



## Research Article

# Intermediary Decentralized Computing and Private Blockchain Mechanisms for Privacy Preservation in the Internet of Medical Things

Rasha Halim Razzaq<sup>1</sup>, Mishall Al-Zubaidie<sup>1,\*</sup>, Rajaa Ghali Atiyah<sup>2</sup><sup>1</sup>Department of Computer Sciences, Education College for Pure Sciences, University of Thi-Qar, Nasiriyah 64001, Iraq.<sup>2</sup>Directorate of Education, Karkh II, Ministry of Education, Baghdad 10011, Iraq.**ARTICLE INFO**

## Article history

Received 08 Aug 2024

Accepted 12 Nov 2024

Published 05 Dec 2024

## Keywords

AES

Cyber intrusions

DTM

EASPI

Fog computing

LZW

NBC

Patient data

Private Blockchain

TF-IDF

**ABSTRACT**

Protecting patient data in the Internet of Medical Things (IoMT) is one of the major challenges facing healthcare organizations because of increasing threats to privacy and security. Although there are many existing protocols and solutions, such as Rivest–Shamir–Adleman (RSA) and El-Gamal cryptographies or centralized methods, that aim to protect data, they suffer from weaknesses such as slow performance or inability to handle large volumes of data. The issue of security in medical records has become an urgent need, and the use of centralized methods can expose them to single-point failure. In this paper, we present the efficient approach to securing patient information (EASPI), which depends on blockchain and integrates innovative techniques such as the advanced encryption algorithm (AES), reverse word frequency analysis (TF-IDF), Lempel-Ziv-Welch (LZW), decision tree model (DTM), and naive Bayes classifier (NBC). EASPI seeks to improve the security of medical data by storing it encrypted and securely via blockchain technology, providing a high level of privacy and reliability. The experimental results indicate that the EASPI reduces the encryption execution time to 0.2 ms and the decryption execution time to 0.3 ms while improving the accuracy of medical diagnosis. The potential of the suggested methods for healthcare systems is further demonstrated by the fact that the TF-IDF algorithm attained an execution time of 0.004 ms, while the blockchain's greatest execution time was 0.014 ms. Additionally, using the formal verification Scyther tool, the security of the suggested system is examined both theoretically and practically. The suggested solution is an appropriate option for healthcare institutions since it offers a strong defense against a range of cyber threats, including targeted and espionage assaults.

**1. INTRODUCTION**

With its integration of an extensive network of medical devices, applications, and health information systems, the Internet of Medical Things (IoMT) has become a game-changer in the healthcare industry, enabling remote monitoring and service delivery [1]. IoMT has several benefits, including better patient care through remote diagnostics and real-time data transmission, but it also poses serious security and privacy issues [2]. Vulnerabilities related to insufficient computing power, storage capacity, and poor defense against malevolent assaults against these devices also rise with the dependence on IoMT [3]. Cyber intrusions are a severe risk since they have the ability to compromise private patient information and erode public confidence in healthcare institutions [4]. Maintaining patient safety and confidence now depends on ensuring the integrity, confidentiality, and privacy of medical data, which is more than just a technical requirement [5]. Some real-world recent instances of security threats are devices in the IoMT collection, and there are over 4,000 weaknesses. On the other hand, eighty percent of IoMT device vulnerabilities are significant, meaning that a device may usually be fully taken over. Comparably, approximately half of the vulnerabilities impacting IoMT devices and operational technology are serious [6].

In particular, in the context of IoMT access services situations, intelligent devices such as sensors gather physiological data and incorporate it into the patient's mobile terminal [7]. Medical data are processed and uploaded by hospital servers or base stations to a blockchain for storage and access control. Physicians, practitioners, investigators, and patient families are just a few examples of authenticated users who can lawfully access medical data and utilize it to provide useful medical

\*Corresponding author. Email: [mishall\\_zubaidie@utq.edu.iq](mailto:mishall_zubaidie@utq.edu.iq).

services such as remote diagnosis and treatment decisions [8]. Figure 1 shows a simplified way of how the Internet of Medical Things works.

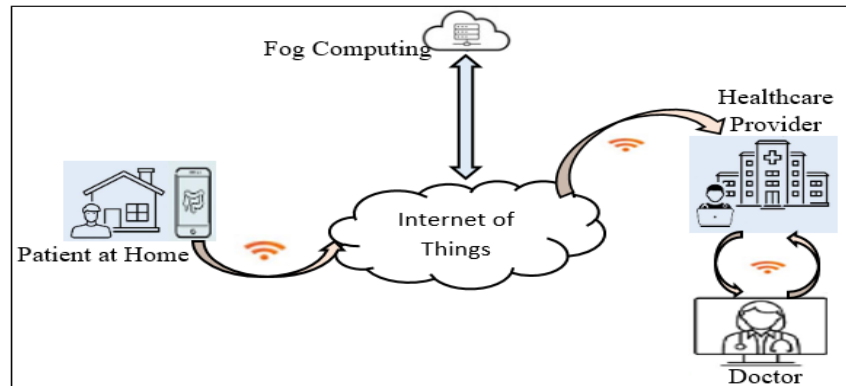


Fig. 1. IoMT working method

While cloud server-assisted access services in IoMT provide users' devices with effective and easy medical assistance, when the security and privacy of a patient's data uploaded to IoMT are unlawfully breached, they may result in medical mishaps or even put the patient's life at risk. Furthermore, a situation may arise where patients need to be able to select who has access to their medical records and implement certain security measures to safeguard the privacy of their data and identities. To avoid unauthorized access to and leakage of medical data held on IoMT, it is imperative that patient-centric data access control and transmission security be improved. Some previous works have relied on centralized networks to transfer patient data, which have become ineffective at present because they may suffer from single-point failure; thus, the use of blockchain has become an important requirement for IoMT networks [9, 10, 11]. Additionally, using encryption techniques such as RSA or El-Gamal may be ineffective in terms of performance when dealing with a large network of patients in IoMT because these algorithms use very long keys and complex operations [12].

The validation of IoMT devices is paramount for establishing secure systems; however, many existing solutions fail to adequately safeguard patient information from cyber threats [13]. Moreover, the transition of data from IoMT devices to cloud databases introduces additional risks, as data can be intercepted or tampered with during transmission, which emphasizes the need for robust mechanisms that can protect medical data at every stage—from collection to storage [14, 15]. In response to these pressing challenges, our research introduces the EASPI, which leverages advanced algorithms and private blockchain technology to create a secure environment for managing patient data [16]. By addressing the multifaceted nature of these threats, the EASPI aims to increase the security and privacy of healthcare data, thereby reinforcing patient trust and ensuring the continued success of IoMT applications in modern healthcare [17, 18, 19].

Therefore, our most important EASPI contributions are as follows:

- Improving the analysis and identity of medical data: EASPI relies on TF-IDF to perform big data analysis and match patient databases. This approach significantly reduces the performance overhead of the EASPI through the measurement of matching, collection, and analysis of medical data, the measurement of similarity via TF-IDF, and the execution time for both blockchain and TF-IDF.
- The search path is defined on the basis of the extracted data: The EASPI uses the DTM to impose questions on the data extracted by the TF-IDF, which leads to useful decisions in classifying patient data. Also, EASPI uniquely compresses medical data with LZW algorithm after data matching, which helps reduce the burden on the system and provides sufficient storage space for patient data storage.
- Increased accuracy of IoMT diagnosis: Using the NBC algorithm and medical data analysis, the EASPI was able to increase the accuracy of predicting critical medical diagnoses, contributing to improving patient care and making correct medical decisions.
- Strengthening blockchain and FCT: The EASPI secures the linked blocks in the blockchain mechanism that are stored in FCT by AES-256 bits. This EASPI opens the door to additional security features and uses in the health sector when advancing blockchain and FCT mechanisms.

