Iraqi Journal for Computer Science and Mathematics

Journal Homepage: http://journal.esj.edu.iq/index.php/IJCM
e-ISSN: 2788-7421 p-ISSN: 2958-0544

Improving security in the 5G-based medical Internet of Things to improve the quality of patient services

Kholood J.Moulood[1], Muneer Sameer Gheni Mansoor [2], Israa Ibraheem Al_Barazanchi [3], Jamal Fadhil Tawfeq [4]

[1] Department of Mathematics, College of education for women, Tikrit University, Iraq
[2]Department of Mobile Communications and Computing Engineering, College of Engineering, University of Information Technology and Communications (UOITC), Baghdad, Iraq
[3] Department of Communication Technology Engineering, College of Information Technology, Imam Ja'afar Al-Sadiq University, Baghdad, Iraq.
[4] Department of Medical Instrumentation Technical Engineering, Medical Technical College, Al-Farahidi University, Baghdad, Iraq

*Corresponding Author: Israa Ibraheem Al_Barazanchi

DOI: https://doi.org/10.52866/ijcsm.2024.05.03.017
Received February 2024; Accepted May 2024; Available online August 2024

ABSTRACT: The Internet of Medical Things (IoMT) is like a tech upgrade that benefits patients by reducing healthcare costs, making medical care more accessible, and improving the quality of treatment. To make IoMT devices smart and capable, they need super-fast 5G support. However, there are security concerns when using IoMT devices that can put a patient's data and privacy at risk. For instance, someone could eavesdrop on your medical data due to weak network access management and data encryption. Many systems use encryption methods to protect data, but these methods often fall short when it comes to the high security standards required for healthcare data and patient service quality. In our research, we introduce a new solution called the Hybrid MD5 and Threefish Encryption (HMTE) to make IoMT more secure and improve the quality of care for patients. To ensure efficient use of energy, we employ a smart approach when choosing a cluster head. When it comes to sending data, we use the Trust-Based Energy Efficient Routing Protocol (TEERP). We carefully evaluate different aspects like cost, encryption and decryption speed, and the level of security while analyzing our proposed method. We also compare our solution with existing methods. Our data shows that our recommended solution outperforms existing methods, particularly in terms of enhancing security to improve the quality of care for patients.

Keywords: Fifth generation(5G), Internet of Medical Things (IoMT), Security Enhancement, Healthcare quality of service (QoS), Encryption, Hybrid MD5 and Threefish Encryption (HMTE)

1. INTRODUCTION

Today, the Internet is used by various entities, including businesses, organizations, governments, and individuals, for a wide range of purposes. By 2020, it was estimated that over fifty billion devices would be connected to the Internet. This interconnected web of devices is what we refer to as the "Internet of Things (IoT)." In simple terms, IoT is a network of devices, like computers, sensors, and other gadgets, that can share information and communicate with each other and their surroundings [1-3]. IoT has many practical applications, such as environmental monitoring and healthcare. The healthcare sector, in particular, places great importance on the Internet of Medical Things (IoMT), sometimes called the Internet of Healthcare Things (IoHT). Think of IoMT as a collection of tools that use the internet to do things like monitoring patients and collecting data through sensors [4-7]. The introduction of 5G technology has brought exciting possibilities, especially in areas like healthcare. With 5G's high-speed data transfer and processing capabilities, we can create real-time healthcare systems that can potentially save lives. For example, wearable devices like smartwatches can quickly share critical health data with both medical professionals and loved ones in emergency situations [8]. However, it's important to ensure the quality of service, especially when it comes to IoMT. This means making sure that the data is transmitted without delay, which is crucial in healthcare. IoMT also has the potential to bring advanced medical services to rural areas, connecting patients with expert care providers. Information security has three main components: availability (making sure data is accessible), integrity (keeping data accurate and complete), and confidentiality (limiting who can access the data). In the digital world of IoMT, we must safeguard information not only from cyber threats but also from physical breaches. The healthcare industry, in particular, relies on patient data confidentiality. Protecting patient data is crucial for the financial stability and reputation of medical facilities, and it can even be a matter of life and death. Health records are often

stored in outdated systems, making data transfer difficult due to different formats and standards. Ensuring the privacy of patient records is vital in evaluating the quality of healthcare providers. IoT and 5G technology offer numerous opportunities, but they also bring a pressing need for enhanced data security, especially in the healthcare sector. Patient confidentiality must be a top priority to protect their well-being and the reputation of healthcare providers [9-13].

