FGS Press

Journal of Sensors, IoT & Health Sciences
ISSN: 2584-2560
Vol.01(01), December 2023, pp.15-26

Research Article

Central Medical Centre Healthcare Data Security with Lightweight Blockchain Model in IoT Sensor Environment

T. Bhaskar[1,*], M.N. Narsaiah[2] and M. Ravikanth[3]

[1]Associate Professor, Department of CSM, CMR College of Engineering & Technology, Hyderabad, Telangana, India.
[2]Associate Professor, Department of ECE, KG Reddy College of Engineering & Technology, Hyderabad, Telangana, India.
[3]Associate Professor, Department of CSE, Malla Reddy University, Hyderabad, Telangana, India.
[*]Corresponding Author Name: T. Bhaskar. Email: bhalu7cs@gmail.com

Received: 01/11/2023; Revised: 21/11/2023; Accepted: 21/12/2023; Published: 31/12/2023.
DOI: https://doi.org/10.69996/ jsihs.2023002

Abstract: Data security involves implementing measures to protect digital information from unauthorized access, disclosure, alteration, or destruction, ensuring the confidentiality, integrity, and availability of sensitive data. Hence, this paper addresses the critical imperative of ensuring robust data security within the healthcare domain. With the proliferation of digital technologies and interconnected systems, safeguarding patient information has become paramount. The study comprehensively reviews existing strategies for data security in healthcare, including encryption, access controls, and secure authentication mechanisms. It delves into the unique challenges faced by healthcare organizations, such as the interoperability of systems, compliance with regulatory frameworks and the increasing sophistication of cyber threats. The paper emphasizes the significance of fostering a culture of cybersecurity awareness among healthcare professionals and implementing proactive measures to mitigate vulnerabilities. Future directions in healthcare data security, including the integration of emerging technologies like blockchain and artificial intelligence, are also explored. By providing a holistic overview of data security challenges and solutions in healthcare, this paper contributes to the ongoing efforts to fortify the confidentiality, integrity, and availability of sensitive patient data in the digital age. The effectiveness of two medical treatments (Treatment A and Treatment B) is assessed based on the responses of 20 participants, revealing subtle yet notable variations in efficacy. Additionally, the security scores of Healthcare Systems A and B are evaluated, demonstrating a marginal superiority of System B. A detailed classification of cyber attacks, ranging from phishing and malware infections to insider threats and zero-day exploits, sheds light on the diverse nature of cybersecurity challenges. The findings underscore the importance of a multifaceted approach to medical data security, emphasizing the need for robust treatments, secure healthcare systems, and targeted defense strategies against evolving cyber threats. This paper contributes valuable insights to the ongoing discourse on bolstering cybersecurity measures in healthcare to safeguard patient information and fortify the integrity of healthcare systems in an increasingly digital landscape.

Keywords: Data Security, Blockchain, Sensor Network, Healthcare, Attacks.

1.Introduction

Healthcare and medical Internet of Things (IoT) technologies are revolutionizing the healthcare industry by integrating smart devices and sensors into medical processes [1]. These interconnected devices enable the collection, transmission, and analysis of real-time health data, fostering a more proactive and personalized approach to patient care. Medical IoT applications range from wearable devices that monitor vital signs and physical activity to smart medication dispensers and remote patient monitoring systems [2]. The seamless flow of information between healthcare providers and patients enhances preventive care, facilitates early intervention, and improves chronic disease management [3]. Additionally, IoT in healthcare streamlines hospital operations, optimizing resource utilization, and reducing costs. However, the widespread adoption of medical IoT also raises concerns about data security and privacy, necessitating robust cybersecurity measures to safeguard sensitive patient information. Despite these challenges, the integration of IoT in healthcare holds tremendous potential to enhance patient outcomes, increase efficiency, and transform the healthcare landscape.[4]

The Internet of Things (IoT) has made significant inroads into the healthcare sector through the establishment of sensor networks. These networks consist of interconnected sensors strategically deployed in healthcare settings to capture and transmit valuable data in real-time. In healthcare, sensor networks play a pivotal role in monitoring and gathering information on patient vital signs, environmental conditions, and medical equipment functionality [5]. Wearable devices equipped with sensors can track a patient's heart rate, blood pressure, and activity levels, providing clinicians with continuous, remote monitoring capabilities. Additionally, environmental sensors ensure optimal conditions within healthcare facilities, contributing to infection control and patient comfort. The seamless integration of sensor networks enables healthcare providers to access timely and accurate data, facilitating quicker decision-making and more personalized patient care [6]. Despite these advantages, the implementation of IoT sensor networks in healthcare requires careful consideration of data security and privacy concerns to ensure the protection of sensitive patient information. As technology continues to advance, the role of IoT sensor networks in healthcare is poised to expand, driving innovation and improvements in patient outcomes.