The sections of the paper are arranged as follows. A topic introduction is given in Section 1. Section 2 highlights relevant works in our area of study. Section 3 provides a brief background on the techniques of this research. Section 4 presents a detailed EASPI methodology. The performance and security results are presented in Section 5. Section 6 presents the conclusion of our proposed approach.

## 2. RELATED WORK

A selection of current studies on IoMT security and their flaws are briefly discussed in this section.

Ning et al. [20] presented a framework focused on selecting the best ultralight ciphers for IoMT environments, analysing ten lightweight ciphers to identify the most suitable ciphers for authentication. However, their system lacked reliance on secure technologies such as blockchain for sharing patient information, making it vulnerable to cyber intrusions that could modify medical data. Ngabo et al. [2] presented a blockchain-based security mechanism for healthcare data in the fog layer of the IoT architecture, using an elliptic curve digital signature and globally accessible database to provide an irreversible protection system and activity visibility and tamper-resistant patient records in fog computing. They noted the challenges regarding the applicability, performance, and scalability metrics of health approaches, which can be greatly mitigated by the adoption of a blockchain system in a fog environment. Nonetheless, their proposed approach did not provide mechanisms for making medical decisions and securing them from cyber intrusions. To detect cyber threats, Muthanna et al. [4] developed an advanced hybrid SDN-enabled architecture that uses a long short-term memory unit (cuLSTMGRU) to detect threats effectively in Internet of Things settings. To fully analyse the proposed solution, they used an existing dataset and industry-standard IoT evaluation measures. The authors confirmed that the proposed approach improves speed efficiency, detection accuracy, and reliability, among other traditional evaluation criteria. However, the constantly changing behavior of these devices makes the entire system and IoT devices susceptible to cyber breaches, such as cyber espionage, drive-by downloads, and targeted attacks. Raj and Prakash [21] discussed blockchain-based techniques in the field of health care and explored their ability to increase the security and stability of medical systems. They evaluated recent research on the safety of smart health care for the Internet of Things via blockchain. They highlighted effective techniques for providing clinical services and ensuring the protection of patient data. However, their analysis of blockchain security against attacks was limited due to a lack of performance assessments, which are decisive in adopting electronic solutions.

Rehman et al. [22] performed a thorough review of findings linked to blockchain and federated education in Healthcare 5.0. The goal of their research was to create a safe monitoring framework for IoMT healthcare 5.0 that uses blockchain and an intrusion detection system (IDS) to identify any harmful cyber activity in the IoMT network. They stated that this allows clinicians to monitor patients via medical sensors and take appropriate steps on a regular basis by forecasting disorders. Their proposed system shows that this method is significantly better for IoMT monitoring. They stated that their strategy is 93.22% accurate for disease prediction and 96.18% accurate for detection of intrusion estimation. However, breaches of consumer privacy and a range of cyber intrusion hazards may occur because consumers do not embrace them. However, violations of patient privacy and a variety of cyber intrusion threats may occur if a clear mechanism to hide patient data is not adopted. To verify the protection of medical devices and data, Khan et al. [23] suggested securing a blockchain security module for a brain-computer interface (BCI) with interactive media lifecycle regulations that securely connects wearable devices with existing BCI lifecycle protection (BCILC) verification. They implemented smart contracts to store multimedia-related content (timestamp, BCICount, blockTransaction, and blockID) and updates. The proposed module creates a critical issue, as most of the stakeholders involved do not desire to share their personal and content-related information to leverage confidentiality against their competitors. Al-Saeed et al. [1] proposed a reliable and lightweight framework for collective authentication in an IoMT system via blockchain technology and integrated FCT techniques. They relied on Shamir secrets and elliptic curve cryptography to support their security approach. However, authentication systems in health applications require mechanisms to classify medical data in a large database, and their proposal lacks this ability, which negatively affects their authentication approach.

Previous studies have reviewed several challenges related to the security of Internet-connected medical systems (IoMTs), with some studies, such as Ning et al. [20], highlighting the importance of choosing lightweight encryption to secure data; however, these studies ignored emerging threats such as cyber espionage and targeted attacks targeting these sophisticated systems. Although blockchain-based systems, such as those introduced by Ngabo et al. [2] and Rehman et al. [22], offer defense against data manipulation, their usefulness in real-world applications is diminished because they frequently lack real-time clinical decision-making mechanisms. Furthermore, although intrusion detection methods like those introduced by Muthanna et al. [4] are successful, the difficulties in striking a balance between security and performance in intricate IoMT environments—such as the influence on system memory and processing time—have not been taken into account in previous research.

The EASPI, the suggested remedy, offers an integrated framework that blends a number of cutting-edge technologies, including blockchain, AES encryption, the TF-IDF algorithm, LZW, FCT, and the DTM. Through effective data classification, strong encryption, and blockchain-ensured data integrity, this solution offers complete safety for medical data. Furthermore, the system attains excellent accuracy in identifying medical diseases and making real-time medical decisions by integrating machine learning techniques including the naive Bayes classification algorithm and TF-IDF data matching. Additionally, FCT helps with local data processing and reduces performance impact, guaranteeing that the

efficacy and scalability of the system remain unaffected. By taking a thorough approach, the EASPI helps close the gaps found by previous studies and offers a dependable and secure way to increase security and productivity in IoMT applications.

### 3. METHODOLOGY

Applications that must handle data in real time and give users or connected devices rapid access to processing and storage resources can benefit from the performance and usability of FCT. Its primary objective is to provide decentralized computing, storage, and processing resources to IoT networks. FCT does this by distributing tasks and activities across the devices linked to the network. Some jobs are directed to nearby local fog sites rather than sending and processing all the data in a faraway cloud. This technique improves the application's responsiveness and reduces latency. PBC technology, a decentralized technology that facilitates transparent and safe data sharing and storage, is incorporated into our suggested system. PBC works by logging and verifying transactions in a network of linked blocks. These code-protected blocks hold details about different transactions, such as dates and people involved. In the framework of IoMT integration, FCT and PBC intersect. Our system additionally employs the NBC, LZW, AES, TF-IDF, and DTM algorithms to ensure confidentiality, transparency, exact monitoring of healthcare data, information matching, data compression, and medical decision-making. Blockchain technology and FCT offer reliable and secure alternatives to the healthcare industry. PBC technology, in particular, ensures the secrecy, genuineness, and reliability of medical data, promoting transparency and data privacy, whereas FCT facilitates the delivery of resources and processing locally for devices with IoMT and applications. The development of EASPI, made feasible by the combination of these advances, has significantly improved healthcare quality by allowing for effective and continuous monitoring of patients without relying on costly and valuable human capital. Our work steps' process and approach are shown in Figure 2. This figure shows the important and main steps of the proposed system, which integrates multiple algorithms and technologies such as data analysis and encryption.