2. METHOD

The 5G-based medical IoT is a rapidly advancing technology that can revolutionize healthcare. It enables the connection of medical devices like wearables, sensors, and implants to the internet, allowing for remote monitoring and diagnosis of patients. However, this technology also introduces security concerns. Therefore, it's crucial to establish safety measures to safeguard patient information and prevent unauthorized access. One effective way to enhance security in the 5G-based medical IoT is through encryption. Encryption ensures that data transmitted across the network is secure and accessible only to authorized users. Additionally, authentication protocols can verify user identities before granting access to sensitive information. Another method to bolster security in the 5G-based medical IoT is by implementing secure communication protocols. These protocols ensure that data sent over the network is both encrypted and authenticated before transmission, reducing the risk of malicious interception or tampering with sensitive data. It's essential to keep all devices connected to the 5G-based medical IoT regularly updated with the latest security patches and software updates. This practice helps protect against known vulnerabilities and ensures that all devices remain resilient against potential threats. By implementing these security measures, healthcare providers can ensure the confidentiality of their patients' data while also enhancing the quality of patient services. This is achieved by providing more accurate diagnoses and treatments based on real-time data collected from connected devices. In this section, we present a unique Hybrid MD5 and Threefish Encryption (HMTE) technique to address these security concerns, ultimately improving patient Quality of Service (QoS) by elevating the security level of health data. This system utilizes a Wireless 5G network to gather patient information from IoMT devices. The data is pre-processed with normalization, and feature selection is employed to reduce the amount of data transmitted. To ensure secure transmission, the data is encrypted and decrypted. An energy-efficient routing protocol is used to ensure trust-based data transmission. Figure 1 illustrates the framework of this system [14-16].

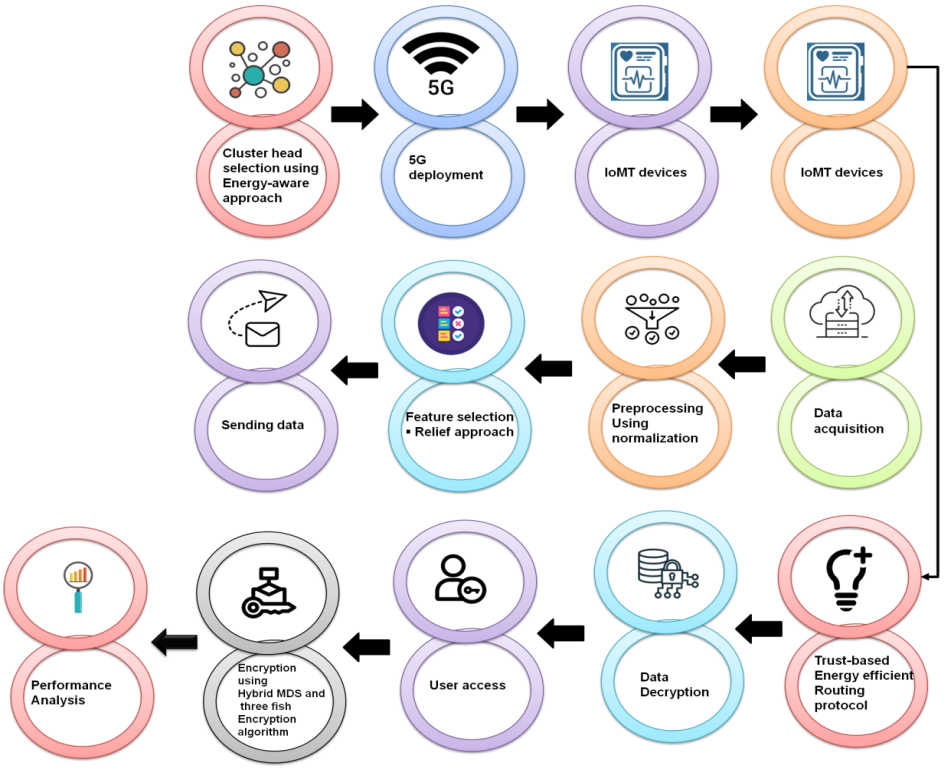

Figure 1. Framework of proposed work

2.1 Data acquisition

A predictive model for assessing the risk of heart disease was meticulously developed by leveraging datasets from the UCI machine learning repository, the Framingham study, and the Public Health Dataset. Through a comprehensive analysis of numerous characteristics, we identified and selected 14 key features for inclusion in our published research [17-30]. These critical attributes are detailed in Table 1. This model has demonstrated remarkable accuracy in predicting heart disease when relying solely on these 14 selected features. Moreover, our model offers an invaluable tool for healthcare professionals in identifying individuals at heightened risk of developing heart disease. Equipped with this model, medical practitioners can promptly recognize such patients and provide them with appropriate and timely treatment, potentially preventing the onset of heart-related health issues. Furthermore, to enhance the robustness and reliability of our research, we also harnessed data from the Hungarian heart disease database [31], which encompassed a total of 76 attributes. This expanded dataset further enriched our understanding of heart disease risk factors, ultimately contributing to the comprehensive insights presented in our study.

