Maintaining Security of Patient Data by Employing Private Blockchain and Fog Computing Technologies based on Internet of Medical Things

Rasha Halim Razzaq and Mishall Al-Zubaidie*
Department of Computer Sciences, Education College for Pure Sciences, University of Thi-Qar, Nasiriyah, 64001, Iraq
E-mail: rashahalim.comp@utq.edu.iq, mishall_zubaidie@utq.edu.iq
*Corresponding author

Keywords: cryptoHSS, IoMT services, jellyfish algorithm, PBC, patient data, security procedures

Received: April 18, 2024

The Internet of Medical Things (IoMT) is a vital component of the Internet of Things (IoT), and its importance lies in the urgent need for it and its provision of many medical services, such as examining and monitoring patients in hospitals and their homes. Given the presence of huge amounts of data based on the IoMT in the cloud system, data storage methods should witness a major revolution, and given the exposure of IoMT systems to electronic attacks, as recent studies have indicated, which makes them unsafe, data must be protected with security systems. In our work, we propose a Cryptography Health Security System (CryptoHSS) to support medical IoT security. Our proposed CryptoHSS relies on Decision Tree (DT), Naive Bayes (NB), Two-Fish, and Jellyfish algorithms within Private Blockchain (PBC) and Fog Computing to build robust security measures. The Two-Fish encryption algorithm is used to provide anonymity of medical information. In our proposed system, NB is used to quickly classify patient data, while DT is used to make accurate medical decisions based on the collected data. The Jellyfish algorithm was used to detect similarities between data and increase the security of data transmission within CryptoHSS. Two-Fish, NB, DT, and Jellyfish algorithms are designed to work in harmony with PBC. CryptoHSS distributes and manages peer-to-peer data in IoMT. The benefit of Fog Computing (FC) is that it speeds up the decision-making process without moving to distant clouds. We analyzed our system in terms of performance and security. Our results indicate that CryptoHSS provides lightweight operations to support complex security measures that qualify it to support health organizations. In terms of security, our system provides reliable security against attacks by keeping medical data encrypted and confidential, with the encryption and decryption rate with the Two-Fish algorithm reaching more than 98%, in addition to providing diagnosis of medical conditions and making appropriate medical decisions.

Povzetek: Prispevek raziskuje varnost pacientovih podatkov z uporabo zasebne verige blokov in tehnologij megličenja, temelječih na Internetu medicinskih stvari (IoMT), ter predlaga sistem CryptoHSS za izboljšanje zaščite podatkov in hitrejše odločanje.

1 Introduction

IoMT has become one of the most powerful, durable, and convenient applications available due to rapid technical advancements in big data collection, cloud computing, deep learning, the IoT, and IoMT services. IoMTs are an integrated ecosystem consisting of interconnected medical sensors, computer systems, and clinical systems [1], and have received great attention in recent years due to significant challenges in the quality and efficiency of medical and healthcare services [2]. Prediction accuracy is greatly impacted by the quality, amount, and significance of data gathered from medical IoT devices. FC provides a good authentication method, it selects a section of data for verification and at the same time solves the requests submitted in real-time, so one of the benefits of Fog Computing is the use of time as it has priority in work [3]. IoMT systems include homogeneous and heterogeneous networks, so it is vulnerable to cyberattacks [4]. Patients and medical institutions have embraced IoMT technology, permitting remote patient monitoring, assessment, and treatment via telehealth services [5, 6]. Smart IoMT nodes are rapidly gaining popularity around the world, especially in pandemic situations, and Figure 1 illustrates the advantages of IoMT.

FC provides a decentralized and scalable network that addresses security, identification, and authentication issues in patient health data. Its operation is to collect process data into blocks for validation and is similar in operation to Blockchain technology. Blockchain is a technology used to store large amounts of data. Completed transactions are recorded and stored in a common block distributed throughout the dynamic systems of the Blockchain network. Blockchain is a stable and reliable platform. With the growing Internet of Healthcare Technologies, which may reach 75.44 billion by 2025, since the vast majority of these devices are unprotected by nature or by powerful process-

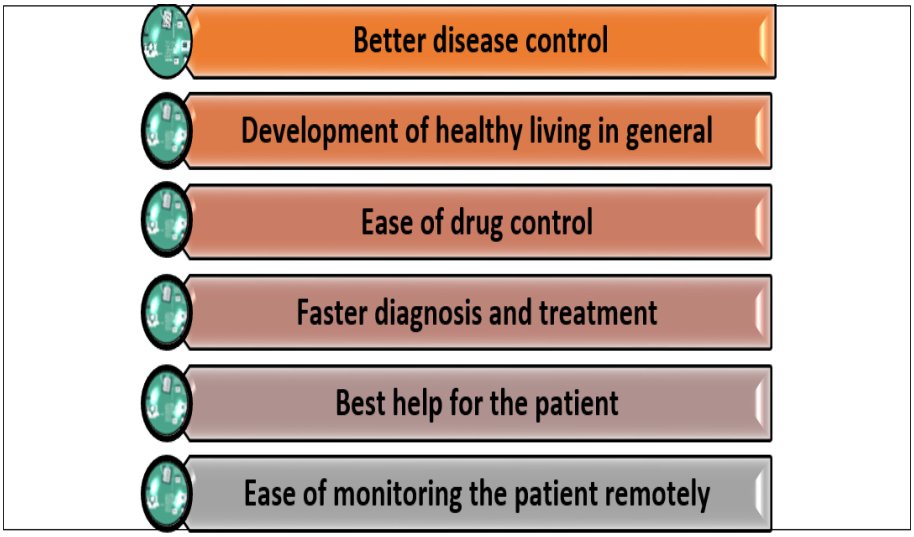

Figure 1: IoMT advantages

ing, this sharp increase in quantity has raised privacy and security issues. Among the attacks that these devices are exposed to are identity theft, exploitation, database, Cloud hacking, advanced phishing, ransomware, spoofing, privacy violations, and many others. To protect these devices from these attacks, it is necessary to identify algorithms or systems that meet the needs of encryption and security [7, 8]. Our research aims to enhance the detection of security threats and reduce the risk of hacking IoMT systems, as well as increase the privacy and security of medical data. In general, the most important contributions of the system are as follows:

- **Proposing CryptoHSS to improve the security and privacy of patient data**: Through the use of PBC and FC procedures, it is possible to provide a safe and reliable manner to save and transmit patient information, protecting them from potential security threats. CryptoHSS uses PBC to distribute and transfer data securely and FC for fast and secure storage.
- **Proposing CryptoHSS to increase the accuracy of medical diagnosis**: Using the NB algorithm and medical data analysis, by increasing the precision of essential medical diagnosis prediction, CryptoHSS succeeded in enhancing patient care and making wise medical judgments.
- **Proposing CryptoHSS to reduce overly similar data**: CryptoHSS uses Jellyfish to reduce redundant and useless replica data and thus reduce the burden on the IoMT network before medical decisions are made by DT.
- **Proposing CryptoHSS to protect against security vulnerabilities and data disclosure**: CryptoHSS adopts reliable Two-Fish encryption to completely anonymize patient data and then store it in the PBC blocks.

The following is the arrangement of the paper's contents. A topic introduction is given in Section 1. Section 2 explores works related to our research topic. Section 3 provides preliminaries for e-health and employed security techniques. Section 4 presents CryptoHSS methodology. Section 5 presents CryptoHSS security and performance analysis. The conclusion is described in Section 6.