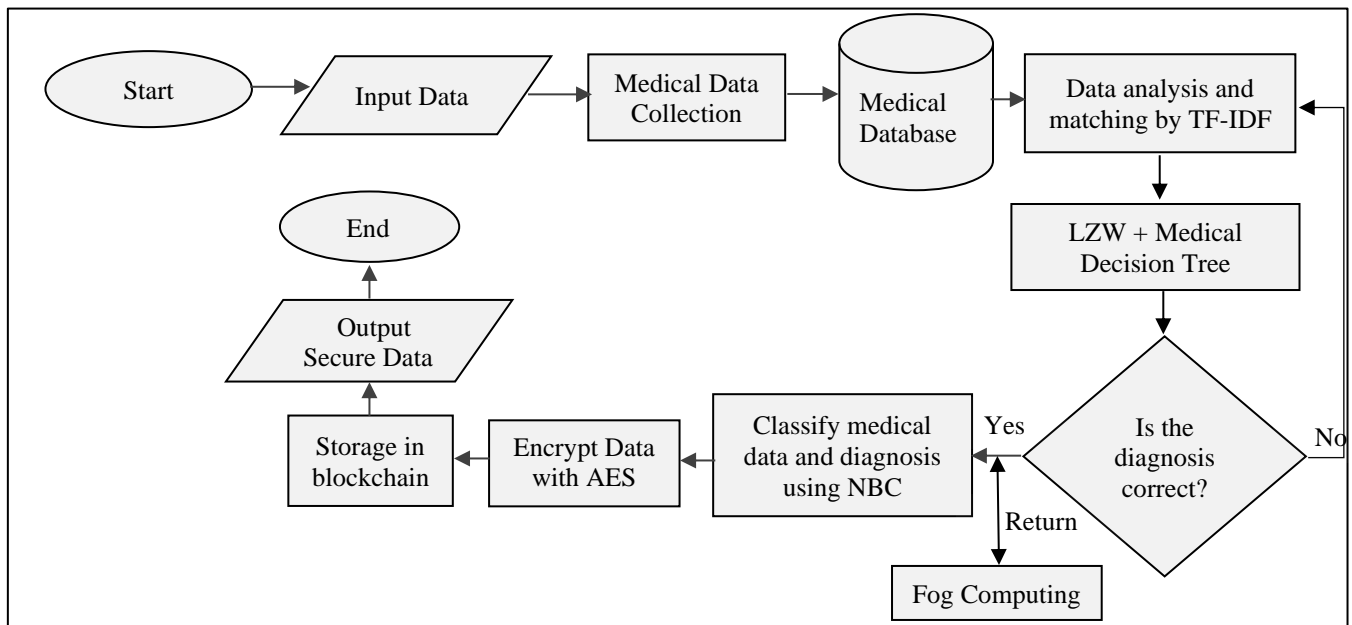


Fig. 2. Methodology and steps of the proposed EASPI system

#### 3.1 EASPI

In this study, we present the EASPI. Healthcare data security has been enhanced through the use of EASPI, which has addressed many forms of specialized research. This method improves the quality and performance of IoMTs by using multiple algorithms (NBC, LZW, DTM, AES, TF-IDF, and PBC) in different combinations. EASPI enhances problem-solving skills, analyses compression and classifies medical data, predicts health diagnoses, and makes timely medical decisions. Finally, this system, which is based on FCT technology, saves and secures medical data after it is encrypted to prevent cyber intrusions (such as targeted attacks, cyber espionage attacks, and data breach attacks).

### 3.2 Data processing and work steps for the EASPI

Initially, the system collects health-related data from medical equipment connected to the IoMT. After data processing, a list of readings from these devices is retrieved and stored in the data processing list (CollectedData). These are the first steps from which the proposed EASPI system begins, as shown in Algorithm 1. The data collection methodology is explained through this algorithm.

---

#### Algorithm 1: CollectMedicalData

---

Input: IoMT\_Devices\_Data

Output: Final\_Data\_Set

Begin

Initialize Final\_Data\_Set  $\leftarrow$  Create\_Data\_Set()

Define procedure Retrieve\_Data()

Initialize Data\_Sources  $\leftarrow$  Discover\_IoMT\_Devices()

For each device in Data\_Sources do

Fetch Raw\_Data  $\leftarrow$  Fetch\_Data\_From\_Device(device)

If Raw\_Data are not empty then

Filter Filtered\_Data  $\leftarrow$  Filter\_Raw\_Data(Raw\_Data)

For each entry in Filtered\_Data do

Enrich Enriched\_Data  $\leftarrow$  Enrich\_Data(entry)

Add Enriched\_Data to Final\_Data\_Set

End for

End if

End for

End procedure

Call Retrieve\_Data()

End

---

After that, the system analyses the data as a second step in its work, as it receives the processed dataset (CollectedData) as input, analyses these data, and matches it by applying the TF-IDF algorithm, which works to match the data and reveal similarities in it, which is shown in Algorithm 2, which represents the steps. Math inside the algorithm.

Where:

$t$  represents the term whose frequency and TF-IDF value we are calculating in the documents, and  $d_i$  represents a specific document in the corpus ( $D$ ). The term frequency (TF) and TF-IDF value of the term  $t$  are calculated in this document, where  $D$  represents the text corpus containing the set of documents ( $d_1, d_2, \dots, d_n$ ). Information is collected from all the documents in this group, and  $N$  represents the total number of documents in text group  $D$ . This number is used to calculate the inverse document frequency (IDF).

---

#### Algorithm2 : TF-IDF

---

Input: Collected Data

Output: Matched and Comprssed\_Data

1. Begin

2. Matched\_Data  $\leftarrow$  []

3. For each document  $d_i$  in Collected Data do

4. For each term  $t$  in  $d_i$  do

5. TF( $t, d_i$ )  $\leftarrow$   $t/d_i$

6. IDF( $t$ )  $\leftarrow$   $\log(N/|\{d \in D : t \in d\}|)$

7. TF\_IDF( $t, d_i$ )  $\leftarrow$  TF( $t, d_i$ )  $\times$  IDF( $t$ )

8. End for

9. End for

10. Compressed\_Data  $\leftarrow$  Compress\_Data (Matched\_Data) // Using LZW algorithm

11. End

---

The TF-IDF algorithm helps us in the field of IoMT. In the context of medical Internet-related things, a large amount of data and information are available, and it is important to extract important and useful information from these data. By applying the TF-IDF technique, we may assess the significance of keywords and words found in accessible health information. We may also utilize the TF-IDF to categorize accessible health information on the basis of its significance and composition.

The third phase of our suggested method involves developing a decision tree model via decision tree methodology. The model in question is built on a list of matching information and employs the outcomes of the TF-IDF technique for pragmatic input. We rely on this model to make medical decisions and diagnoses as well. The fourth stage is as follows. It is the stage of compressing the data with the LZW algorithm before entering it into the data classification stage based on the outputs of the DT model. We trained a classification model on the basis of the naive Bayes algorithm. In conjunction with the work of this model, we created a random secret key so that the outputs of the classification model are inputs to the fifth stage, which is the encryption stage utilizing AES encryption, as shown in Algorithm 3. This algorithm encrypts the data, and medical decisions are output from the classification model. This algorithm uses a Rijndael network to perform the encryption process.

---

**Algorithm 3:** AES process

---

Input: Sorted data X from NBC.

Output: E

1. Begin
  2. Divide the plaintext into 16 bytes (128 bits)
  3. Divide the key into 16, 24, or 32 bytes (128, 192, or 256 bits)
  4. Execute 10, 12, or 14 rounds (depending on the key size):
    - Apply the SubBytes operation
    - Apply the ShiftRows operation
    - Apply the MixColumns operation
    - Add a portion of the key (AddRoundKey)
  5. Return the ciphertext
  6. End
- 

Finally, we store the data on the blockchain. Algorithm 4 also shows the steps of the final stage of the EASPI system.