2.2 Preprocessing using Normalization

Normalization is a preprocessing technique designed to adjust or scale data in a way that ensures each characteristic has an equal impact on the overall result. This technique involves creating a new data range based on an existing one, and it can significantly enhance the quality of predictions and projections derived from this data. Regardless of the transformations applied to the raw data, each feature retains its informative value, addressing significant data challenges that can hinder machine learning algorithms, such as handling outliers and dominant characteristics. Various methods for normalizing data within a specific range have been developed, each of which relies on statistical measures derived from the raw, unnormalized data. In our approach, we utilized the Min-Max and Z-score techniques to adjust our data, resulting in a more consistent distribution. These normalization techniques are categorized based on the statistical properties of the data employed in the process. These properties may encompass measures like the mean, median, standard deviation, and other indicators of central tendency and variability. By thoroughly understanding these statistical properties, we can choose the most appropriate normalization method that best suits the specific dataset and its intended application. Min-max normalization, for instance, linearly transforms data to fit within predefined minimum and maximum bounds, preserving the relative relationships between data points. This strategy ensures that the data retains its integrity while being adjusted to fit within predefined boundaries, a key aspect of effective data normalization.

$$O' = \left(\frac{O - minvalueofO}{maxvalueofO - min\ valueofO}\right) * (S - J) + J \tag{1}$$

In this context, the variable "O" contains essential min-max information, with one boundary specified as [J, S]. The data mappings encompass a range defined by "O," while the actual data values are assigned within this range. A valuable technique to enhance the quality of data is to ensure that all numerical values are transformed to a consistent scale, facilitating easier comparison and analysis. To achieve this, we employ a normalization method known as the "A score normalization." This method serves the purpose of placing the data into a unified and standardized scale. The A score normalization technique ensures that data points are adjusted in a way that allows for fair and meaningful comparisons among them. This is especially useful when dealing with data from different sources or with varying units of measurement. The formula for calculating Z-scores, which is a crucial aspect of A score normalization, is provided in Equation 2. This formula enables the transformation of data into a standardized scale, making it easier to identify trends, anomalies, and patterns in the dataset. By applying such normalization techniques, we ensure that data becomes more interpretable and can be used effectively for analysis and decision-making in various fields, such as statistics, finance, and data science.

$$A = Y - \frac{\mu}{\sigma} \tag{2}$$

In this context, the variable "A" represents the typical frequency of a value within the dataset. On the provider's side, "Y" denotes the logistical quantities of associated characteristics. The variable "Z" serves as a weighted average encompassing all functions of a similar nature that are employed in user operations. This weighted average, often used for assessing and aggregating user interactions, plays a crucial role in the analysis. The normalized mean, often referred to as the "A" score, is a key metric in this context. It is designed to have a mean value of zero and a standard deviation of one when data is correctly normalized. This means that the A score is centered at zero, with a standard deviation of one, ensuring that the data is in a standard form for comparison and analysis. Furthermore, to gauge the variability within the dataset, the average variance can be calculated using Equation 3. This measure provides valuable insights into the spread and distribution of data points, which is essential for assessing the data's

consistency and reliability. By considering variables like "A," "Y," and "Z," along with metrics like the A score and average variance, we create a robust framework for analyzing and understanding data patterns, ensuring that the data is prepared for meaningful analysis and decision-making. These tools and techniques are indispensable in a wide range of fields, including statistics, data science, and business analytics.

$$\sigma = \sqrt{(\sum (Y - \bar{Y})/o)} \quad (3)$$

Considering that "Y" represents the quantity of services requested by users, it is important to note that "Y" also encompasses the items provided by the client. For each specific variable, the average value is denoted by "Y." The total number of data samples obtained from various sources is represented by "O." To ascertain the "A grade," several statistical measures including the standard deviation, mean, and frequency distribution are employed on a supply user test dataset. These measures help in evaluating and grading the data, providing valuable insights for decision-making and analysis.

Table 1. Summary of Dataset

Attribute	Description
Age	Age of the patient in years
Chol	Serum cholesterol level in mg/dL
Sex	Gender of the patient (1 for male, 0 for female)
CAV	Count of major blood vessels visible on fluoroscopy (ranging from 0 to 3)
FBS	Fasting blood sugar level (>120 mg/dL: 1 for true, 0 for false)
ST_Depression	Reduction in ST segment during exercise relative to rest
Resting_BP	Resting blood pressure upon hospital admission (measured in mmHg)
Max_Heart_Rate	Maximum heart rate achieved
Target	Presence of heart disease (0 for no disease, 1-4 for varying levels of narrowing of arteries)
Exercise_Angina	3 = Exercise-induced angina, 0 = No angina, 1 = Yes angina, 6 = Chronic angina
Thal	Thalassemia type
Chest_Pain	Chest pain category (Typical angina, Atypical angina, Non-anginal pain, Asymptomatic)
ST_Slope	ST segment slope during peak exercise (Upsloping, Flat, Downsloping)
Resting_ECG	Resting electrocardiogram findings (Normal, Abnormal ST-T wave pattern, Left ventricular hypertrophy)

