UtilitasMathematica

ISSN 0315-3681 Volume 122 (2), 2025

MATHEMATICALLY ENHANCED LIGHTWEIGHT CRYPTOGRAPIC HASH FUNCTIONS FOR DIGITAL MEDICAL DATA SECURITY IN CLOUD

Mr. R.Palaniyappan
Research Scholar
Department of Computer Science
Sri Vasavi College
Erode, India
palaniraja92@gmail.com

Dr.D. Sasikala
Assistant Professor
Department of Computer Science
Sri Vasavi College
Erode, India

Abstract: The protection of data within healthcare cloud is paramount to safeguard data and users' privacy, maintain data authenticity and prevent unlawful users' access. There are numerous issues and concerns that are associated with health care systems that are cloud based, and some of the major ones include; Cyber security; this is because cloud systems are prone to attacks such as; hacking, leakage of information and other unauthorized accesses to patients' data and information. Most of the existing conventional cryptographic methods are costly in terms of computational power and hence not suitable for low resource environment. The current techniques may not provide enough protection against new forms of attacks including collision and preimage attacks which may result to major problems like tampering and forging of data. Such challenges call for an optimized security solution that corresponds to the needs of cloud-based medical data management. This paper proposes an extensible and secure design of the framework which employs mathematically altered lightweight cryptographic hash functions for protecting digital medical information over cloud networks. This framework provides greater data privacy when compared to the normal approach and the computational cost is very small, which is very suitable for real-world healthcare applications that need efficient data management solutions.

Keywords: *Cloud, security, medical data, hash function, cryptography, privacy, and healthcare.*

1. Introduction

Cloud computing is a transformative technology that provides on-demand access to computing resources over the internet. Instead of relying on local servers or personal devices, users can tap into a vast pool of computing power, storage, and applications hosted on remote servers. This approach offers several key benefits,

including scalability, flexibility, and cost-efficiency [1].

The use of cloud computing means that users can increase or decrease their IT requirements accordingly and without the need to purchase physical equipment or manage them[2]. This model is typically offered through three main service categories[3]: These three models of service delivery include the Infrastructure as a Service (IaaS) that provides virtualized computing resources, the Platform as a Service (PaaS) that offers a platform for application development and deployment and the Software as a Service (SaaS) that delivers software applications through the internet[4].

Security in cloud computing is a critical aspect that ensures the protection of data, applications, and services hosted in cloud environments [5]. It involves a range of practices and technologies designed to safeguard against unauthorized access, data breaches, and cyber threats [6]. Key security measures include encryption, identity and access management, and regular security audits. Providers often offer built-in security features, but it's also crucial for users to implement their own security protocols [7]. Effective cloud security combines robust technological solutions with strong governance and compliance practices, ensuring that sensitive information remains protected while leveraging the flexibility and scalability of cloud services [8].

Digital medical data over the cloud refers to the storage, management, and sharing of healthcare information using cloud computing technologies[9]. This approach enables healthcare providers to securely access patient records, medical imaging, and other critical data from anywhere with internet connectivity[10]. Benefits include enhanced data accessibility, improved collaboration among healthcare professionals, and streamlined operations. Cloud-based solutions also support advanced analytics and telemedicine, driving better patient outcomes and operational efficiency[11]. However, managing this data requires stringent security measures and compliance with regulations like HIPAA to protect patient privacy and ensure data integrity in a rapidly evolving digital landscape [12].

Securing digital medical data in the cloud is a critical concern in today's healthcare landscape. As the adoption of cloud computing in healthcare grows, the protection of sensitive medical information becomes paramount [13]. Cloud platforms offer scalability, cost-

efficiency, and enhanced collaboration, but they also introduce risks such as data breaches and unauthorized access. To address these challenges, healthcare organizations must implement robust security measures including encryption, multi-factor authentication, and regular security audits [14]. Additionally, adherence to regulatory standards like HIPAA in the U.S. and GDPR in Europe is essential to ensure compliance and safeguard patient privacy. By leveraging advanced security technologies and practices, healthcare providers can protect digital medical data from threats, ensuring both patient confidentiality and the integrity of their information [15].