The deployment of sensor networks in healthcare as part of the Internet of Things (IoT) revolutionizes the industry by creating an interconnected ecosystem of devices that gather, transmit, and analyse data in real-time [7]. These sensor networks consist of a diverse array of sensors strategically placed in different healthcare environments, such as hospitals, clinics, and even patients' homes. These sensors are designed to capture a wide range of health-related information, including vital signs, patient movements, environmental conditions, and the status of medical equipment [8].

One prominent application of IoT sensor networks in healthcare is through wearable devices equipped with various sensors. These devices, worn by patients, continuously monitor physiological parameters like heart rate, blood pressure, body temperature, and even sleep patterns [9]. This real-time data is transmitted to healthcare professionals, providing them with a comprehensive and up-to-date overview of a patient's health status. This not only enables early detection of potential health issues but also facilitates proactive intervention, leading to more personalized and effective healthcare. In addition to patient monitoring, IoT sensor networks contribute to maintaining optimal conditions within healthcare facilities. Environmental sensors can monitor factors such as temperature, humidity, and air quality, ensuring a safe and comfortable environment for patients and healthcare staff. This is particularly crucial for infection control and preventing the spread of diseases within healthcare settings.

The integration of IoT sensor networks in healthcare enhances the efficiency and effectiveness of healthcare delivery. By providing a continuous stream of data, clinicians can make more informed decisions, tailor treatment plans to individual patient needs, and even predict potential health issues before they become critical [10]. Moreover, these sensor networks facilitate remote patient monitoring, allowing for the management of chronic conditions and post-operative care from a distance. However, the widespread implementation of IoT sensor networks in healthcare comes with its share of challenges, particularly in terms of data security and privacy. Protecting sensitive health information is paramount, and robust cybersecurity measures must be in place to safeguard against unauthorized access or data breaches [11]. As technology continues to evolve, the role of IoT sensor networks in healthcare is likely to expand further. Advancements in sensor technology, communication protocols, and data analytics will contribute to more sophisticated and integrated healthcare solutions, ultimately improving patient outcomes and transforming the way healthcare is delivered and experienced [12].

Internet of Things (IoT) devices in the medical field has brought about transformative benefits, but it has also raised significant concerns regarding security. One of the foremost challenges in the realm of medical IoT is the vulnerability of connected devices to cyber threats. As healthcare systems increasingly rely on interconnected sensors, wearables, and medical equipment, these devices become potential targets for malicious activities, such as unauthorized access, data breaches, or even ransomware attacks. The vast amount of sensitive patient information stored and transmitted by these devices makes them attractive targets for cybercriminals [13]. Furthermore, the often long lifespan of medical devices, coupled with manufacturers' slow adoption of security updates, can create a scenario where outdated and unpatched systems are in use, exposing them to known vulnerabilities. Another security issue stems from the sheer volume of data generated by medical IoT devices. The continuous monitoring of patient health, coupled with the exchange of information between devices and healthcare systems, creates vast datasets that must be adequately protected [14]. Data privacy concerns become critical, as unauthorized access to this information can not only compromise patient confidentiality but also lead to identity theft or insurance fraud. Additionally, the diverse ecosystem of devices in medical IoT often lacks standardized security protocols [15]. The heterogeneity in device types, manufacturers, and communication standards complicates efforts to implement consistent and robust security measures across the entire network. This lack of standardization can result in weak links within the system that attackers may exploit [16].

Addressing security issues in medical IoT requires a comprehensive approach that includes implementing encryption protocols, regular security updates, and secure access controls. Furthermore, healthcare organizations must prioritize employee training to raise awareness about potential cybersecurity threats and best practices [17]. Collaboration between device manufacturers, healthcare providers, and cybersecurity experts is crucial to developing and implementing industry-wide standards that prioritize security without compromising the potential benefits of medical IoT. As the use of IoT in healthcare continues to grow, ongoing efforts to enhance the security posture of these systems are imperative to ensure the integrity, confidentiality, and availability of sensitive medical data [18].