2 Related research of e-health and Blockchain security

This section briefly presents a collection of recent research and its vulnerabilities related to the topic of IoMT security. Rahman et al. [3] proposed a framework to protect the privacy and security of IoMT data, where Differential Privacy (DP) and Federated Learning (FL) were proposed, where private IoMT data can be trained at the owner's premises. Recent advances in graphics processing units allow devices to run FL within terminals or smartphones that have IoMT connected to their terminal nodes. They presented a lightweight hybrid FL framework where Blockchain smart contracts manage the trust management scheme, edge training, authentication of participating federated nodes, distribution of trained models locally and globally, reputation of edge nodes, and uploaded datasets or models. The test results show a high and strong potential for IoT-based health management to be more widely adopted in a confidential and secure manner. However, it needs to improve missing metrics and accuracy. Alzahrani et al. [9] proposed a model for integrating healthcare big data security with security verification concepts in medical device design and development. Healthcare data and device security are tested using the combined AHP-TOPSIS method. While verifying the security of data parameters, the algorithm is designed and implemented. As a result, appropriate custom security controls are

required to thwart the attack. However, cyber-physical system (CPS) in the healthcare environment faces issues such as the suitability of medical equipment, software reliability, privacy, security, data retrieval, technology display architecture, and system feedback while storing, processing, extracting, and returning data to CPS, and advanced query processing. Muthanna et al. [10] proposed a software-defined networking (SDN)-enabled hybrid intelligence framework that leveraged the Cuda Long Short-Term Memory Unit (cuLSTMGRU) for effective threat detection in IoT environments. A set of standard evaluation metrics, modern data, and IoT-based metrics were used. In terms of speed efficiency, detection accuracy, and accuracy methods in other standard evaluation metrics, the researchers claimed that their proposed model outperforms existing models. However, the dynamic characteristics of these devices make the entire system and IoT devices vulnerable to identity theft attacks, advanced phishing, Cloud hacking, and ransomware attacks.

Dammak et al. [11] focused on providing security countermeasures as well as a cost-effective solution to HCS (HealthCare Monitoring Systems) by integrating IPFS (Interplanetary File Systems) with a Blockchain-based storage model. Blockchain technology is an emerging solution in the pharmaceutical industry that has been implemented at HCS and allows healthcare providers to control access to shared data and track connected devices, thus protecting patient privacy. Also, the addition of edge and FC has improved the HCS system for real-time interaction and enhanced its reliability. However, the autonomy of this system is extremely limited and does not exceed one month. This system also needs better improvement in terms of security and privacy. Bagga et al. [12] provided a detailed description of IoT, its applications, and its architecture. They also presented many security issues, challenges, potential security attacks in the IoT, and countermeasures. They focused on Blockchain, its workings, and how to develop it into the IoT. A detailed description of existing consensus mechanisms and how Blockchain can be used to overcome vulnerabilities in the IoT is highlighted. They have provided a precise, integrated, and comprehensive description of access control protocols. It will not only allow readers to understand the access mechanism but also clarify issues related to use cases of IoT applications. However, the schemes are very complex due to connections to modern schemes without testing and calculation costs. Furthermore, researchers in [13], [14], and [15] presented systems to protect IoMT based on Blockchain, but their proposed systems were not tested against attacks such as Cloud hacking and Exploitation.

Ali et al. [16] proposed an approach to enhance privacy preservation in IoT-based healthcare applications using homomorphic encryption techniques combined with Blockchain. Symmetric encryption makes it easy to perform calculations on encrypted data without the need for decryption, thus protecting data privacy throughout the computational process. This strategy provides a secure and open environment for managing and sharing sensitive patient medical data, while at the same time maintaining the confidentiality of the patients involved. However, when data is stored and managed, data owners (DO) are separated from direct control of their data, leading to privacy violations and security risks. Also, service providers cannot provide extended security confidence to their customers through external data. Raj and Prakash [17] explored the dimensions of Blockchain and its applicability in healthcare, making the innovative healthcare system more stable and secure. They presented a comparative analysis of well-known recent research on the security of IoT-based smart healthcare systems using Blockchain based on different criteria such as data integrity, architecture, medical information sharing, patient encryption key, distributed electronic health records, hardware implementation, and access control. They have developed a great abundance regarding the effective way to serve and guide clinical medical services to patients to keep up with patient information protection and the most popular way to disseminate stable, accurate, and reliable information to clinical experts. Nonetheless, there are issues related to some attacks on patients' encryption keys, as well as, with the security of patient information. Table 1 provides a comparison between the previous research approaches.

3 Preliminaries for e-health and employed security techniques

This section will provide preliminaries about the techniques used in the proposed CryptoHSS system.

3.1 Background

In this subsection, we will initially explain what the IoMTs are, what are the requirements for their architecture, and the work of each layer, in addition to clarifying the Blockchain and FC technologies, the mechanism of each of them, and how to include some algorithms within them.

3.1.1 IoMT

IoMT is an advanced technology that refers to the network of medical devices and equipment connected to the Internet. This connection allows them to exchange medical information and data. The IoMT is considered part of the IoTs and is a field that deals with a group of sensing, operating, and connecting devices. The IoMT has developed significantly due to rapid technological developments in medicine in addition to the development of medical things.

Table 1: Comparison of algorithms, results and gaps of previous research

Researchers	Year of publication	Methods/algorithms	Main results	Identified gaps
Rahman et al. [3]	2020	Differential Privacy (DP) and Federated Learning (FL) with IoMT	High and strong potential for IoT-based health management with a confidential and secure manner	Missing metrics and low accuracy
Alzahrani et al. [9]	2022	Healthcare data security with AHP-TOPSIS	Appropriate custom security controls and thwart some attacks	CPS in the healthcare environment faces security issues during storing, processing, extracting, and returning data to CPS, and advanced query processing
Muthanna et al. [10]	2022	SDN-enabled hybrid intelligence framework and cuLSTMGRU with IoT	Speed efficiency, detection accuracy, and accuracy methods depending on a set of standard evaluation metrics, modern data, and IoT-based metrics	IoT devices vulnerable to identity theft attacks, advanced phishing, Cloud hacking, and ransomware attacks
Dammak et al. [11]	2022	HCS and IPFS with a Blockchain-based storage model	Addition of edge and FC has improved the HCS system for real-time interaction and enhanced its reliability	Autonomy of this system is extremely limited and does not exceed one month and needs better improvement in terms of security and privacy
Bagga et al. [12]	2022	Blockchain and IoT	Allowing readers to understand the access mechanism and clarify issues related to use cases of IoT applications	Extremely complex due to connections to modern schemes without testing and calculation costs
Ali et al. [16]	2023	IoT-based healthcare applications and homomorphic encryption with Blockchain	Providing a secure and open environment for managing and sharing sensitive patient medical data and maintaining the confidentiality of the patient's data	Privacy violations and security risks during storing and managing operations
Raj and Prakash [17]	2023	Blockchain dimensions with IoT-based smart healthcare systems	Abundance regarding the effective way to serve and guide clinical medical services and disseminate stable, accurate, and reliable information to clinical experts	Issues related to some attacks on patients' encryption keys and the security of patient information

3.1.2 Blockchain

Blockchain is a system of encrypted digital records based on distributed technology and the public network. Blockchain consists of a connected chain of blocks [2], where information and transactions are stored in these blocks securely and sequentially [18]. The operations performed on the Blockchain are consistent and tamper-proof since changes in data require the consent and consensus of network participants. In other words, Blockchain provides a secure and transparent way to record and share information and transactions between participating parties without the need for a central intermediary [19]. There are several types of Blockchain technology, and these are some of the common types:

1. **Public Blockchain**: These are types that are open and available to everyone, as anyone can participate in the process of verifying, recording, and confirming transactions by joining the network. A famous example of this is Bitcoin.

2. **Private Blockchain**: These are types that are limited to a specific group of participants. These types are often used in companies and organizations to implement internal systems and collaborative projects.

3. **Hybrid Blockchain**: It is a type of Blockchain that combines private and public Blockchain elements. Hybrids can be partly limited to a specific group of participants and partly open to all.

4. **Permitted Blockchain**: It is a type of Blockchain that requires approval or permission from a specific entity to join the network and participate in the process of verifying and recording transactions. These types are used in cases of cooperation between institutions and government agencies.

3.1.3 Fog computing

FC is a computing model that aims to extend computing, storage, and networking capabilities to the edges or edges near users and Internet-connected devices. Edges represent users and devices used on the Internet, such as medical devices, sensors, smart devices, and technologies related to the IoT. FC provides storage, computing, and networking capabilities at the edge and aims to provide rapid response and improve the performance of services and applications.

3.2 Naïve Bayes algorithm

NB algorithm is used in data classification and machine learning. It relies on Bayes' classification rule and the concept of probability theory. This algorithm is used in several diverse fields, such as statistical learning, data analysis, and machine learning. In it, a specific model of data is trained using a data set that contains pre-defined features, after which it calculates the compatibility probabilities and prior probabilities between the independent features, and this is between each category and the various other categories of data. These probabilities are used to classify new data. The NB relies primarily on the Nevada hypothesis or simplicity theory, by assuming that all variables are independent in the data and not related to each other. Thus, the process of calculating classification and probability is simplified [20].