2. Related Works

Selvakumar and Lokesh (2024) Cloud computing has emerged as a transformative technology in various sectors, particularly in healthcare, where it facilitates the storage and processing of vast amounts of medical data. However, this advancement brings forth significant challenges in terms of security, privacy, and environmental impact ,highlight the importance of cryptographic methods in securing healthcare data transmitted to the cloud, proposing an encryption algorithm that uses DNA cryptography and Huffman coding to enhance data security [16].

Similarly, Walid, Joshi, and Choi (2024) tackle the issue of secure access to cloud-based Electronic Health Records (EHRs) by integrating Attribute-Based Encryption with Semantic Web Technologies. Their novel graph-based EHR system leverages semantic context to query through a knowledge graph, which not only handles heterogeneous medical data effectively but also ensures fine-grained security at the field level. This method is particularly valuable for maintaining patient privacy while accommodating the diverse and growing nature of medical data [17].

Bhansali et al. (2024) discuss the role of cloud computing in the medical field, focusing on secure data storage and access control for Internet of Medical Things (IoMT) using federated learning. In the broader context of cloud computing, examine how federated learning can enhance secure data storage and access control within the Internet of Medical Things (IoMT). Their research highlights the importance of robust access controls and secure data storage solutions to protect sensitive medical information, emphasizing that federated learning provides a promising framework for addressing these challenges. This

perspective aligns with the increasing reliance on cloud services for storing medical data and the need for sophisticated security measures. [18].

Malathi et al. (2024) explore the potential of big data analytics in managing diverse clinical data from various sources, emphasizing the need for effective data integration and interoperability, further organized and accessible information. This capability is crucial for improving efficiency in healthcare delivery and

On a broader scale, Yanamala (2024) reviews the new security threats facing cloud computing such as data leakage and internal threats, Cloud computing as a technology has completely transformed the way that data is stored, accessed and processed on the internet with flexibility and scalability.

Nevertheless, such a shift to the new paradigm has introduced many security issues that need to be solved to maintain data's integrity, confidentiality, and availability. This literature review aims at discussing the security issues in cloud computing which are relatively new and hence include data breaches, insider threats, insecure APIs, and others that are shared in nature. The review draws from the existing literature and best practices, identify the problems and discuss the possible ways of handling them. It is with this view that this review seeks to establish an understanding of the challenges with a view of developing proactive measures to mitigate the risks affecting the security of information in cloud environments [20].

contribute to the discussion by addressing the integration and interoperability of medical data through big data analytics. Their study, which focuses on Apollo Hospital in Kolkata, illustrates how analyzing vast datasets from various sources—such as patient records, lab results, and diagnostic data—can lead to more

making meaningful use of the data collected [19].

While Mark and Bommu (2024) discuss ways of minimizing carbon emission on data transfers in cloud computing systems. This has been made possible by the advancement of technology especially in the use of cloud computing which has led to increased convenience and efficiency in data management. However, this growth also comes with various challenges to environmental sustainability especially on the aspect of carbon footprint of data transmission. This paper aims at discussing different approaches of reducing the carbon footprint of data

transmission in cloud computing. Thus, the combination of these approaches helps cloud service providers to reduce the negative effects on the environment without compromising the service quality. Based on the analysis of the literature and case studies, this paper presents the findings on the state of carbon emissions in cloud computing, and the potential solutions for its minimization [21].

Finally, Mistry et al. (2024) analyze the impact of cloud computing and artificial intelligence (AI) on industry dynamics and competition, noting that these technologies drive efficiency but also introduce new challenges and opportunities. Collectively, these studies underscore the dual nature of cloud computing as both a powerful enabler and a source of complex challenges in modern data management. Their analysis reveals how these technologies enhance operational efficiency and drive innovation, while also presenting new challenges and opportunities for businesses. This examination underscores the transformative potential of cloud computing and AI in shaping modern industry landscapes [22].