2.3 Feature selection using the Relief approach

Feature selection techniques play a pivotal role in the machine learning process as they help identify the most relevant features for effective categorization. Furthermore, they contribute to the acceleration of the execution process. In this paper, we employ the Relief approach for feature selection. Relief is an attribute selection method that assigns weights to each feature in the dataset. These weights are then adjusted progressively. Essential characteristics are given substantial weight, while less crucial features receive lower weightings. To calculate these feature weights, Relief employs techniques similar to those utilized by the k-Nearest Neighbors (KNN) algorithm. It starts by selecting a random instance, denoted as Sj. Then, Relief identifies the two nearest neighbors: the closest hit, denoted as I (belonging to the same class), and the closest miss, denoted as N (belonging to a different class). Based on the values of Sj, N, and I, Relief computes the consistency score X[B] for each feature A. If there is a significant difference between Sj and I, the performance value X[B] is reduced because such discrepancies are undesirable. Conversely, if there is a notable difference between Sj and N for feature B, it suggests that B can effectively distinguish between different classes, and therefore, the weight X[B] is increased. This process is repeated iteratively, typically n times, with n being a modifiable variable. The Relief approach algorithm is an iterative method used to identify the most pertinent features in a dataset. It operates by assessing the disparities between feature values and their closest matches and mismatches for each instance in the dataset. The algorithm then adjusts the feature weights based on these disparities. In essence, Relief assesses feature performance by evaluating how well their values differentiate between similar events. To do this, it randomly selects an instance X from a set S containing k features, then finds the two closest neighbors: one from the same class (the nearest hit, H) and one from a different class (the nearest miss, M). For each feature Sj, Relief updates the quality estimate W[Sj] using the difference function diff for X, H, and M. If a parameter m is set, this process is repeated m times. The diff (Sj(y_1j, y_2j)) function quantifies the gap between two feature Sj values (y_1j and y_2j) for a pair of instances, y_1 and y_2. The normalization with m ensures that all weights fall within the range of [-1, 1].

$$2.4\ diff\left(\mathrm{Sj}, y_{1j}, y_{2j}\right) = \begin{cases} |y_{1j} - y_{2j}| if\ \mathrm{Sj}\ is\ numeric, \\ 0\ if\ \mathrm{Sj}\ is\ nomial\ y_{1j} = y_{2j}, \\ 1\ if\ 1\ \mathrm{Sj}\ is\ nomial\ y_{1j} \neq y_{2j}, \end{cases} \quad (4)$$

Relief has an O-time complexity for N-instance data sets (*yjN*). The Relief family of algorithms has a significant efficiency advantage over competing methods. In the limit when m is fixed, the time complexity is O. (jN). However, a greater m indicates more trustworthy approximations, as m is the number of in stances used to estimate probability. It is common practise that m N be met when N is big.

2.5 Secured multi-path and trust-based Energy Efficient routing protocol (SM-TEERP)

This routing technique employs multipath routing, depending on node queue length and minimal energy usage, to establish routes from the destination to the source. Additionally, it provides defense against various Wireless Sensor Network (WSN) attacks, such as sinkhole and selective forwarding attacks. The protocol assumes random node placement and treats wireless sensor networks as undirected graphs. The transmission range for each sensor node is fixed and cannot be modified. Furthermore, each sensor node possesses both private and public keys. The process begins with the selection of a cluster head node. This protocol consists of two phases: route creation and data transfer. In the route creation phase, every node in the network constructs a routing table. During this phase, each sensor node sends the packet once and updates its routing table accordingly. In the subsequent data transmission phase, the optimal path cost is used to determine the primary path for data transfer. This decision takes into account factors such as the remaining energy in a node and the length of its queue to identify the most efficient routing path. The results of implementing this protocol indicate improvements in data packet delivery, reduced average end-to-end latency, adjusted routing load, and decreased energy usage. Algorithm 1 outlines the procedure of SM-TEERP, providing a structured representation of the protocol's operations.

Algorithm 1: Secured multi-path and trust-based Energy Efficient routing protocol

Initialization:

N = {B}

for every node w

if the trust is maximum when w is next to B.

then $E(W_i) = d(B,w)$

else $E(W_i) = \infty$

Loop

Identify x such that E(x) is the lowest in terms and it is not in N

Power and Trust in Transmission (lower values)

HIGH Trust is indicated by a value of trust; for instance, trust with a value of 1 is regarded as HIGH Trust).

to N, add x.

E(w) should be updated for any w that is close x but not in N.:

$E(w_j)_u = min\ (E(w), E(x) + d(x,w)$

$\left| E(w_{i+1}) = min\ (E(w), max\ (Disjoint\ E(wj))\right.$

/ the previous cost to w or the known cost to w,*

*shortest route costs to x and w */*

until *every node in N*

If $\left| E(wj)_u - E(wj)_{u-1} \right| \leq threshold$ ***then***

$E(wj)_u - E(wj)_{u-1}$ */*No change in the existing path*/*

else

$E(wj)_u$

2.6 Encryption using hybrid MD5 and Threefish encryption algorithm

Encryption using the hybrid MD5 and Threefish encryption algorithm is a data encryption method that combines the MD5 hashing algorithm with the Threefish symmetric-key block cipher. In this process, the MD5 hashing algorithm

generates a unique key for each message, while the Threefish cipher encrypts the message itself. This combination enhances security by ensuring that even if an attacker gains access to the encrypted data, decryption is only possible with the unique key generated by the MD5 hashing algorithm. The MD5-Threefish encryption technique is designed to offer superior security without compromising speed. It consists of three primary components: a key generation module, an MD5 key expansion module, and a Threefish data encryption module. The data encryption module takes the encrypted key from the MD5 key expansion module and the key expansion module and uses it to encrypt the data. You can visualize this process in Figure 2. For further security enhancement, this technique can be integrated with other encryption methods, creating a multi-layered approach that provides even stronger protection against malicious attacks.