---

**Algorithm 4 :** Create and distribute block

---

Input: E, Current date and time T

Output: Block

1. Begin
  2. Create a block: Block  $\leftarrow$  {E, T}
  3. Network\_nodes  $\leftarrow$  get\_all\_nodes(Block)
  4. For each node in Network\_nodes do
  5. Send block to the node
  6. If distribution\_success = false then
  7. Ignore
  8. else
  9. Continue
  10. End if
  11. End for
  12. Output: Block
  13. End
- 

We were able to use blockchain technology in our project to save data. A hash function connects a collection of blocks that make up a blockchain, which is a sequential data structure. When blockchain technology is applied in this system, the processed data (CollectedData) are stored in blocks. Each block contains a set of data as well as a distinct hash. The hash is then generated via a hashing algorithm. This function receives input in the form of data and outputs a distinct numeric string representing the data. What links them together is the hash of the block and the hash of the block that preceded it. As a result, an ordered blockchain was created. Since the hash is determined by the content of the previous block, every change made to the stored data will cause all subsequent blocks to become invalid by changing their hashes. In this sense, we have been able to rely on blockchain technology to maintain security and transparency in the healthcare system. System participants can verify the accuracy of the data by reviewing the hashes and comparing them to previous hashes. If any data in a block are changed, the hash of that block and all subsequent blocks will also change, indicating tampering or unauthorized change. Blockchain technology can also be distributed among multiple devices or users of a system, enhancing security and resistance

to manipulation or malicious attacks. Our system provides a reliable and secure way to store medical records, which can be used to track and verify changes in records.

#### 4. OUTCOMES AND ANALYSIS

In this section, we investigate the evaluation of our proposed approach from security and performance aspects and provide comparisons with recent research results ([24], [25-31]).

##### 4.1 Analysis of cyber intrusions on EASPI

1. **Social Engineering attacks:** Psychological manipulation and lure techniques are used to penetrate systems, such as phone or email fraud, to obtain confidential information or perform unauthorized activities. Our system prevents such attacks by encrypting patient data with the AES algorithm.
2. **Data breach attacks:** These attacks aim to steal or disclose sensitive information and personal data of individuals or institutions, whether by hacking systems, stealing mobile devices, or seizing databases. Our system works to store data in blockchain technology to prevent its leakage.
3. **Cyber espionage attacks:** These attacks aim to obtain sensitive and confidential information from other institutions or countries through electronic penetration and spying on systems and networks. The EASPI system goes through stages of matching, diagnosis, classification, encryption, and storage of data, which makes it difficult for these cyber intrusions to penetrate.
4. **Targeted attack:** Specific attacks target specific targets, such as institutions or individuals who possess sensitive or valuable information, and these attacks are usually targeted and carefully planned. Our proposed system prevents these cyber intrusions because it has several algorithms, including the AES encryption algorithm and multiple algorithms, which provide greater security and privacy than similar systems do.
5. **Drive-by download attacks:** These are carried out by implanting malware on devices that visit infected web pages or open suspicious emails, where the malware is automatically downloaded without the user's knowledge. Our system repels such cyber intrusions via the TF-IDF algorithm. It matches the data and ensures that it is not suspicious before proceeding with medical diagnosis and decision-making.
6. **Attacks on device operating systems:** Most IoMT devices are based on Windows operating systems, yet very few of them are protected by anti-malware programs. The lack of data protection makes them vulnerable to remote control attacks and exploitation via ransomware, so our proposed approach uses the Ubuntu operating system as it is very secure to protect its software data.
7. **Credential Stuffing Attacks:** This type of attack is considered to be a Malware type. In these attacks, hackers use stolen login credentials from data breaches to access medical devices and steal entire hospital data. This attack is very dangerous because it exposes patient data to exploitation, which may cost their lives. Therefore, the proposed approach is included in its series of storage works using blockchain technology, as it increases the security of data preservation by encrypting the data in an excellent and strong way.
8. **Cloud-connected IoMT Exploitation Attacks:** With the development of cloud computing in the Internet of Medical Things, attackers have exploited vulnerabilities in remote and multiple cloud environments and unauthorized access, so the proposed approach uses fog computing to increase the security of clouds and preserve medical data because such attacks affect the availability and integrity of medical services.

Table 1 shows a comparison between our proposed approach and other frameworks in terms of their vulnerability to and resistance to these cyberattacks.

TABLE I. A COMPARISON BETWEEN EASPI AND OTHER FRAMEWORKS IN TERMS OF RESPONDING TO CYBER ATTACKS

Attacks	[26]	[27]	[28]	[29]	[30]	[31]	EASPI
Social Engineering attacks	✓			✓			✓
Data Breach attacks	✓	✓			✓		✓
Cyber Espionage attacks					✓		✓
Targeted attack	✓					✓	✓
Drive-by Download attacks			✓				✓
Device operating systems				✓		✓	✓
Credential Stuffing				✓			✓
IoMT Exploitation				✓			✓

Among the important parameters implemented in the proposed system.

- **Total execution time:** This term refers to the total time required to execute a system or program. The total execution time consists of several elements:
  1. Processing Time: The time required to execute commands and algorithms within the program.
  2. Memory Access Time: The time required to access the required data in memory.
  3. Input/Output Time: The time required to read data from the inputs or write it to the outputs.
  4. Processor waiting time: The time the program spends waiting due to the distribution of processor time among several concurrent tasks.

The highest encryption and decryption times were 0.2 ms and 0.3 ms, respectively, for the suggested system. This time, the blockchain technology utilized in the suggested solution incorporates the AES algorithm. The encryption and decryption times of the algorithms in our suggested system are contrasted with those of other systems in Table 2.

The Intel Core i5 processor in the system environment offers dependable and strong performance for running the codes. The machine is perfect for software creation and testing the suggested solutions because it runs Ubuntu, an open source operating system with great stability and flexibility. With its robust tools and libraries for code editing, debugging, and project management, Eclipse serves as an integrated development environment (IDE) for running the codes. Additionally, the computer has 8192 MB of memory, which guarantees enough space to manage massive data volumes and effectively carry out intricate tasks. With this integrated environment, high performance and excellent efficiency can be achieved in implementing the proposed system, ensuring reliable and stable results in encryption and decryption operations.

TABLE II. A COMPARISON OF ENCRYPTION AND DECRYPTION TIME FOR AES ALGORITHM

TF-IDF algorithm	[24]		[33]		Proposed system	
	Scenario1	Scenario2	Scenario1	Scenario2	Scenario1	Scenario2
Similarity score	89.72%	76.24%	16.46%	18.13%	100%	100%

- **Memory usage:** Memory usage is the amount of memory consumed by the program or algorithm during execution. Memory usage is affected by several factors:
  1. The size of the data used in the program.
  2. The size of the variables and temporary data stored in memory.
  1. The size of the program's code.
  2. Dynamic data and dynamic memory allocation are used.
  3. The arithmetic and logical operations that consume memory resources are implemented.

Effectively managing memory usage is one of the major challenges in software and system development, where a balance must be maintained between memory usage and program performance. Therefore, in our proposed methodology, we use the TF-IDF algorithm to reduce memory consumption, as it detects matches and removes duplicate words and texts. The match rate for the two scenarios was 100%. Table 3 shows a comparison between our methodology scenarios and other methodology scenarios that also use the TF-IDF algorithm.