3.3 Two-Fish algorithm

This algorithm is used to secure digital data, and it is one of the symmetric encryption algorithms. Designed by scientist Bruce Schneier, it is one of the five final algorithms in the advanced encryption standards competition [21]. It has the advantage that its implementation is available to everyone. This algorithm divides the data into fixed blocks of 128 bits and works on applying the FESTEL network, where the F function is applied to half of the block, after which an XOR is performed between the two halves, and this process is applied to the end of the plain text to be encrypted. It divides the data into fixed 128-bit blocks and applies encryption and decryption operations to these blocks. However, it is possible that modifications or different versions of the Two-Fish will be developed in the future. Modifications may include increasing the security level or improving the performance of the algorithm. In addition, these modifications may include methods for applying encryption processes, changes to the data structure, or functions used. Also, it should be noted that the popular and widely used version is the original version of the Two-Fish [22].

3.4 Jellyfish algorithm

This optimization algorithm simulates the movement of Jellyfish in searching for food, the phenomenon of Jellyfish reproduction, and movement within the swarm. It is a metaheuristic algorithm taken from the movements of Jellyfish in the ocean. The algorithm is a recent innovation and shows encouraging results compared to other biologically inspired optimization algorithms. The Jellyfish optimization algorithm strikes a balance between exploration and exploitation, combining exploratory and exploitative aspects in the process of searching for optimal solutions. The algorithm relies on a strategy that balances these two processes to achieve balanced and effective performance in solving problems [23].

3.5 Decision tree algorithm

DT is one of the supervised learning algorithms used in classification and regression. DT gives a clear graphical representation of all possible solutions. Their decisions are based on specific circumstances, where each branch of the tree represents a possible solution according to the data entered into it. The tree contains the root node, which represents the highest decision, and carries the classification, decision, or diagnosis, which are the internal nodes. Classification of a specific set of data using decision trees must be under specific conditions so that the tree can determine the required diagnoses and decisions. An integrated database must be provided according to the required use so that the decisions taken are correct and accurate [24].

3.6 Ethical Considerations and Data Privacy

There are ethical and data privacy issues in healthcare that must be considered when using fog computing and Blockchain technologies, some of which are:

- Patient Consent: Patients are given explicit consent and informed about how their personal health data will be collected before any data is included in the Blockchain and processed on fog computing nodes. Patients retain the right to access their data and modify it if needed or delete it.
- Regulatory Compliance: The proposed system is keen to comply with the regulations that apply to healthcare systems that use Blockchain and fog computing, such as the General Data Protection Regulation (GDPR) in the European Union and the Health Information Portability and Accountability Act (HIPAA) in the United States.
- Access Controls: Access management is important and crucial as is identity verification. Fine-grained access controls are built into our proposed system so that only authorized healthcare providers and relevant parties can interact with and view patient data stored on the Blockchain and processed using fog computing technology.
- Auditability and transparency: Patients can audit how their personal information is accessed and used within the system, as the decentralized nature of Blockchain provides transparency in data transactions.
- Security assurances: Any security breaches could result in sensitive medical data being subject to unauthorized modification or alteration, so in our proposed system, we ensure that comprehensive security measures including access controls, encryption, and intrusion detection are continuously monitored and upgraded to defend against cyber attacks.

By addressing these ethical considerations, our system can leverage the benefits of fog computing and Blockchain.

4 Proposed system methodology

Our proposed system adopts FC which is a technology that aims to provide computing, storage, and processing resources at a decentralized level in IoMT networks. Also, FC aims to improve the performance and responsiveness of Internet applications that require real-time processing and proximity of computational and storage resources to users or connected devices. It is based on distributing tasks and operations among connected devices in an IoMT network. Instead of sending all the data and processing to the remote cloud, some tasks are directed to local fog points located in the vicinity. This reduces lag and improves application

responsiveness. The technology associated with FC in our proposed system is the technology known as PBC, which is a type of decentralized technology that allows data to be stored and exchanged securely and transparently. PBC technology works by recording and confirming transactions in a series of interconnected blocks. These blocks carry information about various transactions including the parties involved, such as date and time, that are protected by hashing and encryption. PBC and FC overlap in the context of integration (IoMT). In our proposed system, we also used Jellyfish, DT, NB, and Two-Fish algorithms to provide security, transparency, accurate medical data tracking, medical data match finding, and medical decision-making. Overall, FC and PBC collaborate to provide reliable and secure solutions in the healthcare industry. In general, the relationship between FC technology and PBC is that we use FC to provide resources and local processing to IoMT devices and applications, while we use PBC technology to secure and authenticate medical data and achieve security and transparency. This integration led to CryptoHSS which has helped us improve the quality of healthcare, providing continuous and efficient patient monitoring without the need for expensive and limited human resources. Figure 2 shows our methodology and flow of work steps.

4.1 Cryptography health security system

In this research, we propose a Cryptography Health Security System (CryptoHSS). CryptoHSS has addressed healthcare data security which has been improved after studying many types of specialized research in Section 2. This system uses more than one algorithm (Jellyfish, DT, NB, Two-Fish, FC, and PBC) in different ways to increase the quality and performance of IoMTs. CryptoHSS analyzes and classifies medical data, predicts health diagnoses, improves problem-solving, and quickly makes appropriate medical decisions. Finally, powered by FC technology, this system encrypts medical data to protect it from cyberattacks (advanced phishing, ransomware attacks, cloud hacking, identity theft attacks, user interface attacks, and exploit attacks), then stores and secures it.

Below we offer an explanation for our choice of algorithms used in the CryptoHSS System:

1. We used the decision Tree algorithm in our proposed system in order to make sensitive and accurate medical decisions based on the patient's data collected and analyzed with the first two steps of the system, and since it is a strong and spontaneous educational algorithm, then it is able to take effective relationships in medical data, This allows her to have accurate diagnoses and treatment recommendations, as well as make the decision to deal with digital data very suitable.

2. Naïve Bayes algorithm is used in the CryptoHSS system to classify patients' data at high speed, which is a highly efficient algorithm and this makes it very suitable for the actual classification tasks in the Internet of Medical Things Environment, as well as a high capacity and a variety of predictions of lost values, and this is useful for filling the diverse and possible patient data.

3. We use the Two-Fish algorithm in our suggested system to provide privacy and secret medical information. It is an algorithm that can achieve a rate of encryption and decomposition of more than 98%, as well as ensure the effective protection of patients' data from unauthorized access or disclosure.

4. The jellyfish algorithm is used in the CryptoHSS system for the purpose of detecting similarities between data and increasing the safety of data transmission, it is a strong algorithm that works to determine and remove repeated and similar data, which can help reduce the burden on the system and improve its efficiency and enhance its safety and privacy by reducing the potential attack area.

In our research, the linking of the above algorithms in our proposed system is well studied and chosen carefully to address the main challenges of security and privacy in the Internet of Medical Things.

Algorithm 1 Collect the first set of data

```
Input: MedicalIoMTData (a reading list of healthcare-related IoMT devices)
Output: CollectedData (list of processed data)
Begin
Procedure CollectDataFromDevices (MedicalIoMTData):
CollectedData ⟵ []
For reading in MedicalIoMTData
    processed data ⟵ ExtractUsefulInformation (reading)
CollectedData.append (processedData)
End
Return CollectedData
```

4.2 CryptoHSS work steps and data processing

At the beginning of the system, it collects medical data related to healthcare devices connected to the IoMT. It then receives the list of readings of these devices as input, processes this data, and stores it in the data processing list (CollectedData). As shown in Algorithm 1, this is the first step of the proposed CryptoHSS system. This algorithm explains the data collection mechanism.