The research gap that has been observed in the current literature is the lack of lightweight and efficient cryptographic solutions that are suitable for cloud healthcare system. Although Selvakumar and Lokesh (2024) use cryptography and Huffman coding, others use attribute-based encryption, federated learning, and data integration, those approaches either have high computational cost or have poor security and efficiency. . The absence of a robust and efficient method to secure medical data over the cloud is filled by the proposed mathematically modified lightweight cryptographic hash function. This approach improves the quality of the data and reduces the load on the processing system while also improving the level of protection without a negative impact on the speed or energy consumption.

3. Proposed Methodology - Mathematically Enhanced Lightweight Cryptographic Hash Functions for Digital Medical Data Security in Cloud

The proposed methodology focuses on developing a mathematically modified lightweight cryptographic hash function tailored for digital medical data security over cloud environments. The objective is to create a secure, efficient, and computationally lightweight framework that can handle the specific

needs of cloud-based healthcare data, ensuring data integrity and confidentiality with minimal computational overhead. This methodology emphasizes the mathematical design of the cryptographic function, detailing each phase with corresponding equations to highlight the performance and security enhancements.

Let M represent the medical data input, expressed in binary form. The proposed cryptographic hash function H(M) undergoes a multi-phase process comprising preprocessing, transformation, compression, and finalization, each mathematically structured to ensure data security and low-latency performance.

where denotes bitwise XOR, ≪ and ≫ are bitwise left and right shifts by k and m bit s, respectively.For each block $M_i$the transformed value is:

$$T(M_i) = Mi \oplus (M_i \ll k) \oplus (M_i \gg m)$$

C. Compression Phase: Iterative Block Combination

A chaining variable V is initialized using an Initial Vector (IV), denoted as V_0. The compression function CCC iteratively combines the transformed blocks:

$$V_i = C(C(V_{i-1}, T))$$

A. Pre-processing Phase: Padding and Block Division

The input M is padded to ensure its length is a multiple of the required block size b. Let P denote the padding such that: The input M is padded to ensure its length is a multiple of the required block size b. Let P denote the padding such that:

$$M = M \parallel P \text{ where } |M| \equiv 0 \bmod b$$

The padded data is divided into n blocks:

$$M = \{M_1, M_2, \dots, M_n\}, |M_i| = b \forall_i \in \{1,2, \dots, n\}$$

B. Transformation Phase: Nonlinear Mathematical Operations Each block $M_i$undergoes a transformation function T to introduce nonlinearity, enhancing diffusion properties. The transformation function is defined as:

$$T(x) = x \oplus (x \ll k) \oplus$$

Such bitwise operations point to a dramatic transformation of the input, making it possible to witness major changes in H(M) even when M is changed slightly.

The compression function $C(a, b)$ is mathematically defined as:

$$C(a, b) = (a \times b + c) \bmod p$$

Where c is constant and p is a prime number that has been chosen in a way that reduces the likelihood of collision in the implementation of the system . The

chaining update for each iteration is given by:

$$V_1 = (V_0 \times R(M_1) + c)\ modp$$

.

D. Finalization Phase: Hash Output Generation

The final hash value H(M) is obtained by applying a modular reduction operation on the final chaining value V_n:

$$H(M) = (V_n + d) modp$$

where*d* is a constant chosen to introduce additional entropy into the final hash out put.