TABLE III. A COMPARISON OF SIMILARITY DETECTION OF TF-IDF ALGORITHM BETWEEN OUR METHODOLOGY AND RECENT RESEARCH

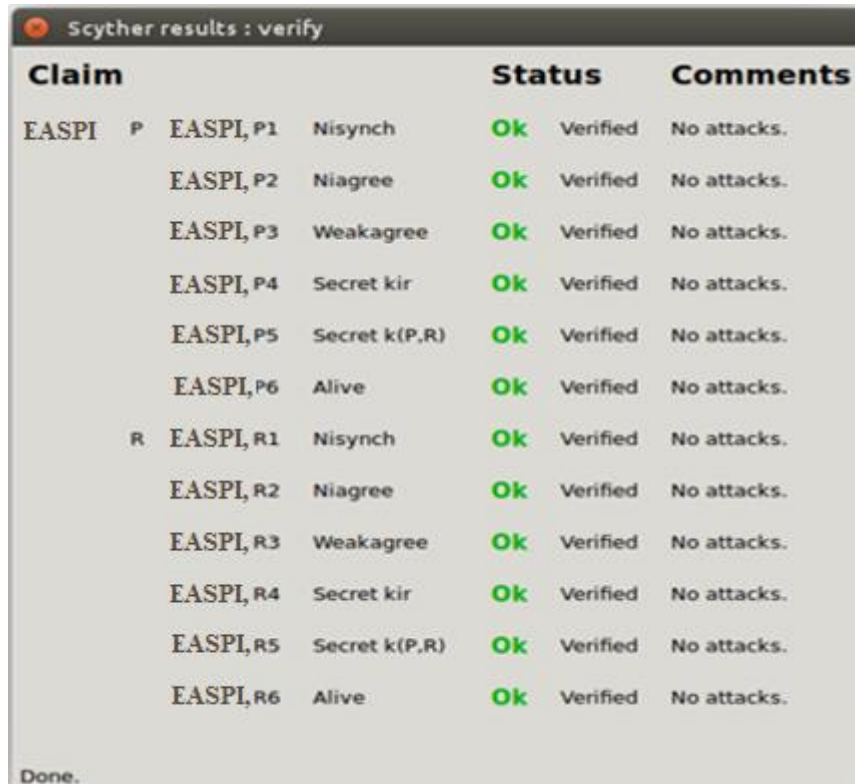
AES in blockchain	Encryption		Decryption	
	min	max	min	max
[15]	0.162 ms	0.228 ms	0.051 ms	0.216 ms
[25]	1.08 ms	1.35ms	2.3 ms	2.52 ms
[32]	1 ms	5 ms	1 ms	5 ms
Proposed system	0.05 ms	0.2 ms	0.05 ms	0.3 ms

Developing cybersecurity solutions through dynamic and ever-evolving approaches to cyber threats contributes to mitigating threats as well as providing a response to future incidents and trying to resolve them [34], Security capabilities can also be enhanced by using AI to detect security threats [35].



## 4.2 Scyther and validated test results

This tool is interesting, as it is an effective tool for validating the cryptosystem and has advanced features that track attacks. Therefore, we use Scyther simulation to verify our proposed security system without the need for approximate methods because it efficiently verifies the majority of methods and systems and shows that all detected attacks are real and do not pose any threat to the system [26]. In our system, Scyther explains some features to verify authentication data between the patient (P) and the party receiving the data (R), and these features include Weakagree, Alive, Niagree, Nisynch, and Secret. In addition, Figure 3 shows the results of testing our approach (EASPI), where we design an attack-resistant system according to the scope of our study, which shows the mutual security parameters between the roles of our system (P, R). Figures 4 and 5 also illustrate the roles of our proposed system.



Claim				Status	Comments	
EASPI	P	EASPI, P1	Nisynch	Ok	Verified	No attacks.
		EASPI, P2	Niagree	Ok	Verified	No attacks.
		EASPI, P3	Weakagree	Ok	Verified	No attacks.
		EASPI, P4	Secret kir	Ok	Verified	No attacks.
		EASPI, P5	Secret k(P,R)	Ok	Verified	No attacks.
		EASPI, P6	Alive	Ok	Verified	No attacks.
R	EASPI, R1	EASPI, R1	Nisynch	Ok	Verified	No attacks.
		EASPI, R2	Niagree	Ok	Verified	No attacks.
		EASPI, R3	Weakagree	Ok	Verified	No attacks.
		EASPI, R4	Secret kir	Ok	Verified	No attacks.
		EASPI, R5	Secret k(P,R)	Ok	Verified	No attacks.
		EASPI, R6	Alive	Ok	Verified	No attacks.

Done.

Fig. 3. The Scyther results



Claim				Status	Comments	Patterns	
EASPI	P	EASPI, P7	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern
		R	EASPI, R7	Reachable	Ok	Verified	Exactly 1 trace pattern.

Done.

Fig. 4. Verification results and trace patterns of Scyther in the proposed system

Figures 3, 4 and 5 illustrate the system's ability to repel the attacks mentioned in addition to how the system's roles in security defense works. Additionally, these figures illustrate the movement of requests between network entities in the Scyther verification tool via several security features.

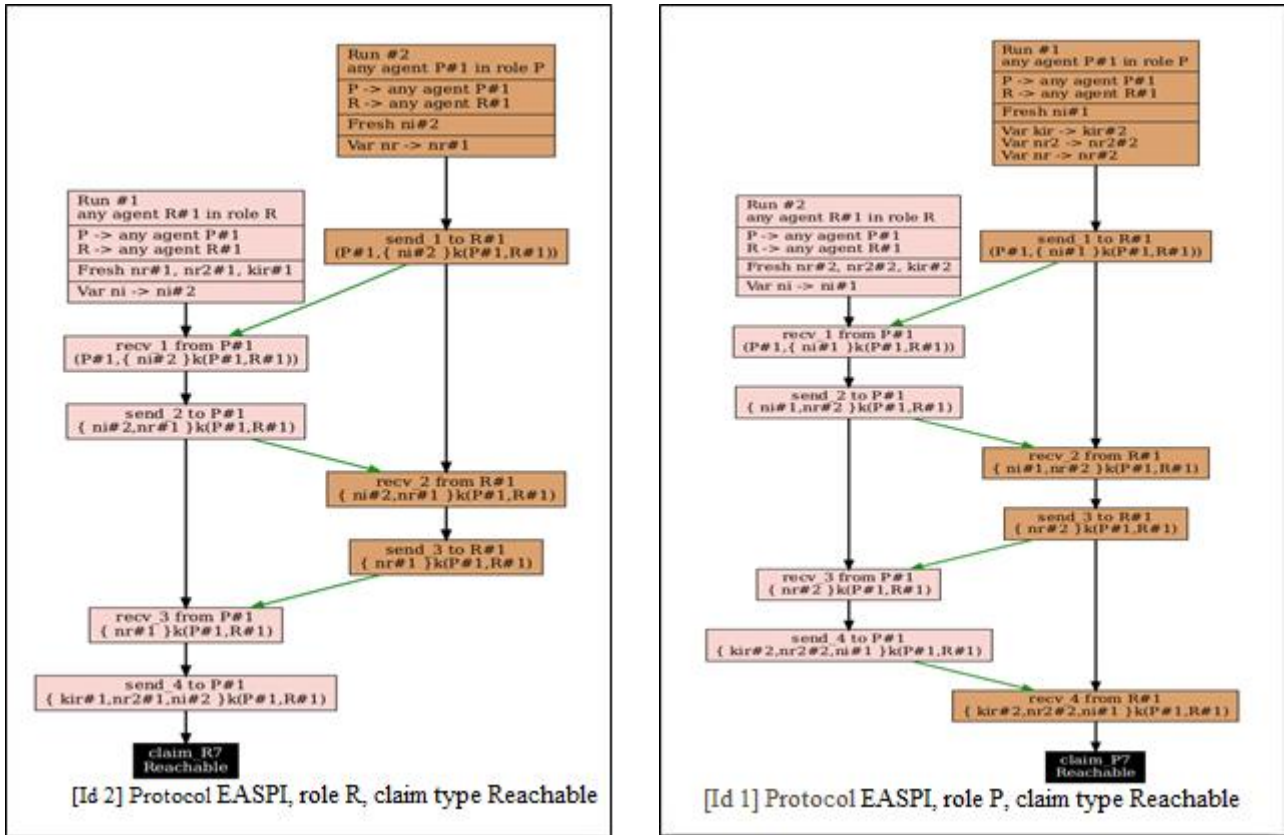


Fig. 5. The distinct roles (P and R) in proposed EASPI system defending against attacks within the Scyther environment

### 4.3 EASPI performance results

To verify the outcomes, our system was applied in an environment based on an Intel(R) Core(TM) i5 CPU, 8192 MB RAM, a 64-bit Ubuntu Pro operating system, and the Java programming language. We run each of our algorithms 100 times to ensure that EASPI works. In Figure 6, the results of the concerted efforts to accurately collect medical data from sensors and medical equipment, analyse them online in the cloud, and match comparable data via the TF-IDF algorithm are shown in Figure 7.