In the second step of the system, we will analyze the data where we receive the processed data set (CollectedData) as input and analyze this data. The AnalyzedData set is updated using the analyst information extracted from each data point in the processed data set. Algorithm 2 describes the data analysis process. In the third step, we will use the Jellyfish algorithm, so we take the analyzed data set (AnalyzedData) and implement the Qandil algorithm on it. We determine the degree of similarity between the extracted data using the Qandil algorithm and compare it with

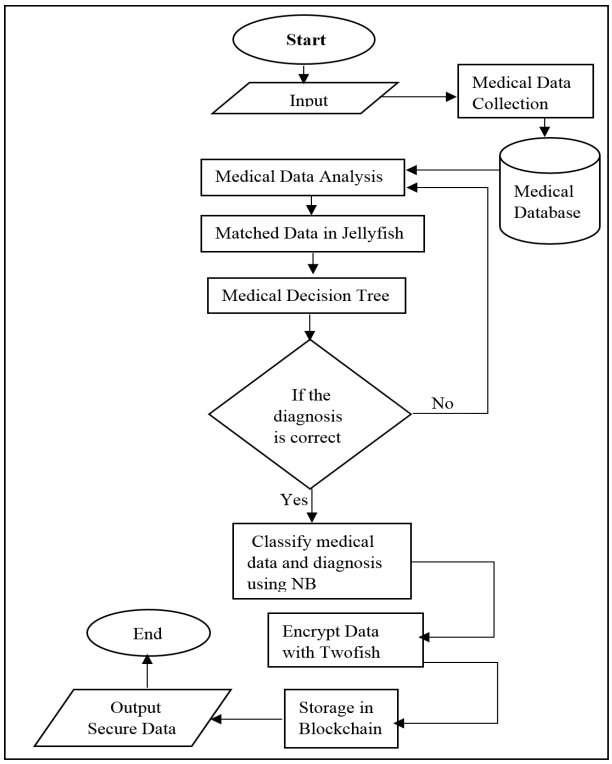

Figure 2: Our system methodology and work steps

Algorithm 2 Data analysis

```
Input: CollectedData
Output: AnalyzedData
Begin
AnalyzedData ⟵ []
For dataPoint in CollectedData
    ExtractedInfo ⟵ AnalyzeDataPoint (dataPoint)
UpdateAnalyzedData (AnalyzedData, EtractedInfo) ⟵ AnalyzedData
End
Return AnalyzedData
```

the specified similarity criterion. If the similarity score exceeds the specified one, the matched pair of data is added to the matched data list (MatchedData). Algorithm 3 describes this step of the system's operation for implementing the Jellyfish algorithm. The fourth step (Algorithm 4) of our work is to build a decision tree model. We take a list of matched data (MatchedData) and build a decision tree model. We will use the results of the Jellyfish to build a decision tree model. Based on the created model, a medical decision is made. If the model is not empty, it is applied to make the decision. If the form is empty, "Unable to decide due to insufficient data" is returned. After we designed the decision-making model, the step of training the NB model came. We take the dataset patients (DB) and the medical decision (MedicalDecision), put them as input, and train a NB model. We set up the probabilities of the categories ($P(C_i)$) and the probabilities of the explanatory variables ($P(X_j|C_i)$) based on the data we provided to the model. We then apply a normalization process to these probabilities. We also generate a random secret key (K) using the NB algorithm, as shown in Algorithm 5. Next comes the

Algorithm 3 Implementing Jellyfish algorithm

```
Input: AnalyzedData, similarity threshold
Output: MatchedData
Begin
MatchedData ⟵ []
For each value i from 1 to the length of AnalyzedData, do:
    For each value j from i+1 to the length of AnalyzedData, do:
        similarity score ⟵ JellyfishSimilarity(AnalyzedData[i], AnalyzedData[j])
    If similarity score similarity threshold, then:
    Matched pair ⟵ (AnalyzedData[i], AnalyzedData[j])
    If the matched pair is not already in MatchedData, then:
    MatchedData.append(matched pair)
End
Return MatchedData
```

Algorithm 4 Building a DT model

```
Input: MatchedData
Output: MedicalDecision
Begin
DecisionTreeModel⟵BuildDecisionTreeModel(JellyfishResults)
MedicalDecision ⟵ []
If DecisionTreeModel is not empty
    MedicalDecision⟵ApplyDecisionTreeModel(DecisionTreeModel)
Else:
    MedicalDecision ⟵ "Unable to decide due to insufficient data"
End
Return MedicalDecision
```

step of using the Two-Fish encryption, we take sorted data to perform Two-Fish procedures. The encryption process includes steps such as Key Expansion, Input Whitening, Feistel Network, and Output Whitening. Then we return the encrypted data (E), as shown in Algorithm 6.

In CryptoHSS, we were able to use Blockchain technology to store data. A Blockchain is a sequential data structure consisting of a set of blocks linked together by a hash function. When we use Blockchain in CryptoHSS, we store the processed data (CollectedData) in blocks. Each block contained a set of data and its hash. The hash is then generated by a hash function, which is a function that takes data as input and generates a unique digital string that represents this data. Blocks are linked together by their hash and the hash of the previous block. Thus, a sequential chain of blocks was created. Since the hash depends on the content of the previous block, any change in the stored data will change the hashes of all subsequent blocks, making them invalid. In this way, we were able to rely on Blockchain technology to provide transparency in the medical treatment system as well as security. Devices participating in CryptoHSS can verify the integrity of the data by examining the hashes and comparing them with previous hashes. If any data within a block is changed, its hash and the hashes of all subsequent blocks will be changed, indicating unauthorized change or tampering.

Also, PBC can be distributed across multiple members or devices in the system, and this enhances resistance and security against malicious attacks and manipulation. By using algorithms and organizing their work, we reach an agreement about the stored data and the changes allowed in the system. Consequently, a secure and reliable storage mechanism for medical data is provided in CryptoHSS, with the ability to verify and track changes to the data. Finally, we store the data in the PBC. Algorithm 7 describes store op-

Algorithm 5 NB training

Input: Dataset Patients_DB, MedicalDecision
Output: $P(Ci)$, $P(Xj|Ci)$, and K
1: Begin
2: Initialize: $P(C_i)$ and $P(X_j|C_i)$ for each C_i and X_j provided with zero
3: For each instance in Patients_DB:
4: Update counts for $P(C_i)$ and $P(X_j|C_i)$ using the instance
5: For each class C_i
6: Normalize $P(C_i)$ and $P(X_j|C_i)$
7: End
8: Generating random secret key)) $\longleftarrow K$
9: End
10: Return $P(C_i)$, $P(X_j|C_i)$

Algorithm 6 Two-Fish cipher

Input: Sorted data X from NB
Output: E
1: Begin
2: Two-Fish_Key_Expansion(K') $\longleftarrow$ Key Expansion: K
3: Input Whitening: $X' \longleftarrow$ Two-Fish_Input_Whitening(X)
4: For each block in X'
5: Two-Fish_Feistel_Network (X', K') $\longleftarrow$ Perform Feistel Network: Y
6: Output Whitening:$E \longleftarrow$Two-Fish_Output_Whitening(Y)
7: End For
8: End
9: Return E

Algorithm 7 Storing data in the Blockchain

Input: E, Current date and time T
Output: Block
1: Begin
2: Create a block: Block $\longleftarrow E, T$
3: network_nodes $\longleftarrow$ get_all_nodes(Block)
4: If distribution_success $\longleftarrow$ false:
5: For each node in network_nodes:
6: Send Block to the node
7: End for
8: Else:
9: Ignore
10: End
11: Return Block

erations in CryptoHSS blocks.

