

Categorical variables such as gender or medical conditions are converted into numeric labels using Label Encoding. This process transforms non-numeric data into a format that can be processed by machine learning models. It ensures that essential patient information is accurately represented for further analysis.

3.3 Encryption

After the data is pre-processed, it undergoes encryption using the Serpent cipher to ensure the confidentiality and security of sensitive healthcare information. Serpent is a symmetric key block cipher known for its high level of security and efficiency. It encrypts the pre-processed data into a secure format, making it unreadable to unauthorized parties. The encryption process ensures that sensitive patient data remains protected during storage and transmission, maintaining privacy. Serpent's robustness provides resistance to various cryptographic attacks, safeguarding data integrity. Once encrypted, the data is ready for secure transmission to the cloud for further processing and analysis.

The Serpent cipher is a symmetric key block cipher, meaning the same key is used for both encryption and decryption. It operates on 128-bit blocks of data and supports key sizes of 128, 192, and 256 bits. It consists of multiple rounds (32 rounds for Serpent) of substitution and permutation operations, making it highly secure.

The encryption process can be mathematically expressed as equation (1),

$$C = E_K(P) \quad (1)$$

Where, C is the ciphertext (the encrypted data), E_K is the encryption function that uses a key K , P is the plaintext (the original preprocessed data), K is the key used for encryption.

The cipher key K is expanded into several subkeys, one for each round of encryption. In each round, the plaintext is subjected to a series of transformations, including, each byte of the data is substituted with another byte based on a substitution table. The data is rearranged (permuted) to increase diffusion. The data is mixed with the subkey for that round. After 32 rounds, the result is the ciphertext C , which is unreadable without the decryption key.

The decryption process uses the inverse of the encryption steps, applying the round keys in reverse order.

3.4 Cloud Storage

After the data is encrypted, it is securely transferred to cloud storage for further processing and long-term storage. Cloud storage allows for scalable, remote access to the encrypted healthcare data, ensuring that it is safely stored and protected from unauthorized access. The encrypted data is housed in cloud servers, where it can be efficiently managed, backed up, and accessed by authorized healthcare providers. Cloud storage also provides high availability and redundancy, ensuring that the data remains accessible even in the event of hardware failures. Security measures like encryption at rest and access control policies further safeguard the stored data. Once in the cloud, the data is ready for analysis and decision-making, while remaining protected throughout its lifecycle.

4. RESULTS

The results section presents an analysis of the key performance metrics used to evaluate the proposed framework. The analysis focuses on the relationship between encryption strength and

key size, along with the effect of data size on transmission latency. These results underline the importance of optimizing both data security and transfer efficiency in healthcare IoT systems.

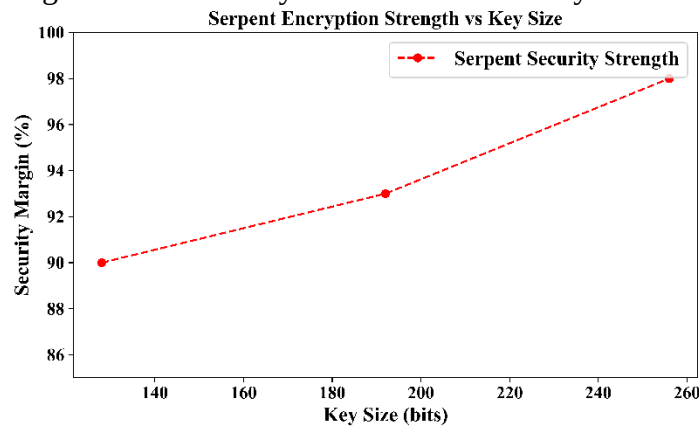


Figure 2: Serpent Encryption strength

Figure 2 illustrates the relationship between Serpent encryption strength and key size. As the key size increases from 128 bits to 256 bits, the security margin steadily improves, reaching approximately 98% for the largest key size. The plot indicates that higher key sizes provide stronger encryption, enhancing data protection. This demonstrates that, as the key size grows, the encryption strength and overall security of the Serpent cipher significantly improve, ensuring greater protection for sensitive healthcare IoT data during transmission and storage.