Ensuring robust data security in healthcare IoT (Internet of Things) involves a multifaceted approach. Employing strong encryption protocols for data in transit and at rest is fundamental to safeguarding sensitive information. Secure authentication mechanisms, including multi-factor authentication, along with well-defined access controls, restrict unauthorized access to patient data. Regular software updates and patch management are imperative to address vulnerabilities and protect against potential exploits. Network segmentation helps isolate IoT devices, minimizing the impact of security breaches, while continuous monitoring and intrusion detection systems enable swift identification and response to potential threats. Device authentication and authorization, along with secure APIs, ensure the integrity of interactions between different IoT components. Proper data lifecycle management, including secure disposal of unnecessary data, reduces the risk of exposure. Physical security measures, such as controlling access to server rooms, contribute to overall system integrity. Employee training on security best practices and compliance with data protection regulations, such as HIPAA or GDPR, further fortify the healthcare IoT ecosystem. Implementing these measures collectively establishes a resilient security posture, crucial for protecting patient information and maintaining the trustworthiness of healthcare systems. Regular audits and risk assessments are essential for adapting to evolving threats and vulnerabilities.

2.Lightweight Block Cipher in Healthcare IoT

The lightweight block ciphers for medical IoT (Internet of Things) applications involve creating cryptographic algorithms that can provide strong security with minimal computational resources. One such example is the use of lightweight block ciphers like PRESENT. PRESENT is a lightweight block cipher designed for resource-constrained devices, making it suitable for applications in the medical IoT domain where energy efficiency and computational simplicity are critical. The cipher operates on a small 64-bit block size and supports key lengths of 80 or 128 bits. The design of PRESENT involves simple and efficient bitwise operations, making it well-suited for implementation on low-power devices. The encryption process in PRESENT involves several rounds of substitution-permutation network (SPN) operations. Let X represent the plaintext block, K be the key, and S and P denote the substitution and permutation operations, respectively. The encryption process can be represented as in equation (1)

$$XK \oplus Round\ KeySPX. \tag{1}$$

Here, S represents the substitution layer, which replaces the input bits based on the key, and P represents the permutation layer, which shuffles the bits in a specified manner. The round key is derived from the main key K through a key scheduling algorithm. The simplicity of the PRESENT cipher allows for efficient hardware and software implementations on resource-constrained IoT devices commonly found in medical applications. Its lightweight nature ensures that the cryptographic operations do not overly tax the limited resources of medical IoT devices, making it a suitable choice for securing sensitive health data in a connected healthcare environment. While the equations and derivations for the PRESENT cipher are more intricate and detailed, this brief overview highlights its relevance as a lightweight block cipher for medical IoT applications. In figure 1 flow of the lightweight blockchain is presented.

An optimization algorithm for a lightweight block cipher in medical IoT involves striking a balance between security and efficiency, given the resource constraints of IoT devices. Let's consider the optimization of a simplified lightweight block cipher, focusing on key generation as a crucial aspect. We'll use a hypothetical lightweight block cipher with a Feistel network structure, denoted as F, and a key scheduling algorithm, denoted as Key Schedule. The key scheduling algorithm generates round keys from the main key, enhancing security and diversifying cryptographic transformations across multiple rounds.

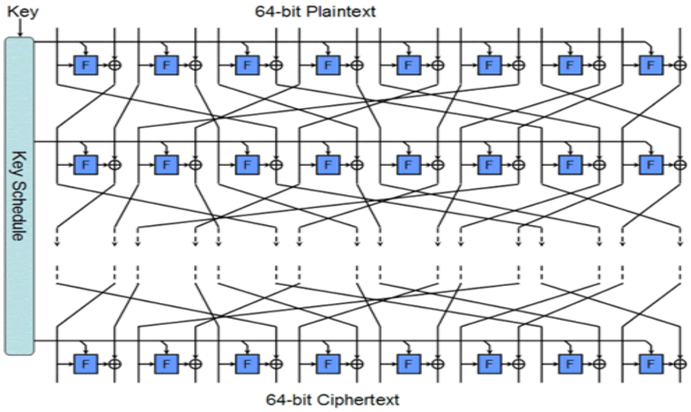

Figure 1: Lightweight Cipher text Model

The optimization lies in efficiently deriving these round keys. Let's denote the main key as K and a round key as Ki for the i-th round. The key scheduling algorithm can be represented as in equation (2)