E. Security Analysis and Parameter Selection

The security of the proposed hash functions is therefore well anchored on the absence of collision attack, preimage attack and second preimage attack. The parameters *k, m, c, p, k,* and *d* are chosen after statistical analyses considering both the computational requirements and the cryptographic security offered there by. The avalanche effect is quantified as

The compression step's modulus p is selected based on its prime properties to ensure effective randomization and minimize cyclic patterns:

$$p = 2^{\alpha} - \beta, \quad \alpha, \beta \in \mathbb{N}$$

with constraints designed to optimize ppp for low-latency performance:

$$V_2 = (V_1 \times R(M_2) + c)\ modp$$

Continuing iteratively

$$V_n = (V_{n-1} \times T(M_n) + c) modp$$

follows: for a small change ΔM in the input:

$$\Delta\,\mathrm{H(M)} = \mathrm{H(M+\Delta M)} - \mathrm{H(M)}$$

Statistical tests are employed to ensure:

$$E[\Delta \mathrm{H(M)}] = \frac{1}{2} \times hashlength$$

Differential cryptanalysis measures the effect of input changes, demonstrating robustness:

$$Pr[\Delta \mathrm{M} \rightarrow \Delta \mathrm{H(M)}] \approx 2^{-\lambda}$$

where λ is the security level parameter ensuring the computational hardness of finding two distinct inputs resulting in the same hash output.

F. Performance Optimization: Mathematical Modifications

The choice of bitwise shift operations k and mmm optimizes processing speed while maintaining nonlinearity.

$$\alpha \approx log_2 \text{ and}$$

β minimizes processing overhead.

This mathematically modified cryptographic framework, with strategically chosen parameters and operations, provides an efficient and secure solution for managing digital

medical data over cloud environments, balancing the need for security, speed, and resource efficiency. The combination of transformation, compression, and modular operations ensures robust cryptographic properties essential for healthcare data protection.

G. Result and Discussion

The evaluation of the proposed cryptographic framework for secure medical data over cloud was done using high end hardware and suitable software platform for proper implementation as well as evaluation of the proposed lightweight cryptographic hash function along with its associated algorithms. The hardware setup was a high end workstation containing an Intel Core i9 processor running at 3. 6 GHz, 32 GB RAM and an NVIDIA RTX 3080 GPU to perform parallel computations. The software environment was installed on a Linux based operating system Ubuntu 22. 04 LTS, Python 3. 10 used for the algorithms' construction and testing. For cryptographic operations, we used PyCryptodome library while the performance tests were tested using scripts created for hash function testing. Data was collected and processed on a secure cloud platform with the use of AWS; AWS S3 was used for data storage while AWS Lambda was used for functions' execution. The data used in the assessment were the patients' demographic data (**See Figure 1**), clinical notes, diagnosis codes, and metadata of medical images from a deidentified Electronic Health Record (EHR) database available to the public via a medical repository. The dataset consisted of roughly 50,000 records with records of different sizes and structures to provide full insight on how the hash function performs in different scenarios, as illustrated in **Figure 2**. Preprocessing also involved the removal of PII to meet requirements such as HIPAA and thus ensure that data privacy had been observed. To match with the block requirements of the hash function, the data was segmented into blocks of 512 bytes, and the enhanced cryptographic function was able to prove its efficacy and security features when dealing with different types of the digital medical data that is usually stored and processed in the cloud environment [22].

.