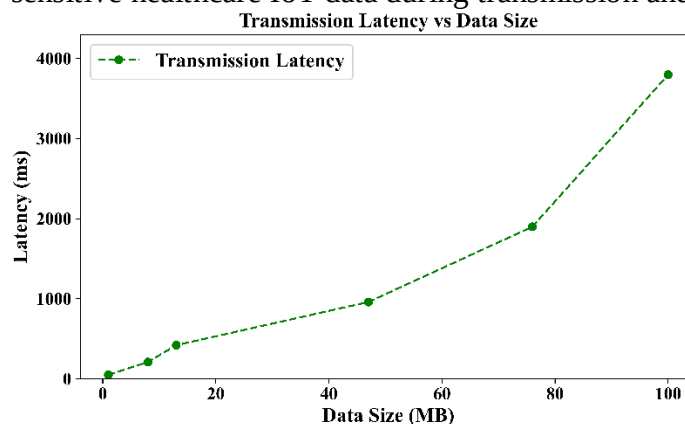


Figure 3: Transmission Latency

Figure 3 shows the relationship between transmission latency and data size. As the data size increases from 1 MB to 100 MB, the transmission latency increases significantly, with latency rising from 50 ms to 3800 ms. This demonstrates that larger datasets require more time for transmission, which can impact performance in healthcare IoT systems. The non-linear trend highlights the need for optimized data transfer techniques to minimize latency, especially when dealing with large volumes of sensitive healthcare data.

5. CONCLUSIONS

The work successfully achieved the objective of developing a secure, efficient, and scalable framework for the transfer of healthcare IoT data in cloud-enabled systems, addressing challenges

related to data security and transmission optimization. Experimental results demonstrate that as the key size increases from 128 bits to 256 bits, the Serpent encryption strength improves from 90% to approximately 98%, providing robust data protection. Additionally, transmission latency increases with data size, ranging from 50 ms for 1 MB to 3800 ms for 100 MB, emphasizing the need for optimized data transfer protocols to handle larger datasets efficiently, especially in healthcare applications. This framework ensures secure data handling while optimizing the computational efficiency of healthcare IoT systems. It successfully balances the trade-off between data security and system performance, providing a reliable solution for cloud-based healthcare data management. Future work will focus on exploring the use of quantum-resistant encryption algorithms to safeguard the system against potential threats from quantum computing.

REFERENCES

- [1] Izevbizua, P. O. (2015). Data security in the cloud using serpent encryption and distributed steganography. *European Scientific Journal*, 11(18), 5845.
- [2] 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).
- [3] Švída, M., & Majerník, J. (2014). Data security management on storage devices in real time. *MEFANET Journal*, 2(1), 5-9.
- [4] 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).
- [5] Bahga, A., & Madiseti, V. K. (2016). Blockchain platform for industrial internet of things. *Journal of Software Engineering and Applications*, 9(10), 533-546.
- [6] Bobba, J., & Prema, R. (2018). Secure financial data management using Twofish encryption and cloud storage solutions. *International Journal of Computer Science Engineering Techniques*, 3(4), 10–16.
- [7] Agosta, G., Barengi, A., Maggi, M., & Pelosi, G. (2014). Design space extension for secure implementation of block ciphers. *IET Computers & Digital Techniques*, 8(6), 256-263.
- [8] Musham, N. K., & Pushpakumar, R. (2018). Securing cloud infrastructure in banking using encryption-driven strategies for data protection and compliance. *International Journal of Computer Science Engineering Techniques*, 3(5), 33–39.
- [9] Darwish, M. A., Yafi, E., Almasri, A. H., & Zuhairi, M. F. (2018). Privacy and security of cloud computing: a comprehensive review of techniques and challenges. *International Journal of Engineering Trends and Technology*, 7(4.29), 239-246.
- [10] 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.
- [11] Verbraecken, J. (2016). Telemedicine applications in sleep disordered breathing: thinking out of the box. *Sleep medicine clinics*, 11(4), 445-459.
- [12] Basani, D. K. R., & RS, A. (2018). Integrating IoT and robotics for autonomous signal processing in smart environment. *International Journal of Computer Science and Information Technologies*, 6(2), 90–99. ISSN 2347–3657.