4.3 Autism and the steps for analyzing and classifying the disease in CryptoHSS

We will take a real example of applying the system for Autism: Suppose the input data collected, analyzed, and transformed into the Jellyfish algorithm includes the following sentence: ”Autism is a neurological disorder that affects communication and social behavior.” After applying the Jellyfish to determine similarity and matching, the following words could be identified as most similar: “Autism”, “Neurological disorder”, “Affect”, “Sociability”, and “Behaviour”. The next step in the system is the DT algorithm. We will use the DT to classify the input data, determine its type, and make a medical decision based on the data type. After identifying similar words using the Jellyfish in the previous step, the DT can contain a question such as: “Does the data contain terms related to Autism symptoms?” If the answer is yes, we will classify the data as textual data and a clinical decision will be made regarding it as autism symptom data. But if the answer is no. We will then move to another question, for example, does the entered data contain information about autistic behavior? If the answer is yes, we will classify the data as behavioral data, and then we will work to make an accurate medical decision about autistic behavioral patterns. If the answer is no, then we will also move to another question, and so the medical questions will continue until this stage ends. Then we move to the next stage in our proposed system, which is the NB algorithm, in order to classify the types of autism based on the outputs we obtained from the DT. From these outputs, if the DT algorithm identifies the data as autism data, the NB will classify the types of autism, for example, classifying it as high-spectrum autism or classic autism, and so on. This leads to entering data containing a number of characteristics associated with autism, such as genetic factors, symptoms, family history, and other characteristics of the patient. Our proposed system will analyze these features for each expected classification, such as high-spectrum autism or classic autism. After our system classifies the type of autism using the NB, it will move to the next stage, which is the data encryption stage using the Two-Fish to secure and encrypt the personal and medical information of patients. At this stage in the system, we ensure the protection of the confidential and accurate details of the data and thus we obtain greatly improved transparency and security. The system then moves to PBC to store autism treatment steps and share information. As well as creating tamper-proof and encrypted records. The doctors responsible for the system, as well as the patients concerned and who are allowed authorized access, can update patient records, and the responsible doctors can also access patient data confidentially and securely due to the decentralized nature of PBC. This facilitates periodic and accurate checking of patient data. This allows analyzes to discover new trends, patterns, and relationships between symptoms, diagnoses, and treatments. These insights contribute to improving patient care and making more effective treatment decisions.

4.4 Variables and resources

a- Variables

- **Patient information**: These variables represent gender, name, age, symptoms, previous diagnosis, medical history, etc.
- **Medical device data**: Such as blood pressure readings, heart rate, blood sugar levels, and any other data related to health status.
- **Hospital or clinic data**: Such as staff, departments, medical beds, and other available resources.

b- Resources

- **Sensors**: Such as blood pressure monitors, heart rate sensors, blood sugar monitors, and any other devices used to measure medical data.

– **Communication Network**: Provides telecommunications for data transmission between medical devices and infrastructure.

– **Database**: Used to store and manage medical data related to patients and medical devices.

– **Analysis and processing software**: Used to analyze medical data and extract patterns and important information.

4.5 Receiving data

Receiving medical data in IoMT requires sensors installed on patients or medical equipment to measure health data. There are several ways to receive medical data in the IoMT, and here are some examples:

– Direct wireless connection: Wireless communication technologies such as Wi-Fi or Bluetooth can be used to transfer measured data directly from medical devices to the designated wireless access point. This access point can be a central device that collects data from many medical devices and transmits it to the platform. Data is received from the appropriate source. This may be via the user interface or from an external data source.

– Mobile network protocols: Mobile network protocols such as MQTT (Message Queuing Telemetry Transport) can be used to transfer medical data from medical devices to the cloud or central server. Protocols such as MQTT are used to communicate between devices connected to the Internet and enable secure and efficient data transfer.

– Smart Sensor Gateways: Smart sensor gateways can be used as interfaces between medical devices and IoMT infrastructure. These portals collect data from various medical devices and convert it into a standard protocol that can communicate with the platform.

– Smartphone technology: Dedicated smartphone applications can be used to collect medical data from connected medical devices Bluetooth or NFC (near field communication) technologies are used to receive the measured data.

5 Analysis and results

This section investigates the security analyzes and performance results of the proposed CryptoHSS system.

5.1 Cyberattacks analysis on CryptoHSS

1. **Identity Theft attacks**: An identity theft attack can impact medical IoMT systems in several ways. When it comes to Internet-connected medical devices, such as blood pressure monitors or blood glucose monitors, we must be wary of any attacks aimed at stealing patients' identity data or tampering with medical devices and their data. Or disabling medical devices to protect Internet systems for medical objects from theft attacks. Identity and strong security measures should be taken, such as securing communications between medical devices and back-end systems. Our proposed system (CryptoHSS) maintained the confidentiality and security of medical data by encrypting this data using the Two-Fish algorithm. Consequently, the level of security provided by CryptoHSS is appropriate to resist this attack.

2. **Ransomware attacks**: The WannaCry attack that occurred in 2017 is a strong example of a ransomware attack. Ransomware attacks are a type of malicious cyberattack where attackers encrypt the victim's data and demand a ransom payment in exchange for regaining access to the data. These attacks can be devastating to individuals, companies, and institutions, as they can lead to data loss, financial losses, and operational disruptions. Our proposed system contributes to protecting patient data from these attacks by preserving medical data encrypted in PBC and preventing attacks from obtaining patient data. This gives a distinctive security character to our proposed CryptoHSS system.

3. **Advanced Phishing**: Using advanced techniques to create fraudulent messages or websites that represent trustworthy companies or organizations intending to steal users' personal or financial data. Advanced phishing refers to complex, targeted phishing attacks that aim to trick individuals or organizations into revealing sensitive information, such as login credentials, financial data, or personal information. These attacks often use advanced techniques to make phishing attempts more convincing and difficult to detect. There are some issues and techniques associated with advanced phishing attacks: spear phishing, spoofed websites, email spoofing, social engineering, and malware delivery. Our proposed system contributes dynamically to preventing such attacks by classifying, hashing, and storing data using high-performance algorithms such as NB. Hashing and PBC, allow CryptoHSS to protect entered medical data from theft and fraud.

4. **Cloud Hacking**: Target data and authentications stored in cloud computing services and attempt to gain unauthorized access to sensitive information. Cloud hacking refers to unauthorized access to or exploitation of cloud computing resources, services, or infrastructure. Cloud environments are attractive targets for hackers due to the huge amount of stored data and the potential to obtain valuable information or computing power. Here are some common cloud hacking techniques account hijacking, data breaches, API vulnerabilities, and server-side attacks. To prevent and

mitigate cloud piracy, CryptoHSS implements strong access controls, updating and patching regularly, encrypting data, monitoring and recording activities, and conducting regular security assessments. This is done through the system's use of prediction, classification, encryption, and storage algorithms, and these algorithms work in concert to protect the data inside FC.

5. **User Interface attacks**: These attacks target the front end of a Blockchain application, such as digital wallets or web applications. Attackers aim to exploit vulnerabilities in the user interface to steal private keys or manipulate transactions. User interface (UI) attacks, also known as UI-based attacks or UI spoofing attacks, involve manipulating or spoofing the user interface of an application or website to deceive users. To carry out unintended actions or disclose sensitive information. These attacks exploit weaknesses in user interface design or implementation to perform malicious activities. This type includes some common types of UI attacks: Clickjacking, UI Redressing, and UI Injection. To protect against user interface attacks, the CryptoHSS system contributes to providing security and data protection by encrypting medical data before storing it in the PBC blocks. This corrects the data on a regular basis as well as provides a strong authentication mechanism and secures encryption operations.

6. **Database attacks**: Database attacks refer to malicious activities that endanger the integrity and security of databases, as attackers can attempt to gain unauthorized access to medical databases and manipulate or steal the data contained therein. Attackers may also attempt to delete sensitive medical data or exploit vulnerabilities for personal or financial gain. Some common types of database attacks are such as brute force attacks, and database misconfiguration. To protect against database attacks, CryptoHSS takes some security measures such as using hashing for database records, complex encryption keys, and enforcing strong authentication by PBC and FC.

7. **Exploitation attacks**: Exploiting security vulnerabilities in hardware and software in order to gain unauthorized access or process data. Exploitation attacks refer to exploiting vulnerabilities or vulnerabilities in a system, software, or network to gain unauthorized access or perform malicious activities. These attacks exploit known or unknown vulnerabilities to compromise the target's security. There are several types of exploit attacks, including remote code execution (RCE), SQL injection, cross-site scripting (XSS), denial of service (DoS), distributed denial of service (DDoS), and zero-day attacks. To protect against exploitation attacks, CryptoHSS followed several security countermeasures, such as matching data and discovering similarities to prevent duplication using the Jellyfish, as well as robust security encryption using the Two-Fish encryption algorithm, and implementing strong access controls and authentication mechanisms.