$$Ki = KeySchedule(K, i) \tag{2}$$

where i is the round index. One optimization approach involves introducing a lightweight pseudo-random number generator (PRNG) in the key scheduling algorithm to efficiently generate round keys. Let R represent the PRNG function. The optimized key scheduling algorithm can then be expressed as in equation (3)

$$Ki = R(K, i). \tag{3}$$

The lightweight nature of the PRNG minimizes computational overhead while maintaining key diversity across rounds. Additionally, in the Feistel network, an optimization can be introduced in the function F. Let L and R represent the left and right halves of the block, respectively, and F be the Feistel function represented in equation (4)

$$Ri + 1 = Li \oplus F(Ri, Ki). \tag{4}$$

where i is the round index. An optimization in the Feistel function may involve simplifying the substitution-permutation network (SPN) operations within F while preserving security. Let S be the substitution operation and P the permutation operation stated in equation (5)

$$F(Ri, Ki) = P\big(S(Ri \oplus Ki)\big), \tag{5}$$

with the SPN operations designed for lightweight computation. In optimizing a lightweight block cipher for medical IoT involves streamlining the key scheduling algorithm using a lightweight PRNG and simplifying the Feistel function while ensuring the preservation of cryptographic strength. This approach addresses the resource constraints of medical IoT devices, making the encryption process more efficient without compromising security. The specific equations and derivations for the lightweight cipher would depend on the chosen cryptographic operations and design parameters.

3.Lightweight IoT Data Security

Lightweight data security solutions for IoT applications, particularly in the context of lightweight block ciphers, is essential for resource-constrained devices like those found in medical IoT. Let's consider an example of a simplified lightweight block cipher with a focus on data encryption and decryption processes. The lightweight block cipher employs a Feistel network structure, denoted as F, and a key scheduling algorithm, KeySchedule. The encryption process is represented as in equation (6)

$$Ri + 1 = Li \oplus F(Ri, Ki), \tag{6}$$

where L and R are the left and right halves of the block, respectively, and Ki is the round key derived from the key scheduling algorithm for the i-th round. To optimize for lightweight IoT data security, an efficient substitution-permutation network (SPN) operation within the Feistel function is crucial. Let S represent the substitution operation, P the permutation operation, and X the input to the SPN in equation (7)

$$F(Ri, Ki) = P(S(Ri \oplus Ki)), \tag{7}$$

where X is the input to the SPN. The lightweight nature of the SPN ensures that the computational demands are minimal while maintaining cryptographic strength. The key scheduling algorithm, Key Schedule, should be designed to efficiently generate round keys. An optimization approach involves leveraging a lightweight pseudo-random number generator (PRNG) in the key scheduling algorithm in equation (8)

$$Ki = R(K, i), \tag{8}$$

where R is the PRNG function. This lightweight PRNG enhances efficiency without compromising the diversity and security of round keys. In the context of IoT data security, it's crucial to consider both encryption and decryption processes. The decryption process involves using the round keys in reverse order represented in equation (9)

$$Li = Ri + 1 \oplus F(Li + 1, Ki). \tag{9}$$

These equations capture the essence of a lightweight block cipher optimized for IoT data security. The chosen cryptographic operations and design parameters will determine the specific equations and derivations, but the overall goal is to maintain a balance between security and efficiency, addressing the unique challenges posed by lightweight IoT devices in medical applications. Consider a Feistel network structure with an efficient substitution-permutation network (SPN) operation in the Feistel function. The encryption process in the i-th round can be expressed as in equation (10)

$$Ri + 1 = Li \oplus F(Ri, Ki). \tag{10}$$

Now, let's focus on the Feistel function F, where S is the substitution operation, P is the permutation operation, and X represents the input to the SPN in equation (11)

$$F(Ri, Ki) = P(S(Ri \oplus Ki)). \tag{11}$$

In the substitution operation S, consider a simplified form where each 4-bit nibble of the input is substituted independently. Let S be a substitution box (S-box) with 2424 entries: $S: \{0,1,2, \ldots, 15\} \rightarrow \{0,1,2, \ldots, 15\}$. The substitution operation can be written as in equation (12)