-
- [13] Dehrouyeh, Z., & Azmi, R. (2018). Using smart contract for privacy preserving in Internet of Things (IoT) environments. *Journal of Advances in Computer Networks*, 6(1), 71-76.
- [14] 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.
- [15] Singh, K. J., & Gagneja, K. (2017). Overview of securing multimedia content using efficient encryption methods and modes. *International Journal of Advanced and Applied Sciences*, 4(10), 84-96.
- [16] 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.
- [17] Garber, L. (2014). Security, privacy, policy, and dependability roundup. *IEEE Security & Privacy*, 12(3), 6-8.
- [18] 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.
- [19] Kuznetsov, A. B., Mukhin, A. S., Simutis, I. S., Shchegolkov, L. A., & Boyarinov, G. A. (2018). Information technology in health care: Information retrieval, processing, and protection. *Современные технологии в медицине*, 10(3 (eng)), 213-222.
- [20] Pulakhandam, W., & Bharathidasan, S. (2018). Leveraging AI and cloud computing for optimizing healthcare and banking systems. *International Journal of Mechanical Engineering and Computer Science*, 6(1), 24–32.
- [21] Naeemabadi, M., Mehri Dehnavi, A., & Rabbani, H. (2014). Statistical Analysis of Encryption Quality for Medical Images Based on Rijndael Encryption Algorithm Using Both Static and Chaotic Cipher Key. *Journal of Health and Biomedical Informatics*, 1(1), 32-44.
- [22] 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.
- [23] Chignola, S. (2018). The mole & the snake. *SOFT POWER: REVISTA EURO-AMERICANA DE TEORÍA E HISTORIA DE LA POLÍTICA*, 6(1), 54-76.
- [24] Jayaprakasam, B. S., & Hemnath, R. (2018). Optimized microgrid energy management with cloud-based data analytics and predictive modelling. *International Journal of Mechanical Engineering and Computer Science*, 6(3), 79–87.
- [25] Huang, C. W., Huang, C. H., Hung, Y. H., & Chang, C. Y. (2018). Sensing pipes of a nuclear power mechanism using low-cost snake robot. *Advances in mechanical engineering*, 10(6), 1687814018781286.
- [26] Gudivaka, B. R., & Palanisamy, P. (2018). Enhancing software testing and defect prediction using Long Short-Term Memory, robotics, and cloud computing. *International Journal of Mechanical Engineering and Computer Science*, 6(1), 33–42.
- [27] Sarkar, S., & Akila, A. (2018). Exploration of Cryptographic Techniques based on Diversity of Features. *International Journal of Advanced Studies of Scientific Research*, 3(10).
- [28] Ayyadurai, R., & Vinayagam, S. (2018). Transforming customer experience in banking with cloud-based robo-advisors and chatbot integration. *International Journal of Marketing Management*, 6(3), 9–17.
-

-
- [29] Wang, F. Y., Yuan, Y., Zhang, J., Qin, R., & Smith, M. H. (2018). Blockchainized Internet of minds: A new opportunity for cyber–physical–social systems. *IEEE Transactions on Computational Social Systems*, 5(4), 897-906.
- [30] 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.
- [31] Romano, D., & Schmid, G. (2017). Beyond bitcoin: A critical look at blockchain-based systems. *Cryptography*, 1(2), 15.
- [32] 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.
- [33] Quilala, T. F. G., Sison, A. M., & Medina, R. P. (2018). Modified blowfish algorithm. *Indonesian Journal of Electrical Engineering and Computer Science*, 12(1), 38-45.
- [34] Valivarthi, D. T., & Hemnath, R. (2018). Cloud-integrated wavelet transform and particle swarm optimization for automated medical anomaly detection. *International Journal of Engineering Research & Science & Technology*, 14(1), 17–27.
- [35] Niazi, M. A. (2014). Emergence of a Snake-Like Structure in Mobile Distributed Agents: An Exploratory Agent-Based Modeling Approach. *The Scientific World Journal*, 2014(1), 140309.
- [36] 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.
- [37] Lee, J. (2018). Patch transporter: Incentivized, decentralized software patch system for WSN and IoT environments. *Sensors*, 18(2), 574.
- [38] 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.
- [39] Dener, M., & Bay, O. F. (2016). TeenySec: a new data link layer security protocol for WSNs. *Security and Communication Networks*, 9(18), 5882-5891.
- [40] Ubagaram, C., & Mekala, R. (2018). Enhancing data privacy in cloud computing with blockchain: A secure and decentralized approach. *International Journal of Engineering & Science Research*, 8(3), 226–233.
- [41] Sagner, M., McNeil, A., Puska, P., Auffray, C., Price, N. D., Hood, L., ... & Arena, R. (2017). The P4 health spectrum—a predictive, preventive, personalized and participatory continuum for promoting healthspan. *Progress in Preventive Medicine*, 2(1), e0002.
- [42] Vallu, V. R., & Palanisamy, P. (2018). AI-driven liver cancer diagnosis and treatment using cloud computing in healthcare. *Indo-American Journal of Life Sciences and Biotechnology*, 15(1).
- [43] Bellizia, D., Scotti, G., & Trifiletti, A. (2016). On-chip current-mode approach to thwart CPA attacks in CMOS nanometer technology. *International Journal of Microelectronics and Computer Science*, 7(4), 147-156.
- [44] Sareddy, M. R., & Jayanthi, S. (2018). Temporal convolutional network-based shortlisting model for sustainability of human resource management. *International Journal of Applied Sciences, Engineering, and Management*, 12(1).
-

-
- [45] Wang, C., Zhu, L., Gong, L., Zhao, Z., Yang, L., Liu, Z., & Cheng, X. (2018). Accurate sybil attack detection based on fine-grained physical channel information. *Sensors*, 18(3), 878.
- [46] 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).
- [47] Bagchi, R. (2017). Using blockchain technology and smart contracts for access management in IoT devices. *Computer Science*, 80(9).
- [48] 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).
- [49] Vigneswari, S., & Dhenakaran, S. S. (2014). Mining Medicinal Information using Flowers. *International Journal of Computer Applications*, 95(22), 15-20.
- [50] 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).