Table 2 shows the comparison of the strength of the system with similar security systems. The security of the Cryptohss System has been evaluated intensively for the purpose of making sure of its effectiveness against various cyber attacks, and we clarify these assessments as follows:

- The premature warning rate: The CryptoHSS system and its ability to detect and monitor is evaluated by monitoring abnormal behaviors. Where legal operations were incorrectly recognized as harmful, and the wrong warning rate was very low, legitimate user activities were not restricted as a result of strict security measures.
- The mission's success rate: Our proposed system is subject to a set of threats, such as exploitation, stealing identity, data infiltration, advanced fraud, and ransom programs. The attacks had a very low success rate, indicating the effectiveness of system safety mechanisms. Stop time: Throughout the attack simulator, CryptoHSS took very little time. This short stopping time guarantees that health information remains available and medical services continue even in the event of a violation of security.
- Encryption power: Two-Fish is analyzed in the CryptoHSS system in terms of encryption power. It turns out that the encryption and jaw rates exceed 98%, which provides a high level of secrecy for the patient's data even if the attacker gets unauthorized access.
- Dragon resistance: Blockchain technology is included in CryptoHSS that the patient's data stored in COMPINQUES is resistant to manipulation. Any attempts to modify data will be discovered immediately and rejected it through the compatibility mechanisms distributed on Blockchain.

In general, the security analysis shows that the CryptoHSS System is very effective in discovering and reducing a wide range of electronic threats that target Internet medical environments.

5.2 Security analysis using Scyther

Scyther is a powerful tool used to analyze and evaluate the security of various protocols using the Python language. The security requirements properties contain some authentication information that this tool verifies, and these properties include Alive, Secret, Weakagree, and other properties. This tool also has some advanced capabilities, as it tracks attack speed and is also at the forefront of verification. It also efficiently verifies most protocols for any number of sessions. It also has an amazing feature to detect all

Table 2: Comparison of CryptoHSS with similar security systems

Attacks on System	CryptoHSS	PBFL-ADS [14]	SECS/GEM [13]	BIoMT [15]
User interface attacks	Strong	Strong	Medium	Medium
Identity theft attacks	Strong	Strong	Strong	Medium
Exploitation attacks	Strong	Medium	Weak	Weak
Database attacks	Strong	Medium	Strong	Weak
Cloud hacking	Strong	Weak	Medium	Medium
Advanced phishing	Strong	Weak	Strong	Weak
Ransomware attacks	Strong	Weak	Strong	Strong

real attacks on models without having to use approximation techniques [25]. Using Scyther, users can detect attacks and perform unfettered verification. This tool is distinguished from similar protocol analysis tools by methods based on open-ended verification or by its ability to combine the strengths of theorem-proof and attack and termination analysis models. In addition, Scyther provides new features not available in other tools, such as attack selection and full profiling. Scyther is used through a GUI or command line interface as a backend for analysis programs that use Python interface functions. Scyther is used to detect attacks on information, meet different security requirements for a variety of protocols, and verify the confidentiality and authenticity of this information, whether in communications between companies and institutions, between patients and doctors, or between hospitals.

5.2.1 CryptoHSS system summary in Scyther

In order to evaluate the effectiveness of the proposed CryptoHSS, we use the Scyther tool, so we prepare CryptoHSS roles for analysis and use the security protocol description language (SPDL) within the Scyther tool. Here we use a set of commands between the patient (SI) and the doctor (DR). Our proposed system has been subjected to simulation between role events to facilitate communication between entities and verify security requirements. Events include tests: Alive, Weak, and Secret. Using the send() and receive() directives we can identify potential attacks or violations resulting from the protocol design as well as evaluate the security and confidentiality of patient information. For the system to be acceptable in health institutions, this system should provide transaction efficiency (directness) and meet confidentiality requirements, ensuring information privacy and availability for all parties involved. Therefore, it is very important to examine the proposed CryptoHSS system in Scyther and verify the security of information transfer between patients and health institutions.

5.2.2 CryptoHSS system evaluation in Scyther

Here we present a test of the CryptoHSS protocol proposed by Scyther. Figure 3 depicts the results of our protocol testing based on the "Alive," "Weakagree," and "Secret" events. The test displays the public key (k), the private key (kir), the sending patient information (SI), and the receiving physician's decisions (DR) as confidential. Our proposed protocol resists attacks in our research topic area.

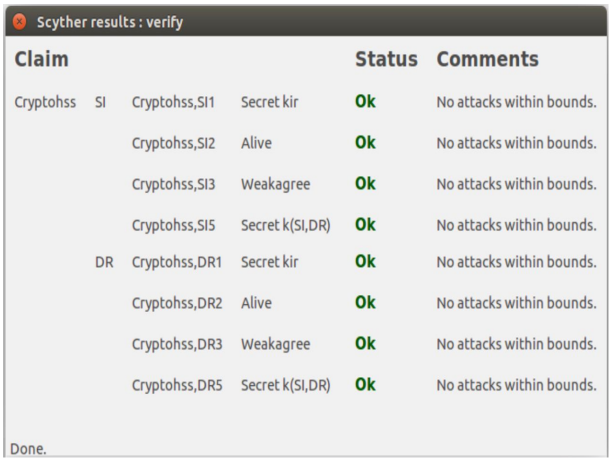

Figure 3: Validation of the proposed security protocol using the Scyther tool

5.3 CryptoHSS performance results

This section describes the performance analysis of our proposed system and Figures 4-8 show the results of CryptoHSS.

5.3.1 System performance analysis

To verify the results, our system was implemented in an environment based on an Intel(R) Core(TM) i5 CPU, 8192MB RAM, 64-bit Ubuntu Pro operating system, and the Java programming language. An internal storage space with a hard disk capacity of 500 GB, a Full HD screen with 15.6 inches, an integrated graphics card from Intel, three USB ports, an HDMI port, and a memory card reader. All our algorithms have been executed 100 times to verify the performance of CryptoHSS.

Figure 4 shows the accuracy of medical data collection from medical devices and sensors. Online object-based medical datasets can be analyzed in the cloud, as shown in Figure 5. Moreover, Figure 6 shows the matching of similar data through the use of the Jellyfish. Furthermore, decision trees provide many benefits such as ease of understanding and predictability. Ability to analyze, apply, examine, and document. In the context of the current research, we used the decision tree algorithm to improve the accuracy of medical diagnosis and reduce security threats in IoMT, and the results were interesting. We also obtained an increase in the accuracy of medical diagnosis through the use of the

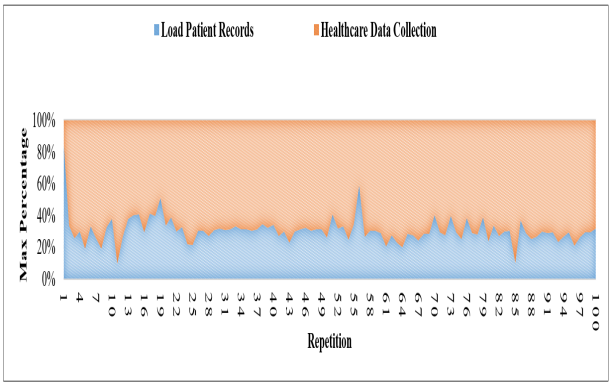

Figure 4: Medical data collection

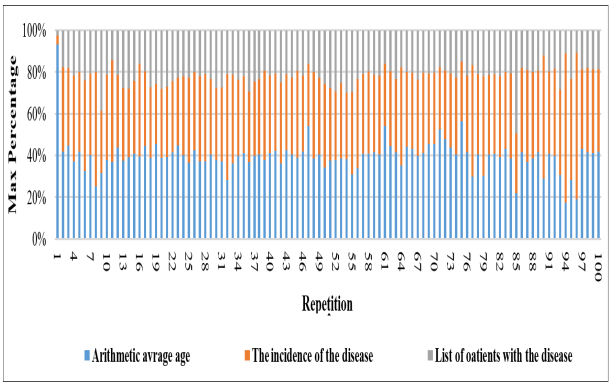

Figure 5: Medical data analysis

NB algorithm. Additionally, medical data is classified according to what data should be included in the medical diagnosis. IoMT applications suffer from distinct homogeneous and heterogeneous parts and are therefore vulnerable to cybersecurity attacks most of the time. Therefore, the CryptoHSS system aims to find security solutions, preserve patient data, and avoid hacking or providing false medical data through the use of Two-Fish encryption.
Figure 7 shows the consistency of the work of DT, NB, and Two-Fish. It also shows the (Frok Solution Time) factor, which refers to the time it takes for the system to solve problems or conflicts that may arise in the system's structure, and also the (Synchronization Time) factor, which refers to the time it takes for the system to be able to synchronize data or operations between its elements. Figure 8 shows the results of memory consumption and transmission rate. From the results of Figures 4-8, the proposed algorithms and their procedures (data collection, data analysis, Jellyfish, DT, NB, Two-Fish, Frok solution time, transfer rate, synchronization time, and memory consumption) provide high and consistent performance for IoMT applications in e-Health organizations.