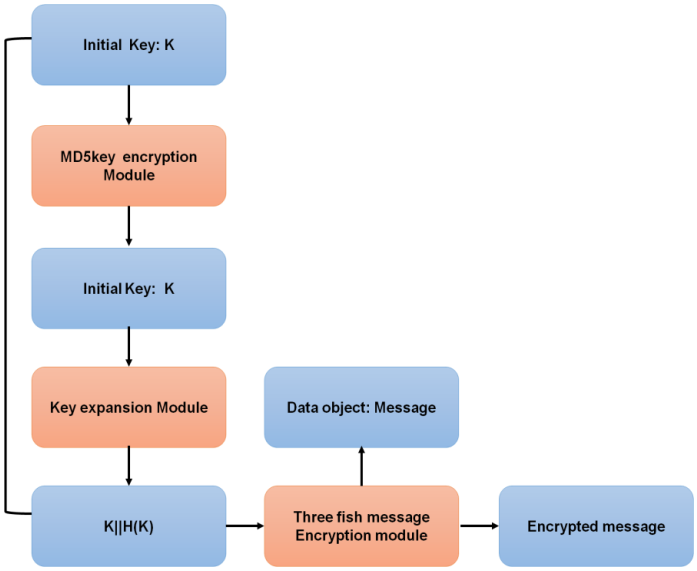

Figure 2. Modules for MD5-three-fish message encryption

When a user selects a system-wide encryption key, the key is transmitted to the MD5 key encryption module. User (private) keys can be of any length, but the output is standardized at 128 bits. Unlike some other common encryption algorithms like AES and DES, MD5 doesn't impose limits on input plaintext sizes. Because of this flexibility, MD5 has gained popularity in secure communications, making it easier for users to choose keys that suit their needs. The key expansion module receives the encrypted key K' generated by the MD5 key encryption module and adds complexity to the process. In this module, the original user key K is augmented with the encrypted key H(K). If the total length of K||H(K) is less than 448 bytes, this combined key is passed to the Threefish message encryption module. However, if the length exceeds 448 bytes, only the first 448 bytes are sent to ensure proper functionality. This added complexity significantly enhances the overall security of the encryption process. Unlike encryption algorithms like Blowfish and Twofish, the Threefish block cipher is designed for easy identification. Threefish is a block ciphering algorithm that can be customized. This algorithm requires three inputs: a key, a tweak, and a block of data. Each block of data is encoded using a unique tweak value, and all block sizes have a tweak value of 128 bits. Threefish encryption supports three key sizes: 256, 512, and 1024 bits, with the key size matching the block size. When dealing with a 1024-bit block size, it requires 72 encryption rounds instead of the usual 72, ensuring a robust level of security. To prevent timing attacks, Threefish avoids employing S-BOX or any other table lookups, relying on a specific round function. The Threefish encryption process follows the steps outlined below.

- Threefish employs $N_s/4 \ + 1$ unique round keys.
- These keys are computed by adding the original keywords $L_0, L_1, \ldots, L_{NX-1}$.
- According to the following, the terms t0 and t1 are added.

$u2 = u0 \oplus u1$

$lNx = d240 \oplus l0 \oplus l1, \ldots . \oplus lNx - 1$

- The keywords Lt, J are defined as

$$Lt,J = \begin{cases} l(t+j)mod\,(Nx+1, j = 0, \ldots, Nx-4 \\ l(t+j)mod(Nx+1) + sumod3, j = Nx-3 \\ l(t+1)mod(Nx+1) + sumod3, j = Nx-2 \\ l(t+1)mod(Nx+1) + t, j = Nx-1 \end{cases}$$

- The mix function accepts a (Y_0, Y_1) and returns the tuple: (Z_0, Z_1)

- The function $Z_0 = Y_0 + Y_1 mod 2^{64}$ is calculated as follows:

$Z1 = (Z1 \lll S(e \ mod \ 8), k) \oplus Z0$

- $S_{e,k}$ is a collection of rotation constants.
- If e mod 4==0 then the round key $L_{e/4}$ is being appended.
- If e mod 4 = 0, the round key $L_{e/4}$ is inserted.
- Then, the mix function is applied.

A symmetric key object has to be taken into account for the Threefish computation in Mathematical. All the data required for encryption, decryption and other operations in a symmetric cryptographic system is represented by Symmetric Key [assoc] in Wolfram language. Symmetric Key objects are compatible with operations like Encrypt and Decrypt. The "Initialization Vector"-> no parameter instructs Encrypt to create a fresh initialization vector each time it is invoked when it is used in Encrypt. The encrypted data is transferred to the user through a trusted energy-efficient path which is identified by SM-TEERP. The user reads the original form of the data-by-data decryption using a hybrid MD5 and Threefish encryption algorithm.