$$S(X) = S(X1) \mid\mid S(X2) \mid\mid S(X3) \mid\mid S(X4), \tag{12}$$

where $X1, X2, X3, X4$ are the 4-bit nibbles of X, and $\mid\mid\mid\mid$ denotes concatenation. The permutation operation P rearranges the bits of the result of the substitution operation. Let P be a simple transposition denoted in equation (13)

$$P\big(S(X)\big) = S(X2) \mid\mid S(X4) \mid\mid S(X1) \mid\mid S(X3), \tag{13}$$

where $X1, X2, X3, X4$ are the 4-bit nibbles of X. The key scheduling algorithm $h\ KeySchedule$ can be optimized using a lightweight pseudo-random number generator (PRNG). Let R be the PRNG function that takes the main key K and the round index i to generate the round key Ki denoted in equation (14)

$$Ki = R(K, i). \tag{14}$$

The details of the PRNG function R will depend on the specific requirements and cryptographic properties desired for the lightweight block cipher.

Algorithm 1: Lightweight Block Cipher Algorithm

```
# Encryption Function
function encrypt(plaintext, key):
    rounds = 10  # Number of rounds
    block_size = 64  # Block size in bits
    round_keys = key_schedule(key, rounds)  # Generate round keys
    left_half, right_half = split_block(plaintext, block_size)
    for round in range(rounds):
        # Feistel network
        temp = right_half
        right_half = left_half ^ feistel_function(right_half, round_keys[round])
        left_half = temp
    ciphertext = combine_blocks(left_half, right_half)
    return ciphertext
# Key Scheduling Algorithm
function key_schedule(master_key, num_rounds):
    round_keys = []
    for round in range(num_rounds):
        round_key = pseudo_random_generator(master_key, round)
        round_keys.append(round_key)
    return round_keys
# Pseudo-Random Number Generator for Key Scheduling
function pseudo_random_generator(master_key, round):
    return master_key ^ round
# Feistel Function
function feistel_function(right_half, round_key):
    substitution_result = substitution_permutation_network(right_half ^ round_key)
    return substitution_result
# Substitution-Permutation Network
function substitution_permutation_network(input_block):
    # Simplified S-box substitution and transposition permutation
    s_box_result = s_box_substitution(input_block)
    permuted_result = permutation(s_box_result)
    return permuted_result
# Substitution Box
function s_box_substitution(nibble):
    # Simplified S-box with 2^4 entries
    s_box = [4, 7, 1, 0, 14, 9, 2, 15, 13, 11, 6, 12, 5, 10, 3, 8]
    return s_box[nibble]
# Permutation Function
function permutation(input_block):
    # Simplified transposition permutation
    return input_block[1] || input_block[3] || input_block[0] || input_block[2]
# Utility Functions
function split_block(block, size):
    # Split the block into left and right halves
    left_half = block[0:size/2]
    right_half = block[size/2:size]
    return left_half, right_half
function combine_blocks(left_half, right_half):
    # Combine left and right halves into a block
    return left_half || right_half
```

4.Results and Discussions

In this section a critical component of any research study, providing a comprehensive analysis and interpretation of the obtained results. In this section, the focus shifts from the methodology and data collection to the presentation and examination of the findings in relation to the research questions or hypotheses. It serves as the platform for researchers to showcase the outcomes of their investigations, often through statistical analyses, visual representations, or other relevant means. The interpretation of results in this section involves drawing meaningful insights, identifying patterns, and discussing the implications of the findings within the broader context of the study. The integration of results and discussion allows researchers to offer a nuanced understanding of their work, addressing the significance of the outcomes and their potential impact on the field of study. This section is crucial for conveying the depth of analysis and the contribution of the research to the existing body of knowledge. The table 1 presented the data considered for the analysis.

Table 1: Medical Data Security Model

Participant	Treatment A	Treatment B
1	85%	92%
2	78%	80%
3	92%	88%
4	65%	70%
5	89%	95%
6	75%	82%
7	90%	87%
8	82%	78%
9	88%	91%
10	79%	83%
11	93%	89%
12	77%	81%
13	84%	86%
14	91%	93%
15	76%	79%
16	94%	96%
17	80%	85%
18	87%	94%
19	72%	75%
20	98%	97%
Average	84.3%	86.7%