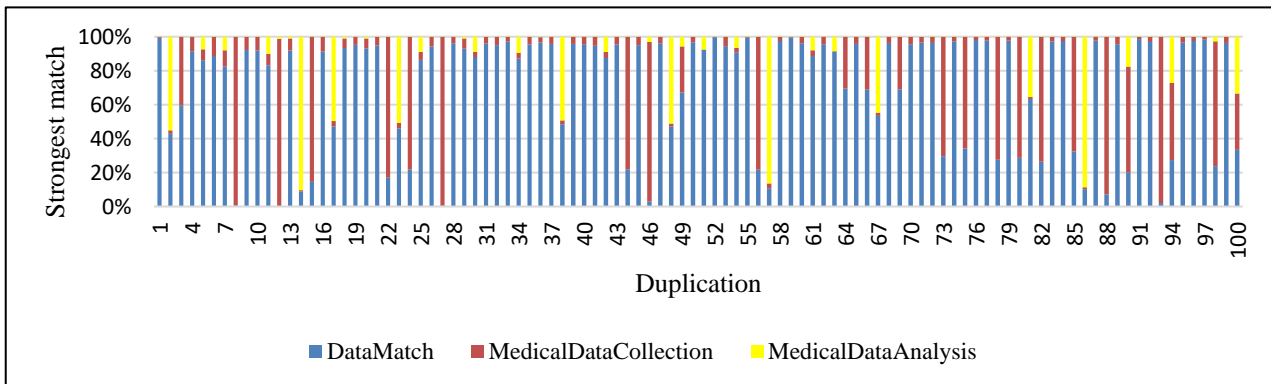


Fig. 6. Outcomes of gathering, analysing, and matching data

Figure 6 shows the results of testing the proposed system in terms of performance (data matching, medical data collection and medical data analysis). This includes a depiction of the effectiveness of the EASPI system.

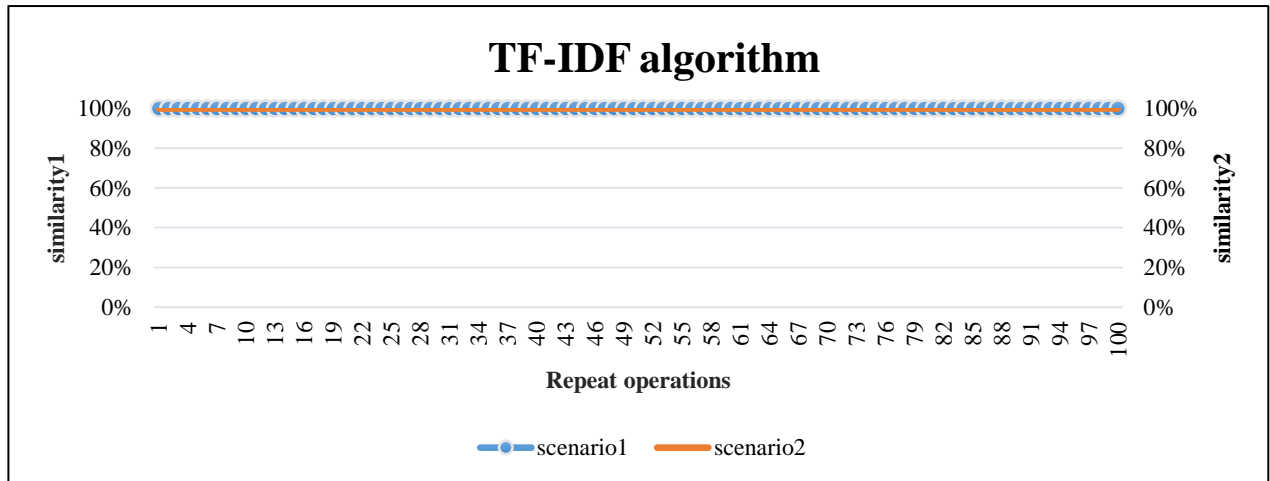


Fig. 7. TF-IDF algorithm execution similarity results

Figure 7 shows the data analysis using TF-IDF technology, as well as the results of improving the accuracy in diagnosing diseases and the ability of the proposed system to improve the accuracy of medical decisions.

The results are interesting. DTM has many advantages, including predictive power and ease of understanding. The ability to apply, analyse, evaluate, and record. In the current study, we employed the decision tree method to reduce security risks in the medical Internet of Things and increase the accuracy of medical diagnosis. The results were impressive, and the application of the NBC algorithm increased the accuracy of medical diagnosis. In addition, medical data are classified on the basis of the information that needs to be disclosed. When diagnosing medical conditions. Since medical Internet of Things applications contain separate homogeneous and heterogeneous components, they are often the target of cybersecurity threats. Therefore, by using AES encryption, Figure 8 depicts the execution time results of encryption and decryption, as the EASPI seeks to prevent hacking and provide fraudulent medical data while preserving patient data and finding security solutions.

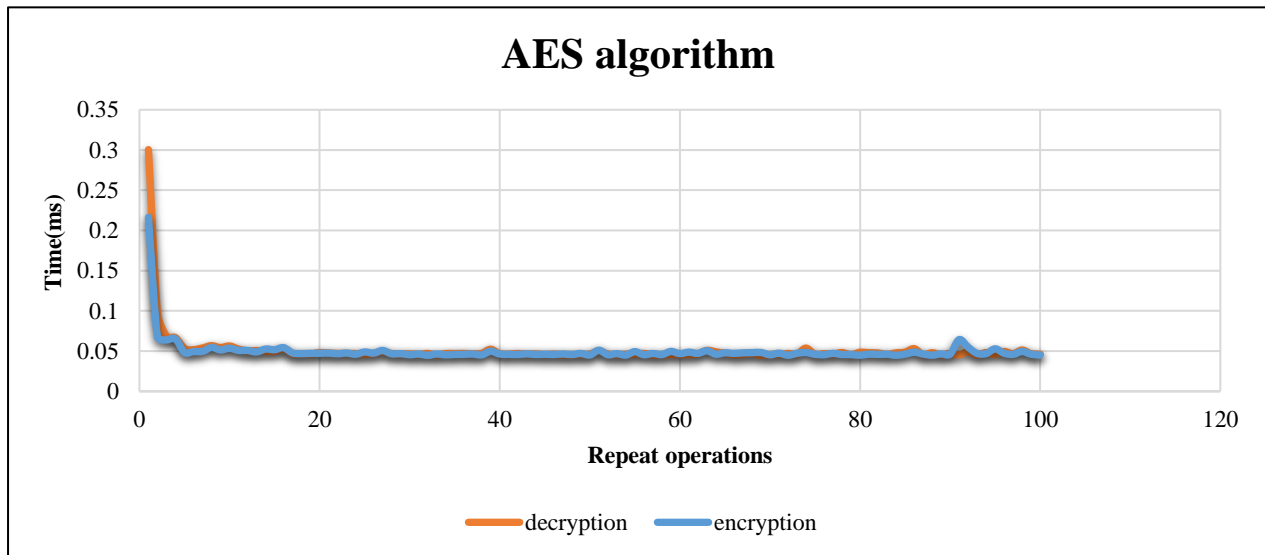


Fig. 8. AES algorithm for data encryption and decryption

Figure 9 shows the consistency of the work of the TF-IDF, AES, and blockchain. The results are shown in Figures 6, 7, 8, and 9. Figure 9 is intended to emphasize the integration between the different mechanisms and how they work together to enhance performance and, subsequently, security. The proposed methods (data collection, data analysis, TF-IDF, DTM, NBC, and AES) can be used to develop medical IoT applications, e.g., healthcare businesses with excellent performance.