5.3.2 The most important parameters of the results

In this subsection, we explain the most important parameters used by the CryptoHSS system. We have chosen

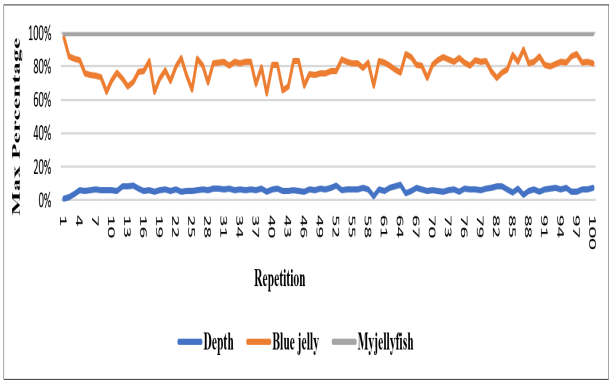

Figure 6: Matching of similar data in the Jellyfish

them from among many parameters because of their importance in the process of analyzing the system's performance, which are as follows:

1. Frok Resolution Time: This parameter indicates the time it takes for the system to resolve problems or conflicts that may arise in the system structure. When a conflict or problem occurs in the system, the system may be unable to continue in the usual way or perform operations correctly. Therefore, solving the problem requires analyzing and examining the root cause of the problem and applying changes or procedures to solve it. The benefits of solving problems quickly include increasing system efficiency, improving its responsiveness, and avoiding negative effects on performance. Frok resolution time for CryptoHSS ranges between 88% and 94% as shown in Figure 7.

2. Synchronization Time: Synchronization means ensuring that the data or processes related to the system are consistent with each other in operation. The synchronization time parameter refers to the time it takes for the system to coordinate the work of data or processes between its components. This parameter includes synchronizing processes and updating data as well as coordination between system elements. The benefits of excellent synchronization include reducing errors, increasing accuracy in operations, improving the overall performance of the system, as well as improving data coordination. The percentage of synchronization time ranged from 96% to more than 99%, as shown in Figure 7. This is the highest percentage reached compared to the synchronization time in previous research [26], which reached 77%.

3. Memory Consumption: Excessive memory consumption can affect the overall system performance, and can also cause the system resources to slow down and perform their work. This parameter indicates the amount of memory that the system uses to store information and data in cache or random access memory (RAM). Memory consumption depends on the size of the data stored in the system and the en-

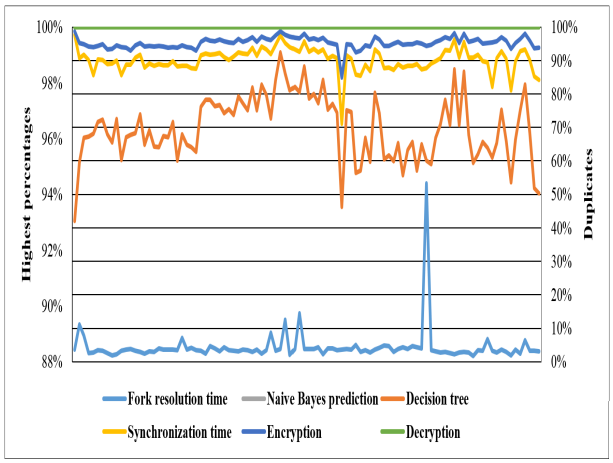

Figure 7: Frok Resolution Time, NB, DT, Synchronization Time and Two-Fish

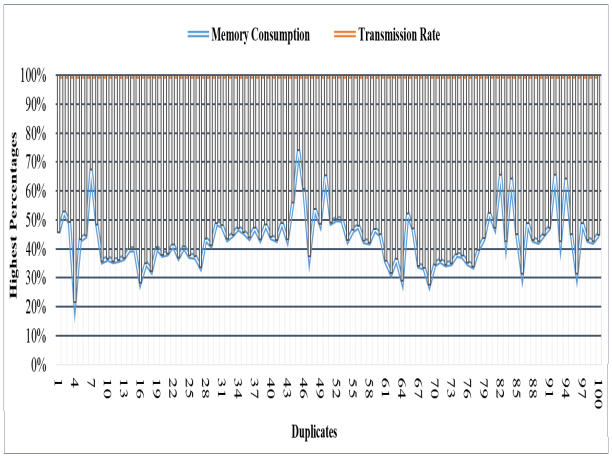

Figure 8: Memory Consumption and Transmission Rate

cryption and decryption processes used. In the proposed CryptoHSS system, we used the Two-Fish algorithm to provide lightweight encryption and decryption with small keys, and the encrypted data was stored in a PBC. Also, using the Jellyfish algorithm in CryptoHSS significantly reduced the storage because we used this algorithm to detect similarities in the aggregated database. This helped improve memory consumption, which reduced resource usage and improved responsiveness and overall system performance.

4. Transmission Rate: Increasing the speed of transferring data between different devices or elements of the system leads to increasing the efficiency of the system, improving its response to carrying out operations, and also increasing the efficiency of the system. As for the transfer rate, it depends on the speed of data transfer between the different medical Internet devices in the system. FC is used to distribute and manage data between devices connected to the Internet. We used the FC technique in CryptoHSS to speed up the decision-making process without requiring access to remote clouds. Hence, a higher transfer rate and lower response time are achieved.

We noted that the actual benefits and exact importance of these parameters depend on the context of the proposed system and its application. We consider security factors, overall system performance, and application requirements before determining the exact benefits that can be achieved using these parameters in the CryptoHSS. The memory consumption results reached approximately 80% and the transfer rate reached 100% as shown in Figure 8.

5.3.3 Discussion of performance results

In this section, we will discuss the results of our proposed solution, CryptoHSS, with the results mentioned in the previous research abstract. We will discuss the differences observed between our results and the current state-of-the-art methods in the field. We will explain why these differences arise and what they mean in the context of IoMT security. First, CryptoHSS provides an integrated solution for protecting patient data using Fog Computing and Private Blockchain technologies, as well as encryption, classification, and similarity detection algorithms. This harmonious integration of these advanced technologies is a novelty in the field of IoMT security, providing multi-level protection of patient data in a cost-effective and performance-effective manner. Compared to previous research, the contributions of CryptoHSS stand out in several aspects:

1. Improving the accuracy of medical diagnosis using NB algorithm and medical data analysis, leading to improved patient care and informed medical decisions compared with [3] and [9].

2. Reduce similar data using the Jellyfish algorithm, which reduces the burden on the IoMT network before making medical decisions using the DT algorithm compared with [11] and [12].

3. Provide reliable protection against security attacks by encrypting patient data using the Two-Fish algorithm and storing it securely in private blockchain blocks compared with [10], [16] and [17].

6 Conclusion

In this part of our research, we will explain the most important conclusions that we obtained through our study, which are reducing the risks of hacking medical systems, as well as enhancing the detection of security threats, and also increasing the privacy and security of medical data through our use of FC and PBC, to provide a safe and reliable way to store/transfer patient data and protect it from potential security threats.