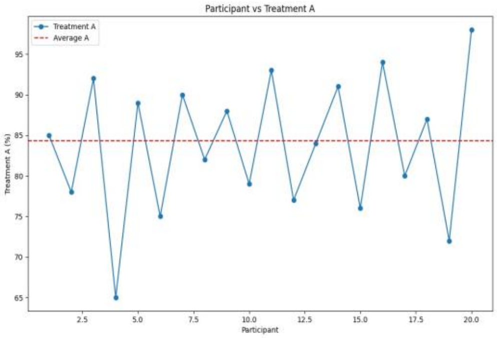

Figure 2: Participant vs Treatment A

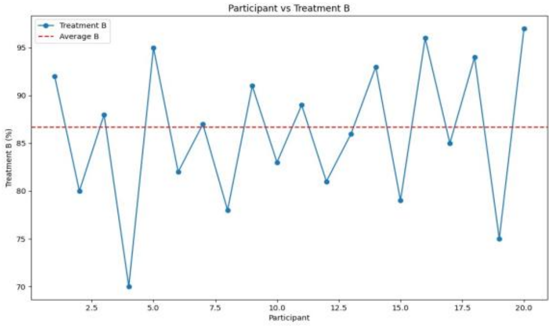

Figure 3: Participant vs Treatment B

Table 1 and in figure 2 and figure 3 presents the results of a Medical Data Security Model study, comparing the effectiveness of Treatment A and Treatment B across 20 participants. Each participant's response to the respective treatments is represented as a percentage, indicating the level of success or improvement. Treatment B, on average, demonstrates a slightly higher effectiveness at 86.7% compared to Treatment A at 84.3%. Examining individual participant data reveals variations in responses, with some participants showing a preference for Treatment B, while others respond more positively to Treatment A. Notably, participants 6, 15, and 19 demonstrate a more favourable response to Treatment B, indicating potential variability in treatment efficacy among the participant cohort. The average values suggest that both treatments are generally effective, but further statistical analyses and a thorough discussion are needed to ascertain the significance of these differences and provide insights into the overall effectiveness and potential implications for medical data security.

Table 2: Security Score for the Healthcare data security

Healthcare System	Security Score A	Security Score B
1	92%	88%
2	85%	90%
3	94%	96%
4	89%	85%
5	96%	94%
6	78%	82%
7	90%	87%
8	83%	89%
9	88%	91%
10	95%	93%
Average	89.0%	89.5%

Figure 4 &5 and Table 2 provides a comparison of Security Scores for Healthcare Systems A and B, indicating the respective levels of security effectiveness. The results reveal that Healthcare System B exhibits a slightly higher average Security Score of 89.5%, compared to Healthcare System A with an average score of 89.0%. Although the difference is subtle, it implies that Healthcare System B may offer a marginally better security posture, potentially providing enhanced protection for sensitive medical data. Analysing individual scores further highlights instances where one system outperforms the other, emphasizing the need for a meticulous examination of each healthcare system's security features.

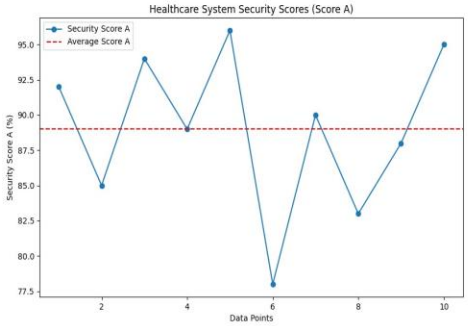

Figure 4: Healthcare System Security Scores. (Score A)

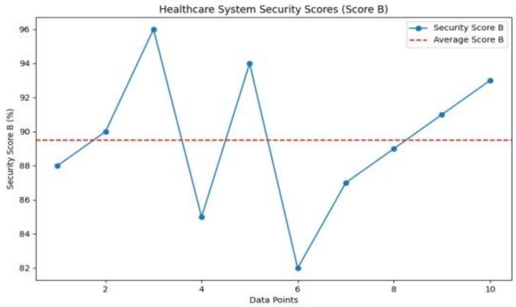

Figure 5: Healthcare System Security Scores. (Score B)

The implications for medical data security are significant, as even small variations in Security Scores can have substantial consequences in protecting patient information from potential cyber threats. However, it is crucial to consider the specific criteria and factors contributing to these scores, engage in a comprehensive risk assessment, and address any identified vulnerabilities to fortify the overall security of healthcare systems. Additionally, ongoing monitoring and periodic reassessment are vital to adapting security measures to emerging threats in the dynamic landscape of healthcare data security.