3. EXPERIMENTAL RESULT

In our research, we conducted an analysis of the security enhancements in the 5G-based Internet of Medical Devices (IoMD) with the aim of improving service quality for patients. Additionally, we compared the effectiveness of our proposed approach to that of existing methods. The performance evaluation simulation was carried out using "NetSim (Network Simulator and Emulator)," and the results are presented in Table 2.

Table 2. Hardware and software configuration

Components	Value
Processor	Intel I7 2.3 GHz
Memory	12 GB
Area of sensor deployment	100 x 100m
Operating System	Windows 10
Total number of nodes	50

In this study, we conducted an analysis to validate the performance of the proposed technique in comparison to existing approaches, which include the AES-based key distribution scheme (AES-KDS [32]), Attribute-based Encryption Algorithm (AEA [33]), Bio-cryptographic Key Generation (BCKG [34]), and Improved Identity-Based Encryption Algorithm (IIBE [35]). A comprehensive comparison between the proposed method and these existing alternatives is presented in Table 3, demonstrating that the proposed technique outperforms them in terms of security, speed, and scalability. The primary objective of this research was to assess and compare the performance of the proposed method with established methods, taking into account factors such as accuracy, speed, scalability, and other relevant metrics. Additionally, the study explores potential avenues for enhancement to optimize performance while addressing any potential limitations. Finally, the implications of these findings are discussed, shedding light on prospects for future research and development within this field.

Table.3. Evaluation of the proposed and existing techniques' effectiveness

Methods	Performances analysis parameters			
	Encryption time (ms)	Decryption time (ms)	Security level (%)	Cost consumption (%)
AES-KDS	94	92	55	95
AEA	82	87	69	80
BCKG	77	80	76	76
IIBE	68	75	82	69
HMTE [Proposed]	60	60	98	61

Encryption time, which measures the duration required to transform plaintext into a key stream, is essential for assessing the efficiency of encryption techniques. It signifies the rate at which data is encrypted and is typically measured in milliseconds (ms). The chart titled "Encryption Time" provides an analysis of the encryption time for a set of media files. Notably, our proposed Highly Efficient Method for Text Encryption (HMTE) outperforms current methods, requiring only 60 ms, compared to 94 ms, 82 ms, 77 ms, and 68 ms needed by AES-KDS, AEA, BCKG, and IIBE, respectively, for data encryption. This demonstrates HMTE's superior security level compared to these existing techniques. Decryption, on the other hand, involves the process of reversing encrypted data back to its

original form and typically requires a secret decryption key. Our proposed HMTE stands out by decrypting data in just 60 milliseconds, a significant improvement compared to the decoding times of current techniques. This strengthens the security aspect, where data integrity, authentication, and protection are critical. HMTE's security level is notably higher, at 98%, compared to AES-KDS, AEA, BCKG, and IIBE, further emphasizing its effectiveness in safeguarding patient data in the Internet of Medical Things (IoMT) system. Additionally, HMTE demonstrates cost-effectiveness in securely transmitting patient data within the IoMT environment, setting it apart from established methods. Various parameters demonstrate the superiority of the suggested method over the current system, addressing numerous flaws and positioning itself as a comprehensive solution. Notably, AES-based distribution techniques suffer from poor encryption speeds, and attribute-based encryption requires each user's public key for data protection. Vulnerabilities in electrocardiogram and electroencephalogram measurements indicate potential attacks, hindering real-time implementation. Enhanced identity-based encryption, while secure, relies on subsets of identifying bit strings for generating keys. Computational complexity determines safety levels, where HMTE excels by overcoming limitations inherent in existing methods.

4. CONCLUSION

The proposed solutions, including the use of 5G technology and advanced encryption algorithms, have the potential to significantly improve the security of medical IoT devices. However, there are also potential implementation challenges that need to be addressed. One of the main challenges is the cost of implementing these solutions. Healthcare organizations may need to invest in new hardware and software, as well as hire additional staff to manage and maintain the new systems. Additionally, there may be resistance from healthcare providers who are not familiar with the new technology or who are concerned about the potential risks associated with it. Another challenge is the need for interoperability between different systems and devices. Medical IoT devices are often manufactured by different companies and may use different communication protocols, which can make it difficult to integrate them into a single system. This can create security vulnerabilities and make it harder to manage and monitor the devices. Despite these challenges, the benefits of enhancing security measures in the healthcare industry are clear. By improving the security of medical IoT devices, healthcare organizations can provide better patient services, reduce the risk of data breaches and cyber attacks, and improve overall efficiency and productivity. As such, it is important for healthcare organizations to carefully consider the potential benefits and challenges of implementing these solutions and to work towards developing a comprehensive security strategy that addresses the unique needs of their organization.