CryptoHSS is designed to support security in IoMT. The system relies on data similarity matching (Jellyfish), decision-making (DT), classification (NB), and encryption (Two-Fish) to provide reliable protection of IoMT data. The system uses medical classification and decision-making algorithms to improve patient care and make accurate medical decisions. It provides lightweight, powerful performance to support complex security measures in healthcare organizations. When we combine the algorithms PBC, FC, Two-Fish, DT, Jellyfish, and NP into the proposed system, CryptoHSS, we obtain protection for medical data from tampering and hacking and also reduce the risks of electronic attacks. The results of our study in Section 5 show that our proposed CryptoHSS system provides high performance, sufficient security, and complete confidentiality to protect medical data in IoMT. It also shows that the performance of the encryption and decryption process was higher than 98%. For future work, we intend to develop CryptoHSS as follows:

– Protection mechanisms and encryption techniques can be improved and developed to better ensure the privacy and security of patient data. Zero inference techniques and emerging technologies such as edge-to-edge encryption may be explored to enhance protection.

– The cost and efficiency of using the CryptoHSS can be improved, as resource consumption can be reduced and system performance can be improved through the use of quantum techniques.

– Support CryptoHSS security by including lightweight signatures and a multi-criteria decision-making procedure to prevent attackers from modifying patient data as well as improve the accuracy of decision-making.

Conflict of interest

The authors declare that they have no conflict of interest.

Data availability

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

References

[1] M. Al-Zubaidie, Z. Zhang, and J. Zhang, "PAX: Using pseudonymization and anonymization to protect patients' identities and data in the healthcare system," *International Journal of Environmental Research and Public Health*, vol. 16, no. 9, p. 1490, 2019. https://doi.org/10.3390/ijerph16091490.

[2] S. A. Yousiff, R. A. Muhajjar, and M. H. Al-Zubaidie, "Designing a Blockchain approach to secure firefighting stations based Internet of Things," *Informatica*, vol. 47, no. 10, pp. 09–26, 2023. https://doi.org/10.31449/inf.v47i10.5395.

[3] M. A. Rahman, M. S. Hossain, M. S. Islam, N. A. Alrajeh, and G. Muhammad, "Secure and provenance enhanced Internet of health Things framework: A Blockchain managed federated learning approach," *IEEE Access*, vol. 8, pp. 205 071–205 087, 2020. https://doi.org/10.1109/ACCESS.2020.3037474.

[4] M. Al-Hawawreh and M. S. Hossain, "A privacy-aware framework for detecting cyber attacks on Internet of medical Things systems using data fusion and quantum deep learning," *Information Fusion*, vol. 99, p. 101889, 2023. https://doi.org/10.1016/j.inffus.2023.101889.

[5] M. Al-Zubaidie, Z. Zhang, and J. Zhang, "REISCH: Incorporating lightweight and reliable algorithms into healthcare applications of WSNs," *Applied Sciences*, vol. 10, no. 6, p. 2007, 2020. https://doi.org/10.3390/app10062007.

[6] M. Al-Zubaidie, "Implication of lightweight and robust hash function to support key exchange in health sensor networks," *Symmetry*, vol. 15, no. 1, p. 152, 2023. https://doi.org/10.3390/sym15010152.

[7] M. Al-Zubaidie, Z. Zhang, and J. Zhang, "Efficient and secure ECDSA algorithm and its applications: A survey," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 11, pp. 7–35, 2019. https://doi.org/10.17762/ijcnis.v11i1.3827.

[8] M. Al-Zubaidie, Z. Zhang, and J. Zhang, "RAMHU: A new robust lightweight scheme for mutual users authentication in healthcare applications," *Security and Communication Networks*, vol. 2019, 2019. https://doi.org/10.1155/2019/3263902.

[9] F. A. Alzahrani, M. Ahmad, and M. T. J. Ansari, "Towards design and development of security assessment framework for Internet of medical Things," *Applied Sciences*, vol. 12, no. 16, p. 8148, 2022. https://doi.org/10.3390/app12168148.

[10] 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. 22 756–22 768, 2022. https://doi.org/10.1109/ACCESS.2022.3153716.

[11] B. Dammak, M. Turki, S. Cheikhrouhou, M. Baklouti, R. Mars, and A. Dhahbi, "LoRaChainCare: An IoT architecture integrating Blockchain and LoRa network for personal health care data monitoring," *Sensors*, vol. 22, no. 4, p. 1497, 2022. https://doi.org/10.3390/s22041497.

[12] 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.

[13] S. U. A. Laghari, S. Manickam, A. K. Al-Ani, M. A. Al-Shareeda, and S. Karuppayah, "ES-SECS/GEM: An efficient security mechanism for SECS/GEM communications," *IEEE Access*, vol. 11, pp. 31 813–31 828, 2023. https://doi.org/10.1109/ACCESS.2023.3262310.

[14] T. M. Ghazal, M. K. Hasan, S. N. H. Abdallah, and K. A. Abubakkar, "Secure IoMT pattern recognition and exploitation for multimedia information processing using private Blockchain and fuzzy logic," *Transactions on Asian and Low-Resource Language Information Processing*, 2022. http://dx.doi.org/10.1145/3523283.

[15] A. Lakhan, M. A. Mohammed, K. H. Abdulkareem, M. khanapi Abd Ghani, H. A. Marhoon, J. Nedoma, R. Martinek, and B. Garcia-Zapirain, "Secure Blockchain assisted Internet of medical Things architecture for data fusion enabled cancer workflow," *Internet of Things*, vol. 24, p. 100928, 2023. https://doi.org/10.1016/j.iot.2023.100928.

[16] A. Ali, B. A. S. Al-Rimy, F. S. Alsubaei, A. A. Almazroi, and A. A. Almazroi, "Healthlock: Blockchain-based privacy preservation using homomorphic encryption in Internet of Things healthcare applications," *Sensors*, vol. 23, no. 15, p. 6762, 2023. https://doi.org/10.3390/s23156762.

[17] 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.

[18] A. Djeddai and R. Khemaissia, "Privykg: Security and privacy preservation of knowledge graphs using Blockchain technology," *Informatica*, vol. 47, no. 5, 2023. https://doi.org/10.31449/inf.v47i5.4698.

[19] S. Ahamad, P. Gupta, P. B. Acharjee, K. P. Kiran, Z. Khan, and M. F. Hasan, "The role of block chain technology and Internet of Things (IoT) to protect financial transactions in crypto currency market," *Materials Today: Proceedings*, vol. 56, pp. 2070–2074, 2022. https://doi.org/10.1016/j.matpr.2021.11.405.

[20] B. Gbadamosi, R. O. Ogundokun, E. A. Adeniyi, S. Misra, and N. F. Stephens, "Medical data analysis for IoT-based datasets in the cloud using Naïve Bayes classifier for prediction of heart disease," in *New frontiers in cloud computing and Internet of Things*. Springer, 2022, pp. 365–386, ISBN: 978-3-031-05527-0.

[21] G. S. Shyaa and M. Al-Zubaidie, "Utilizing trusted lightweight ciphers to support electronic-commerce transaction cryptography," *Applied Sciences*, vol. 13, no. 12, p. 7085, 2023. https://doi.org/10.3390/app13127085.

[22] W. Haryono, "Comparison encryption of how to work caesar cipher, hill cipher, Blowfish and Twofish," *Data Science: Journal of Computing and Applied Informatics*, vol. 4, no. 2, pp. 100–110, 2020. https://doi.org/10.32734/jocai.v4.i2-4004.

[23] A. Khare, G. M. Kakandikar, and O. K. Kulkarni, "An insight review on Jellyfish optimization algorithm and its application in engineering," *Journal homepage: http://iieta. org/journals/rces*, vol. 9, no. 1, pp. 31–40, 2022. https://doi.org/10.18280/rces.090103.

[24] F. E. Botchey, Z. Qin, and K. Hughes-Lartey, "Mobile money fraud prediction–a cross-case analysis on the efficiency of support vector machines, gradient boosted decision trees, and Naïve Bayes algorithms," *Information*, vol. 11, no. 8, p. 383, 2020. https://doi.org/10.3390/info11080383.

[25] M. Al-Zubaidie and G. S. Shyaa, "Applying detection leakage on hybrid cryptography to secure transaction information in e-commerce apps," *Future Internet*, vol. 15, no. 8, p. 262, 2023. https://doi.org/10.3390/fi15080262.

[26] R. Matzutt, B. Kalde, J. Pennekamp, A. Drichel, M. Henze, and K. Wehrle, "Coinprune: Shrinking bitcoin's Blockchain retrospectively," *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 3064–3078, 2021. https://doi.org/10.1109/TNSM.2021.3073270.