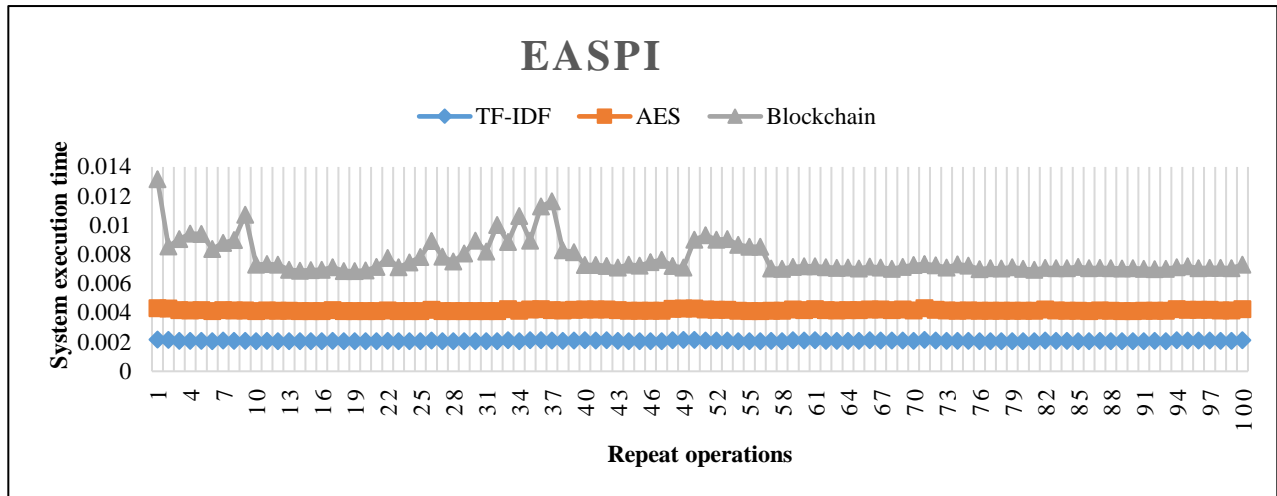


Fig. 9. Consistency of our proposed system techniques (EASPI)

In the context of the EASPI, the type of performance overhead referred to is related primarily to the computational resources required for processing and analysing medical data. This includes:

1. Processing Time: The time taken to execute algorithms such as TF-IDF, DTM, and NBC for data analysis and classification.
2. Memory Usage: The amount of memory consumed during the execution of these algorithms can impact the efficiency of data handling, especially in resource-constrained environments such as IoMT devices.
3. Latency: The delay involved in transferring data across the network is particularly relevant when using fog computing and blockchain technologies.

By optimizing these aspects, the EASPI aims to minimize the overall performance overhead associated with data security measures, ensuring that security does not significantly compromise system efficiency.

## 5. CONCLUSION

Overall, this study enhances the capacity to recognize security risks, reduces the possibility of IoMT system intrusion, and fortifies the confidentiality and security of medical information. PBC and FCT technologies can be used to reliably and securely store and transmit patient data, protecting it from potential security threats. The EASPI design supports IoMT security. The system uses categorization (NBC), decision making (DTM), data similarity matching (TF-IDF), LZW algorithm to reduce the storage space of patient data, and encryption (AES) to safely protect medical data. All things considered, medical data privacy and security are reinforced, the likelihood of IoMT system hacking is reduced, and the ability to identify security threats is enhanced. According to the experimental findings, the EASPI shortens the execution times for encryption and decryption to 0.2 and 0.3 ms, respectively. Some future study areas are indicated by the points below: The goal of implementing the EASPI system in actual health centers or hospitals is to evaluate how well it handles patient data. This entails choosing the application experience's location, collaborating with nearby medical facilities, and gathering information on the system's functionality in actual use cases. Combining machine learning and other artificial intelligence technology increases the EASPI system's categorization and health prediction accuracy. Neurological networks or enhanced learning can be used to improve medical decisions on the basis of patient data. Additionally, improving user interfaces facilitates interaction with the EASPI system by doctors and medical employees. This includes the design of easy-to-use user facades that allow rapid access to important information. By reducing resource consumption and enhancing system performance through methods such as improving the performance of classification, analysis, and decision-making algorithms as well as enhancing cloud computing, the cost and efficiency of using the proposed system can be increased. These points can contribute to enhancing the effectiveness of research and its practical applications, which improves safety and privacy in the health sector.

## Conflicts of interest

The authors declare that they have no conflicts of interest.

## Funding

There was no funding for this research study.