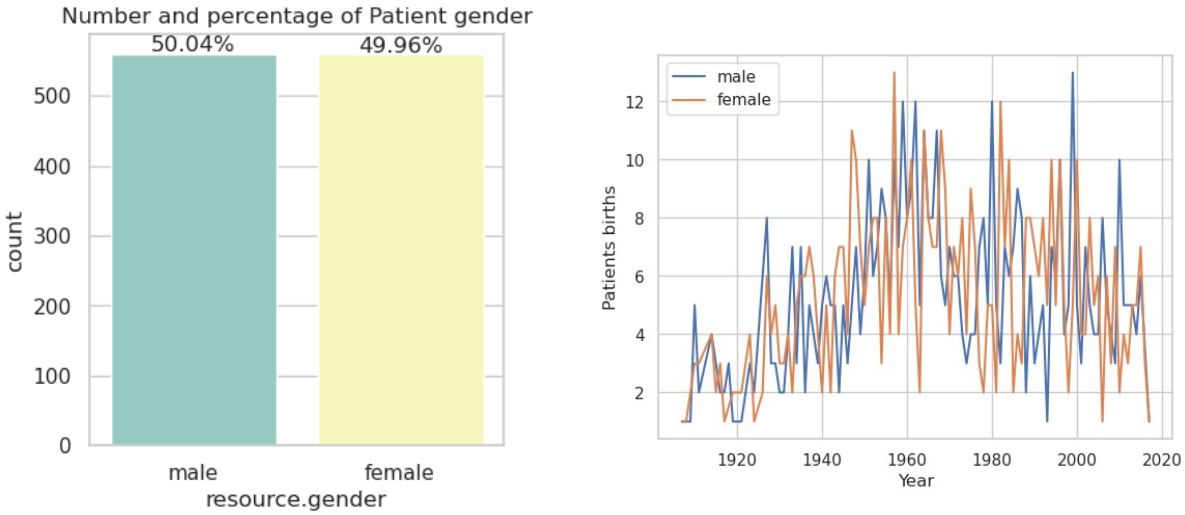

Figure 1. Patient Gender and Birth

Figure 2. Data Distribution

To assess the efficiency of the proposed lightweight cryptographic hash function similar data loads were used to compare significant factors such as processing time, space complexity and energy consumption in cloud environment. The goal was to compare the efficiency of the modified hash function with the standard hash functions like SHA-256 and MD5, to know whether it will fit the requirements of cloud health care systems or not.

Time or T represents the amount of time that the hash functions takes to generate the hash value of a given input data block. This metric is important for all real time applications such as healthcare where data has to be processed in real time.

The processing time T is calculated as:

$$T = \frac{\sum_{i=1}^{n} t_i}{n}$$

where t_i denotes the time taken to process the i^{th} data block and n is the total no of blocks. To this evaluation, the hash function was performed on 50,000 records divided into numerous blocks of 512 bytes as used in the real medical data processing environment.

Memory usage or memory consumption, represented as Mc, depicts the amount of memory required by the cryptographic hash function during its running cycle. This metric is crucial in determining the resource utilization and more so in cloud environment where memory is limited. Memory consumption was measured by monitoring the memory allocation during the execution of the hash function, using the formula:

$$M_C = \frac{\sum_{j=1}^{m} m_i}{m}$$

Where m_j is the memory used in MB during the j^{th} execution and mmm represents the average number of executions performed to reduce variability.

Energy efficiency also known as E_e quantifies the amount of energy used to perform a hash operation, which is essential in cloud setting because decreased energy consumption implies lower cost and environmental impact. Energy efficiency is determined with the energy used by the computing system during hash computation and it is in joules per operation. The energy consumed E can be calculated using the relation:

$$E = P \times T$$

where P represents the power in watts utilized in the system during the execution of the hash function and T represents the time taken. The energy efficiency metric E_e is then calculated as:

$$E_e = \frac{E}{n}$$

where n is the number of times hash operation is to be done

The performance comparison is given in **Table 1** and **Figure 3**.

Table 1. Performance Comparison

Techniques	Time Consumption (ms)	Energy Consumption (j)	Memory Usage (MB)
DNA and HC	765	32.43	5.23
Secured IoMT	652	29.38	6.23
Proposed	453	14.34	3.23