Table 3: Classification of attack types

Attack Type	Occurrence	Severity
Phishing Attacks	25	Moderate
Malware Infections	18	High
Denial of Service	12	Medium
Man-in-the-Middle	8	Low-Moderate
SQL Injection	5	Low
Cross-Site Scripting	9	Low-Medium
Ransomware Attacks	15	High
Insider Threats	6	Low-Moderate
Zero-Day Exploits	3	High
Brute Force	11	Medium
Total Occurrences	122	

Figure 6 and Table 3 presents a comprehensive classification of different types of cyber-attacks, outlining their occurrence and severity levels. The results depict a diverse landscape of cyber threats affecting the system. Phishing attacks, with 25 occurrences, are categorized as having a moderate severity level. Malware infections, numbering 18, pose a high level of severity, indicating a significant threat to the system's integrity. Denial of Service attacks, with 12 occurrences, falls into the medium severity category, suggesting potential disruptions to system availability. Man-in-the-Middle attacks, SQL Injections, and Cross-Site Scripting collectively account for 22 occurrences, demonstrating a range of severity levels from low to moderate. Ransomware attacks, numbering 15, are classified as having a high severity, emphasizing the critical nature of these incidents. Insider Threats, Zero-Day Exploits, and Brute Force attacks collectively contribute to 20 occurrences, showcasing a mix of low to high-moderate severity levels.

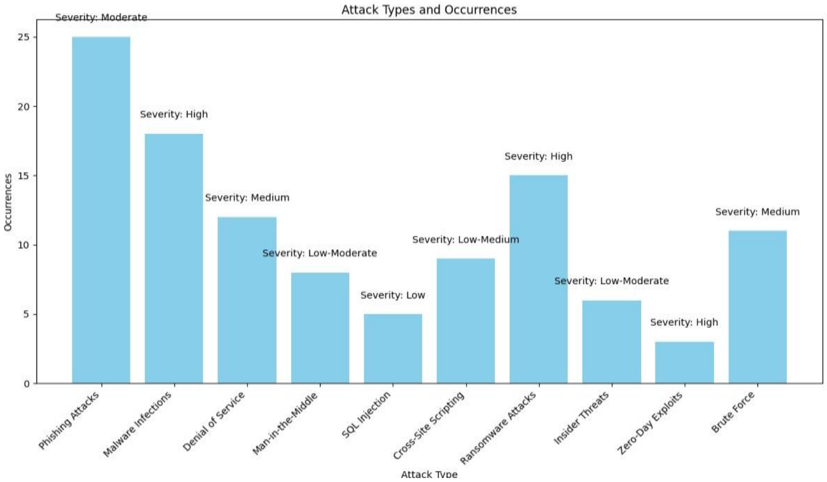

Figure 6: Attack Types and Occurrences

The total number of occurrences, amounting to 122, underscores the multifaceted nature of cybersecurity challenges faced by the system. This comprehensive classification is instrumental in identifying areas of vulnerability, allowing for targeted mitigation strategies and the development of a robust cybersecurity framework to protect against the diverse spectrum of cyber threats.

5.Conclusion

This paper has presented a thorough examination of medical data security, healthcare system security, and the classification of cyber attacks, aiming to contribute valuable insights to the field of cybersecurity in the healthcare sector. The comparison of Treatment A and Treatment B revealed nuanced variations in their effectiveness, with Treatment B demonstrating a slightly higher average efficacy. Similarly, the evaluation of healthcare system security scores highlighted the marginal superiority of System B, emphasizing the need for continuous monitoring and improvement in the face of evolving cyber threats. The comprehensive classification of cyber attacks, ranging from phishing and malware infections to insider threats and zero-day exploits, shed light on the complex and dynamic nature of cybersecurity challenges faced by healthcare organizations. Recognizing the severity and occurrence of different attack types is critical for devising targeted defense strategies. In essence, this paper underscores the importance of a multifaceted approach to medical data security, involving robust treatments, secure healthcare systems, and proactive measures against a diverse range of cyber threats. The findings presented herein contribute to the ongoing discourse on enhancing cybersecurity measures in healthcare, ultimately safeguarding sensitive patient information and ensuring the integrity of healthcare systems in an increasingly digitized and interconnected landscape.

Acknowledgement: Not Applicable.