FUNDING

None

ACKNOWLEDGEMENTS

The authors want to convey their gratitude to the "Iraqi Ministry of Higher Education and Scientific Research (MOHESR)" for their assistance with the technological aspects of this study.

DECLARATION OF CONFLICT OF INTEREST

None

REFERENCES

[1] Y. Xu, J. Zhang, and Y. Li, “5G-Enabled Artificial Intelligence: A Comprehensive Survey,” IEEE Access, vol. 8, pp. 84568–84588, 2020. DOI: 10.1109/ACCESS.2020.2995102.

[2] Y. Zhang, X. Li, and X. Wang, “Artificial Intelligence for 5G Networks: A Comprehensive Survey,” IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1777–1808, 2020. DOI: 10.1109/COMST.2020.2978983 .

[3] Z. Li, L. Zhang and H Wang “Artificial Intelligence for 5G Network Slicing: A Comprehensive Survey and Future Directions” IEEE Communications Surveys & Tutorials vol 22 no 4 pp 3168–3205 2020 DOI: 10.1109/COMST.2020.

[4] S Wang H Chen and Y Zhang “Artificial Intelligence in 5G Networks: A Comprehensive Survey and Future Directions” IEEE Communications Surveys & Tutorials vol 22 no 2 pp 1090–1119 2020. DOI: 10.1109/COMST.2020.2977861

[5] Li, X., & Wang, Y. (2020). Artificial Intelligence and Internet of Medical Things: A Systematic Review of Recent Developments and Future Directions. IEEE Access, 8, 91702-91725. DOI: 10.1109/ACCESS.2020.2976219

[6] Y Liu., “Artificial Intelligence and Internet of Medical Things: A Survey on Recent Developments in Services Delivery Models for Healthcare Systems,” IEEE Access , vol 8., pp 1–25 , 2020. DOI: 10.1109/ACCESS.2020.2975863

[7] Y. Liu and L. Zhang, “Artificial Intelligence and Internet of Medical Things: A Survey on Recent Developments in Healthcare Systems and Services Delivery Models,” IEEE Access, vol. 8, pp. 51401–51425, 2020. DOI: 10.1109/ACCESS.2020.

[8] H. Zhang and X. Yang, “Artificial Intelligence and Internet of Medical Things: An Overview on Recent Advances in Healthcare Applications,” IEEE Access, vol. 8, pp 25201–25225, 2020. DOI: 10.1109/ACCESS.2020.3027071.

[9] J. Wang and X Li., “Artificial Intelligence and Internet of Medical Things: A Comprehensive Review on Future Directions in Healthcare Systems Delivery Models," IEEE Access , vol . 8 , pp . 12101 -12125 , 2020. DOI: 10.1109/ACCESS.2020.3037862.

[10] J. Kaur and S. Sharma, “Artificial Intelligence and Internet of Medical Things: A Comprehensive Review,” IEEE Access, vol. 8, pp. 116050-116070, 2020.. DOI: 10.1109/ACCESS.2020.3034012.

[11] B. A. Salau, A. Rawal, and D. B. Rawat, “Recent Advances in Artificial Intelligence for Wireless Internet of Things and Cyber–Physical Systems: A Comprehensive Survey,” IEEE Internet of Things Journal, vol. 9, no. 15, pp. 12916–12930, Aug. 2022, doi: 10.1109/jiot.2022.3170449.

[12] S. M. S. Hossain, M. A. Hossain, and M. A. Uddin, “A survey on wireless body area network (WBAN) for healthcare applications,” International Journal of Computer Applications, vol. 175, no. 4, pp. 1–7, 2017. DOI: 10.5120/ijca2017913335.

[13] Y.-H. Kim and J.-Y. Park, “A survey of wireless body area networks for healthcare applications: Architecture and challenges,” IEEE Communications Surveys & Tutorials, vol. 15, no. 3, pp. 1351–1376, 2013. DOI: 10.1109/SURVCOMNETWKINFOCOMMSTECHNOLTUTORIALS2012-2013-1-0019.

[14] Y.-H Kim and J.-Y Park “Wireless Body Area Networks: A Survey on Protocols and Applications” IEEE Communications Magazine vol 49 no 11 pp 40-47 Nov 2011 DOI: 10.1109/MCOMMUNICATIONSMAGAZINE2011-11-0040.

[15] S. U. Amin and M. S. Hossain, “Edge Intelligence and Internet of Things in Healthcare: A Survey,” IEEE Access, vol. 9, pp. 45–59, 2021, doi: 10.1109/access.2020.3045115.

[16] B. A. Salau, A. Rawal, and D. B. Rawat, “Recent Advances in Artificial Intelligence for Wireless Internet of Things and Cyber–Physical Systems: A Comprehensive Survey,” IEEE Internet of Things Journal, vol. 9, no. 15, pp. 12916–12930, Aug. 2022, doi: 10.1109/jiot.2022.3170449.

[17] H. Wu, H. Han, X. Wang, and S. Sun, “Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey,” IEEE Access, vol. 8, pp. 153826–153848, 2020, doi: 10.1109/access.2020.3018170.