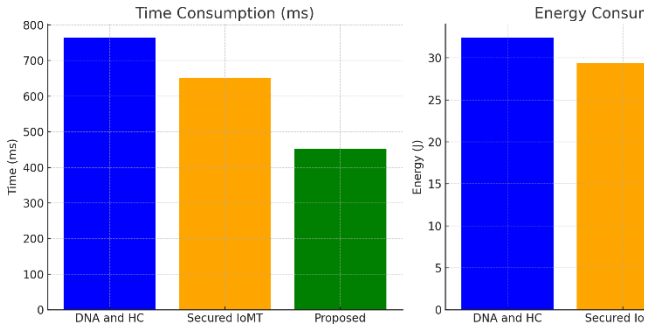

Figure 3. Comparison of Performance

From the results of the comparative analysis of the performance indicators where the values of DNA and HC, Secured IoMT, and the developed cryptographic hash function indicate an increase in the efficiency by 1.7-3 times. Concerning the time complexity, the proposed method is the most efficient with an average time of 453ms, as compared to DNA and HC with an average time of 765ms and Secured IoMT with an average of 652ms. This reduction in time is important especially for real-time health care applications since time is of essence when handling large data sets.

According to the energy consumption aspect, the proposed technique utilizes 14 which is less than the existing techniques. 34 joules which is below half of DNA and HC (32. 43 joules) and much below Secured IoMT (29. 38 joules). This improvement makes it more favourable for scenarios where resources are limited, as is the case of cloud-based systems, where energy consumption is of high concern.

When it comes to memory consumption, the proposed solution takes only 3. 23 MB which is much lesser than DNA and HC (5. 23 MB) and Secured IoMT (6. 23 MB). This implies that the proposed hash function is lighter than the existing ones in terms of memory usage which is a key requirement in cloud environments where memory is usually scarce. The proposed cryptographic method outperforms the benchmark in all three performance parameters of processing

time, energy consumption and memory usage, thereby confirming its applicability for efficient and secure lightweight cryptographic operations in cloud based healthcare data management.

4. Conclusion

The proposed framework of incorporating mathematically modified lightweight cryptographic hash functions improves the overall security of digital medical data over the cloud while at the same time reducing computational costs. The results demonstrate that the framework effectively responds to typical security vulnerabilities in terms of unauthorized access, data contamination, and fake medical records. Due to its ability to run faster, consume less energy and require less memory, it is suitable for cloud based healthcare systems which are very sensitive to resource utilisation. Furthermore, due to the light weight of the hash functions, it can be implemented in real world applications with little resource demands unlike the traditional cryptographic methods.

To conclude, for further improvement the proposed framework may be enhanced and fortified to counter novel threats like quantum computing attacks by the use of post-quantum cryptography. Moreover, with the help of artificial intelligence for threat identification and dynamic security measures, the system's reliability can be enhanced. The adaptability of the framework to work seamlessly with different cloud platforms could also improve its operation in the healthcare systems across the world.

5. Reference

1. Sunyaev, A., & Sunyaev, A. (2020). Cloud computing. *Internet computing: Principles of distributed systems and emerging internet-based technologies*, 195-236.
2. Sadeeq, M. M., Abdulkareem, N. M., Zeebaree, S. R., Ahmed, D. M., Sami, A. S., & Zebari, R. R. (2021). IoT and Cloud computing issues, challenges and opportunities: A review. *Qubahan Academic Journal*, *1*(2), 1-7.
3. Bello, S. A., Oyedele, L. O., Akinade, O. O., Bilal, M., Delgado, J. M. D., Akanbi, L. A., ... & Owolabi, H. A. (2021). Cloud computing in construction industry: Use cases, benefits and challenges. *Automation in Construction*, *122*, 103441.
4. Yanamala, A. K. Y. (2024). Emerging Challenges in Cloud Computing Security: A Comprehensive Review. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(4), 448-479.
5. Thabit, F., Alhomdy, S., Al-Ahdal, A. H., & Jagtap, S. (2021). A new lightweight

cryptographic algorithm for enhancing data security in cloud computing. *Global Transitions Proceedings*, *2*(1), 91-99.