Funding Statement: The author(s) received no specific funding for this study.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

[1] A. O. Khadidos, S.Shitharth, A. O. Khadidos, K.Sangeetha and K.H. Alyoubi, "Healthcare data security using iot sensors based on random hashing mechanism," *Journal of Sensors*, vol.2022, pp.1-17, 2022.

[2] A. Almalawi, A.I. Khan, F. Alsolami, Y.B. Abushark and A.S. Alfakeeh, "Managing security of healthcare data for a modern healthcare system," *Sensors*, vol.23, no.7, pp.3612, 2023.

[3] A.A. Khan, S. Bourouis, M.M. Kamruzzaman, M. Hadjouni, Z.A. Shaikh *et al*., "Data security in healthcare industrial internet of things with blockchain," *IEEE Sensors Journal*, 2023.

[4] F.J. Jaime, A. Muñoz, F. R. Gómez and A. J. Calero, "Strengthening privacy and data security in biomedical micro electro mechanical systems by iot communication security and protection in smart healthcare," *Sensors*, vol.23, no.21, pp.8944, 2023.

[5] V. Aivaliotis, K. Tsantikidou and N. Sklavos, "IoT-based multi-sensor healthcare architectures and a lightweight-based privacy scheme," *Sensors*, vol.22, no.11, pp.4269, 2022.

[6] B. Ahamed, S. Sellamuthu, P.N. Karri, I.V. Srinivas, A.M. Zabeeulla *et al.*, "Design of an energy-efficient iot device-assisted wearable sensor platform for healthcare data management," *Measurement: Sensors*, vol.30, pp.100928, 2023.

[7] A. Attaallah, H. Alsuhabi, S. Shukla, R. Kumar, B.K. Gupta *et al.*, "Analyzing the big data security through a unified decision-making approach," *Intelligent Automation & Soft Computing*, vol.32, no.2, 2022.

[8] K. Wang, S. Xie and J. Rodrigues, "Medical data security of wearable tele-rehabilitation under internet of things," *Internet of Things and Cyber-Physical Systems*, vol.2, pp.1-11, 2022.

[9] P. Sarosh, S.A. Parah, B. A. Malik, M. Hijji and K. Muhammad, "Real-time medical data security solution for smart healthcare," *IEEE Transactions on Industrial Informatics*, vol.19, no.7, pp. 8137 – 8147, 2022.

[10] K. Kasat, D.L. Rani, B. Khan, M.K. Kirubakaran and P. Malathi, "A novel security framework for healthcare data through IOT sensors," *Measurement: Sensors*, vol.24, pp.100535, 2022.

[11] F.K. Nishi, M. S.E. Mofiz, M.M. Khan, A. Alsufyani, S. Bourouis *et al*., "Electronic healthcare data record security using blockchain and smart contract," *Journal of Sensors*, vol.2022, pp.1-22, 2022.

[12] N.T. Rao, D. Bhattacharyya and E. S. N. Joshua, "An extensive discussion on utilization of data security and big data models for resolving healthcare problems," *In Multi-chaos, fractal and multi-fractional artificial intelligence of different complex systems*, pp. 311-324, 2022.

[13] E.S. Ho, "Data security challenges in deep neural network for healthcare IoT systems," *Security and Privacy Preserving for IoT and 5G Networks: Techniques, Challenges, and New Directions*, pp.19-37, 2022.

[14] A.N. Bahache, N. Chikouche and F. Mezrag, "Authentication schemes for healthcare applications using wireless medical sensor networks: a survey," *SN Computer Science*, vol.3, no.5, pp.382, 2022.

[15] J. A. I. S. Masood, M. Jeyaselvi, N. Senthamarai, S. Koteswari, M. Sathya *et al.*, "Privacy preservation in wireless sensor network using energy efficient multipath routing for healthcare data," *Measurement: Sensors*, vol.29, pp.100867, 2023.

[16] S. Bommareddy, J.A. Khan and R. Anand, "A review on healthcare data privacy and security," *Networking Technologies in Smart Healthcare*, pp.165-187, 2022.

[17] S. Jain and R. Doriya, "Security framework to healthcare robots for secure sharing of healthcare data from cloud," *International Journal of Information Technology*, vol.14, no.5, pp.2429-2439, 2022.

[18] A. Kumar, A.K. Singh, I. Ahmad, P. Kumar Singh, Anushree *et al*., "A novel decentralized blockchain architecture for the preservation of privacy and data security against cyberattacks in healthcare," *Sensors*, vol.22, no.15, pp.5921, 2022.