[18] M. Awad, F. Sallabi, K. Shuaib, and F. Naeem, “Artificial intelligence-based fault prediction framework for WBAN,” J. King Saud Univ. - Comput. Inf. Sci., vol. 34, no. 9, pp. 7126–7137, 2022, doi: 10.1016/j.jksuci.2021.09.017.

[19] B. L. Sujaya and S. B. BhanuPrashanth, “An efficient hardware-based human body communication transceiver architecture for WBAN applications,” Glob. Transitions Proc., vol. 2, no. 2, pp. 152–156, 2021, doi: 10.1016/j.gltp.2021.08.070.

[20] S. Q. Salih, A. R. A. Alsewari, and Z. M. Yaseen, “Pressure vessel design simulation: Implementing of multi-swarm particle swarm optimization,” 2019, doi: 10.1145/3316615.3316643.

[21] Y. K. Salih, O. H. See, S. Yussof, A. Iqbal, and S. Q. Mohammad Salih, “A proactive fuzzy-guided link labeling algorithm based on MIH framework in heterogeneous wireless networks,” Wirel. Pers. Commun., vol. 75, no. 4, pp. 2495–2511, 2014, doi: 10.1007/s11277-013-1479-z.

[22] H. Tao et al., “A Newly Developed Integrative Bio-Inspired Artificial Intelligence Model for Wind Speed Prediction,” IEEE Access, vol. 8, pp. 83347–83358, 2020, doi: 10.1109/ACCESS.2020.2990439.

[23] S. Q. Salih et al., “Integrative stochastic model standardization with genetic algorithm for rainfall pattern forecasting in tropical and semi-arid environments,” Hydrol. Sci. J., vol. 65, no. 7, pp. 1145–1157, May 2020, doi: 10.1080/02626667.2020.1734813.

[24] S. Q. Salih and A. R. A. Alsewari, “A new algorithm for normal and large-scale optimization problems: Nomadic People Optimizer,” Neural Comput. Appl., vol. 32, no. 14, pp. 10359–10386, 2020, doi: 10.1007/s00521-019-04575-1.

[25] J. P. Lemayian and F. Al-Turjman, “Intelligent IoT Communication in Smart Environments: An Overview,” Transactions on Computational Science and Computational Intelligence, pp. 207–221, 2019, doi: 10.1007/978-3-030-04110-6_10.

[26] V. V. Dixit and M. B. Gulame, “Artificial Intelligence and Machine Learning in Biomedical Applications,” Artificial Intelligence, Internet of Things (IoT) and Smart Materials for Energy Applications, pp. 101–116, Aug. 2022, doi: 10.1201/9781003220176-7.

[27] N. Chouhan, “Artificial Intelligence–Based Energy-Efficient Clustering and Routing in IoT-Assisted Wireless Sensor Network,” Artificial Intelligence for Renewable Energy Systems, pp. 79–91, Feb. 2022, doi: 10.1002/9781119761686.ch3.

[28] A. Nurminen and A. Malhi, “Green Thumb Engineering: Artificial intelligence for managing IoT enabled houseplants,” 2020 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT), Dec. 2020, doi: 10.1109/gcaiot51063.2020.9345850.

[29] L. Ahmad and F. Nabi, “IoT (Internet of Things) Based Agricultural Systems,” Agriculture 5.0: Artificial Intelligence, IoT, and Machine Learning, pp. 69–121, Mar. 2021, doi: 10.1201/9781003125433-4.

[30] H. K. Sharma, A. Kumar, S. Pant, and M. Ram, “Application of Artificial Intelligence in Smart Healthcare,” Artificial Intelligence, Blockchain and IoT for Smart Healthcare, pp. 37–46, Oct. 2022, doi: 10.1201/9781003333050-4.

[31] M. A. Khan, “An IoT Framework for Heart Disease Prediction Based on MDCNN Classifier,” IEEE Access, vol. 8, pp. 34717–34727, 2020.

[32] V. Upadrista, “Artificial Intelligence in the IoT World (Applied IoT),” IoT Standards with Blockchain, pp. 183–199, 2021, doi: 10.1007/978-1-4842-7271-8_10.

[33] M. Kiruthika and P. P. Ponnuswamy, “Fusion of IoT, Blockchain and Artificial Intelligence for Developing Smart Cities,” Blockchain, Internet of Things, and Artificial Intelligence, pp. 155–177, Feb. 2021, doi: 10.1201/9780429352898-9.

[34] P. Srividya and S. Rajendran, “Smart City Using Artificial Intelligence Enabled by IoT,” Artificial Intelligence (AI), pp. 279–292, Apr. 2021, doi: 10.1201/9781003005629-14.

[35] A. M. Ali, M. A. Ngadi, I. I. Al Barazanchi, and P. S. JosephNg, “Intelligent Traffic Model for Unmanned Ground Vehicles Based on DSDV-AODV Protocol,” Sensors (Basel)., vol. 23, no. 14, pp. 1–13, 2023, doi: 10.3390/s23146426.