6. Yalamati, S. (2024). Data Privacy, Compliance, and Security in Cloud Computing for Finance. In *Practical Applications of Data Processing, Algorithms, and Modeling* (pp. 127-144). IGI Global.
7. Awadallah, R., Samsudin, A., Teh, J. S., & Almazrooie, M. (2021). An integrated architecture for maintaining security in cloud computing based on blockchain. *IEEE Access*, *9*, 69513-69526.
8. Velmurugadass, P., Dhanasekaran, S., Anand, S. S., & Vasudevan, V. (2021). Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm. *Materials Today: Proceedings*, *37*, 2653-2659.
9. Egermark, M., Blasiak, A., Remus, A., Sapanel, Y., & Ho, D. (2022). Overcoming pilotitis in digital medicine at the intersection of data, clinical evidence, and adoption. *Advanced Intelligent Systems*, *4*(9), 2200056.
10. Sun, M., Xie, L., Liu, Y., Li, K., Jiang, B., Lu, Y., ... & Yang, D. (2022). The metaverse in current digital medicine. *Clinical eHealth*, *5*, 52-57.
11. Berisha, V., Krantsevich, C., Hahn, P. R., Hahn, S., Dasarathy, G., Turaga, P., & Liss, J. (2021). Digital medicine and the curse of dimensionality. *NPJ digital medicine*, *4*(1), 153.
12. Agrawal, R., & Prabakaran, S. (2020). Big data in digital healthcare: lessons learnt and recommendations for general practice. *Heredity*, *124*(4), 525-534.
13. Mahajan, H. B., Rashid, A. S., Junnarkar, A. A., Uke, N., Deshpande, S. D., Futane, P. R., ... & Alhayani, B. (2023). RETRACTED ARTICLE: Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems. *Applied Nanoscience*, *13*(3), 2329-2342.
14. Wu, Z., Xuan, S., Xie, J., Lin, C., & Lu, C. (2022). How to ensure the confidentiality of electronic medical records on the cloud: A technical perspective. *Computers in biology and medicine*, *147*, 105726.
15. Kim, M., Yu, S., Lee, J., Park, Y., & Park, Y. (2020). Design of secure protocol for cloud-assisted electronic health record system using blockchain. *Sensors*, *20*(10), 2913.
16. Selvakumar, K., & Lokesh, S. (2024). A cryptographic method to have a secure communication of health care digital

data into the cloud. *Automatika*, *65*(1), 373-386.

17. Walid, R., Joshi, K. P., & Choi, S. G. (2024). Leveraging semantic context to establish access controls for secure cloud-based electronic health records. *International Journal of Information Management Data Insights*, *4*(1), 100211.
18. Bhansali, P. K., Hiran, D., Kothari, H., & Gulati, K. (2024). Cloud-based secure data storage and access control for internet of medical things using federated learning. *International Journal of Pervasive Computing and Communications*, *20*(2), 228-239.
19. Malathi, K., Shruthi, S. N., Madhumitha, N., Sreelakshmi, S., Sathya, U., & Sangeetha, P. M. (2024). Medical Data Integration and Interoperability through Remote Monitoring of Healthcare Devices. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, *15*(2), 60-72.
20. Veeraiah, V., Thejaswini, K. O., Dilip, R., Jain, S. K., Sahu, A., Pramanik, S., & Gupta, A. (2024). The Suggested Use of Big Data in Medical Analytics by Fortis Healthcare Hospital. In *Adoption and Use of Technology Tools and Services by Economically Disadvantaged Communities: Implications for Growth and Sustainability* (pp. 275-289). IGI Global.
21. Mark, J., & Bommu, R. (2024). Tackling Environmental Concerns: Mitigating the Carbon Footprint of Data Transmission in Cloud Computing. *Unique Endeavor in Business & Social Sciences*, *3*(1), 99-112.
22. Mistry, H. K., Mavani, C., Goswami, A., & Patel, R. (2024). The Impact Of Cloud Computing And Ai On Industry Dynamics And Competition. *Educational Administration: Theory and Practice*, *30*(7), 797-804.
23. https://www.kaggle.com/code/gpreda/electronic-health-records-ehrs-data-exploration