## References

- [1] N. Alsaeed, F. Nadeem, and F. Faisal Albalwy, "A scalable and lightweight group authentication framework for Internet of medical things using integrated blockchain and fog computing," *Future Generation Computer Systems*, 151(2024) 162-181, 2024. <https://doi.org/10.1016/j.future.2023.09.032>.
- [2] D. Ngabo, D. Wang, C. Iwendi, J. H. Anajemba, L. A. Ajao, and C. Biamba, "Blockchain-based security mechanism for the medical data at fog computing architecture of Internet of Things," *electronics*, 10, 2110, 2021. <https://doi.org/10.3390/electronics10172110>.
- [3] D. H. Tahayur, and M. Al-Zubaidie, "Enhancing electronic agriculture data security with a blockchain-based search method and e-signatures," *Mesopotamian Journal of CyberSecurity*, 4(3), 129-149, 2024. <https://doi.org/10.58496/MJCS/2024/012>.
- [4] M. S. A. Muthanna, R. Alkanhel, A. Muthanna, A. Rafiq, and W. A. M. Abdullah, "Towards SDN-enabled, intelligent intrusion detection system for internet of things (IoT)," *IEEE Access*, vol. 10, pp. 22756–22768, 2022. <https://doi.org/10.1109/ACCESS.2022.3153716>.
- [5] R. U. Rasool, H. A. F. Ahmad, W. Rafique, A. Qayyum, and J. Qadir, "Security and privacy of internet of medical things: A contemporary review in the age of surveillance," *botnets, and adversarial ML. Journal of Network and Computer Applications*, 201, 103332, 2022. <https://doi.org/10.1016/j.jnca.2022.103332>.
- [6] FORESCOUT, "The 5 riskiest connected devices in 2023: IT, IoT, OT, IoMT," *Forescout Research - Vedere Labs*, 2023. <https://www.forescout.com/blog/riskiest-connected-devices-it-iot-ot-iomt/>
- [7] R. H. Razzaq, M. Al-Zubaidie, "Formulating an advanced security protocol for Internet of medical Things based on blockchain and fog computing technologies," *Iraqi Journal for Computer Science and Mathematics* 5 (3), 723-734, 2024. <https://doi.org/10.52866/ijcsm.2024.05.03.046>.
- [8] A. Xiang, H. Gao, Y. Tian, L. Wang, and J. Xiong, "Attribute-based key management for patient-centric and trusted data access in blockchain-enabled IoMT," *Computer Networks*, 246, 110425, 2024. <https://doi.org/10.1016/j.comnet.2024.110425>.
- [9] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent advances in the Internet-of-medical-things (IoMT) systems security," *IEEE Internet of Things Journal*, 8(11), 8707-8718, 2020. <https://doi.org/10.1109/IJOT.2020.3045653>.
- [10] S. A. Yousiff, R. A. Muhajjar, and M. Al-Zubaidie, "Designing a blockchain approach to secure firefighting stations based Internet of things," *Informatica*, 47(10), 2023. <https://doi.org/10.31449/inf.v47i10.5395>.
- [11] P. Bagga, A. K. Das, V. Chamola, and M. Guizani, "Blockchain-envisioned access control for internet of things applications: A comprehensive survey and future directions," *Telecommunication Systems*, vol. 81, no. 1, pp. 125–173, 2022. <https://doi.org/10.1007/s11235-022-00938-7>.
- [12] M. Al-Zubaidie, and W. A. Jebbar, "Providing security for flash loan system using cryptocurrency wallets supported by XSalsa20 in a blockchain environment," *Applied Sciences*, 14(14), 6361, 2024. <https://doi.org/10.3390/app14146361>.
- [13] G. S. Shyaa, and M. Al-Zubaidie, "Utilizing trusted lightweight ciphers to support electronic-commerce transaction cryptography," *Applied Sciences*, 13(12), 7085, 2023. <https://doi.org/10.3390/app13127085>.
- [14] J. Jeyavel, T. Parameswaran, J. M. Mannan, and U. Hariharan, "Security vulnerabilities and intelligent solutions for IoMT systems," *Internet of Medical Things: Remote Healthcare Systems and Applications*, 175-194, 2021. [https://doi.org/10.1007/978-3-030-63937-2\\_10](https://doi.org/10.1007/978-3-030-63937-2_10).
- [15] M. Al-Zubaidie, and R. A. Muhajjar, "Integrating Trustworthy Mechanisms to Support Data and Information Security in Health Sensors," *Procedia Computer Science*, 237, 43-52, 2024. <https://doi.org/10.1016/j.procs.2024.05.078>.
- [16] M. Al-Zubaidie, "Implication of lightweight and robust hash function to support key exchange in health sensor networks," *Symmetry*, 15(1), 152, 2023. <https://doi.org/10.3390/sym15010152>.
- [17] S. Shukla, S. Thakur, S. Hussain, J. G. Breslin, and S. M. Jameel, "Identification and authentication in healthcare Internet-of-things using integrated fog computing based blockchain model," *Internet of Things*, 15, 100422, 2021. <https://doi.org/10.1016/j.iot.2021.100422>.
- [18] V. O. Nyangaresi, "Privacy preserving three-factor authentication protocol for secure message forwarding in wireless body area networks," *Ad Hoc Networks*, Volume 142, 1 April 2023, 103117. <https://www.sciencedirect.com/science/article/abs/pii/S1570870523000379>.
- [19] V. O. Nyangaresi, K. A.-A. Mutlaq, Z. A. Abduljabbar, M. A. Hussain, Z. A. Hussien, "Forward and backward key secrecy preservation scheme for medical Internet of things," *Human-Centric Smart Computing*, vol 316, 2022. [https://link.springer.com/chapter/10.1007/978-981-19-5403-0\\_2](https://link.springer.com/chapter/10.1007/978-981-19-5403-0_2).
- [20] L. Ning, Y. Ali, H. Ke, S. Nazir, and Z. Huanli, "A hybrid MCDM approach of selecting lightweight cryptographic cipher based on ISO and NIST lightweight cryptography security requirements for Internet of health Things," *IEEE Access*, vol. 8, pp. 220165–220187, 2020. <https://doi.org/10.1109/ACCESS.2020.3041327>.

- [21] A. Raj, and S. Prakash, "Privacy preservation of the Internet of medical Things using blockchain," *Health Services and Outcomes Research Methodology*, pp. 1–28, 2023. <https://doi.org/10.1007/s10742-023-00306-1>.
- [22] A. Rehman, S. Abbas, M. A. Khan, T. M. Ghazal, K. M. Adnan, and A. Mosavi, "A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique," *Computers in Biology and Medicine*, vol. 150, p. 106019, 2022. <https://doi.org/10.1016/j.combiomed.2022.106019>.
- [23] A. A. Khan, A. A. Laghari, M. A. Shaikh, V. V. Dootio, Estrela, and R. T. Lopes, "A blockchain security module for brain-computer interface (BCI) with multimedia life cycle framework (MLCF)," *Neuroscience Informatics*, vol. 2, no. 1, p. 100030, 2022. <https://doi.org/10.1016/j.neuri.2021.100030>.
- [24] A. Sanjaya, A. B. Setiawan, D. P. Pamungkas, I. N. Farida, and M. A. D. Widyadara, "Measuring meaning similarity using TF/IDF and term synonym ID," In 2023 6th International Conference on Information and Communications Technology (ICOIACT), pp. 206-211, 2023. <https://doi.org/10.1109/ICOIACT59844.2023.10455894>.
- [25] S. W. Lee, and K. B. Sim, "Design and hardware implementation of a simplified DAG-based blockchain and new AES-CBC algorithm for IoT security," *Electronics*, 2021, <https://doi.org/10.3390/electronics10091127>.
- [26] W. Jebbar, and M. Al-Zubaidie, "Transaction security and management of blockchain-based smart contracts in e-banking-employing microsegmentation and yellow saddle Goatfish," *Mesopotamian Journal of CyberSecurity*, 4(2), 1-19, 2024. <https://doi.org/10.58496/MJCS/2024/005>.
- [27] M. Wazid, P. Gope, "BACKM-EHA: A novel blockchain-enabled security solution for IoMT-based e-healthcare applications," *ACM Transactions on Internet Technology*, 23(3), 1-28, 2023. <https://doi.org/10.1145/3511898>.
- [28] M. A. ALGHAMDI, "A fine-grained system driven of attacks over several new representation techniques Using Machine Learning," *IEEE Access*, pp. 96615 – 96625, 2023. <https://doi.org/10.1109/ACCESS.2023.3307018>.
- [29] M. HIJJI, and G. ALAM, "A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: challenges and prospective solutions," *IEEE Access*, pp. 7152 - 7169, 2021. <https://doi.org/10.1109/ACCESS.2020.3048839>
- [30] C. A. Headland, "Mitigating cyber espionage: A network security strategy using notifications," Akron edu, 2024.
- [31] A. AL-Hawamleh, "Cyber resilience framework: Strengthening defenses and enhancing continuity in business security," *International Journal of Computing and Digital Systems*, 15(1), pp. 1315-1331, 2024. <http://dx.doi.org/10.12785/ijcds/150193>.
- [32] G. C. C. F. Pereira, R. C. A. Alves, F. L. da Silva, R. M. Azevedo, B. C. Albertini, and C. B. Margi, "Performance evaluation of cryptographic algorithms over IoT platforms and operating systems," *Security and Communication Networks*, 2017(1), 2046735, 2017, <https://doi.org/10.1155/2017/2046735>.
- [33] s. Albitar, S. Fournier, and B. Espinasse, "An effective TF/IDF-based text-to-text semantic similarity measure for text classification," In *Web Information Systems Engineering–WISE 2014: 15th International Conference, Thessaloniki, Greece, October 12-14, 2014, Proceedings, Part I 15* (pp. 105-114), Springer International Publishing. [https://doi.org/10.1007/978-3-319-11749-2\\_8](https://doi.org/10.1007/978-3-319-11749-2_8).
- [34] M. A. Khalaf, A. Steiti, "Artificial Intelligence Predictions in Cyber Security: Analysis and Early Detection of Cyber Attacks," *Babylonian Journal of Machine Learning*, Vol.2024, pp. 63–68 DOI: <https://doi.org/10.58496>.
- [35] R. H. K. Al-Rubaye, A. K. TÜRK BEN, "Using Artificial Intelligence to Evaluating Detection of Cybersecurity Threats in Ad Hoc Networks," *Babylonian Journal of Networking*, Vol.2024, pp. 45–56, <https://doi.org/10.58496/BJN/2024/006>.