2023, 20(6 Suppl.): 2651-2671
https://dx.doi.org/10.21123/bsj.2023.9203
P-ISSN: 2078-8665 - E-ISSN: 2411-7986

Baghdad Science Journal

A Novel System for Confidential Medical Data Storage Using Chaskey Encryption and Blockchain Technology

Aymen Mudheher Badr[1, 2], **Lamia Chaari Fourati** [1], **Samiha Ayed** [3]*

[1]Digital Research Center of Sfax (CRNS) Laboratory of Signals, Systems, Artificial Intelligence and Networks (SM@RTS), Sfax University, Sfax, Tunisia.
[2]Department of Political Sciences, College of Law and Political Sciences, University of Diyala, Diyala, Iraq.
[3]Institute Charles Delaunay-ERA, University of Technology of Troyes, France.
*Corresponding Author.

Received 08/06/2023, Revised 08/09/2023, Accepted 10/09/2023, Published 05/12/2023

Abstract

Secure storage of confidential medical information is critical to healthcare organizations seeking to protect patient's privacy and comply with regulatory requirements. This paper presents a new scheme for secure storage of medical data using Chaskey cryptography and blockchain technology. The system uses Chaskey encryption to ensure integrity and confidentiality of medical data, blockchain technology to provide a scalable and decentralized storage solution. The system also uses Bflow segmentation and vertical segmentation technologies to enhance scalability and manage the stored data. In addition, the system uses smart contracts to enforce access control policies and other security measures. The description of the system detailing and provide an analysis of its security and performance characteristics. The resulting images were tested against a number of important metrics such as Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), bit error rate (BER), Signal-to-Noise Ratio (SNR), Normalization Correlation (NC) and Structural Similarity Index (SSIM). Our results showing that the system provides a highly secure and scalable solution for storing confidential medical data, with potential applications in a wide range of healthcare settings.

Keywords: Blockchain, BFlow, Chaskey, Healthcare, IoT, Security.

Introduction

In today's digital age, storing and sharing sensitive data, such as medical records, has become a major concern. The need for secure and efficient methods of storing and sharing such data has led to the development of various encryption and storage technologies. One such technology is blockchain, which provides a decentralized and tamper-proof way of storing and sharing data.

Blockchain-enabled health Data Protection in the IoT is an emerging field focusing on leveraging blockchain technology to secure and manage health data generated by IoT devices. The Internet of Things (IoT) is a network of interconnected devices that collect, analyze, and exchange data. In the healthcare industry, IoT devices such as wearables, sensors, and medical equipment can generate vast amounts of health data, which can be used for personalized medicine, population health management, and other healthcare initiatives. However, the collection, storage, and sharing of health data on the IoT pose significant challenges related to privacy, security, and data integrity[1]. These problems can be solved by using blockchain technology to create a decentralized, unchangeable, and open platform for managing health data.

In a blockchain-enabled health data protection system, health data is stored in a distributed ledger, which is maintained by a network of users or nodes. Each node has a copy of the ledger, and any updates or changes to the ledger are recorded securely and transparently. The use of advanced cryptographic techniques ensures the privacy and security of health data, making it virtually impossible for unauthorized parties to access or modify the data[2]. Blockchain-enabled health data protection on IoT can revolutionize the healthcare industry by enabling efficient and secure health data sharing, promoting data-driven decision-making, and improving patient outcomes. Scalability, interoperability, and regulatory compliance are a few of the issues that still need to be resolved. Even yet, the IoT health data protection offered by blockchain is a promising area for study and development in the field of healthcare[3].

Data protection is critical in healthcare because it involves sensitive personal information that can have severe consequences if it falls into the wrong hands. Health data includes information about an individual's medical history, symptoms, diagnoses, treatments, and medications, which can reveal sensitive information about the person's physical and mental health, lifestyle, and genetic makeup. The importance of data protection in healthcare can be seen in the potential consequences of a data breach[4]. If health data is accessed or stolen by unauthorized parties, it can lead to identity theft, medical identity theft, financial loss, reputational damage, and even physical harm. For example, if a person's medical record is accessed by a hacker, they could use the information to obtain prescription drugs or medical equipment that is not suitable for their condition, which could lead to serious health complications.

Furthermore, healthcare organizations have legal and ethical responsibilities to protect health data. Healthcare organizations are obligated by laws like HIPAA in the United States and the GDPR in the European Union to take precautions to protect patient's personal health information and guarantee its privacy, security, and accessibility at all times[5].

The Internet of Things (IoT) has introduced new challenges for managing health data[6]. Some of the challenges associated with managing health data on the IoT include:

1- Security: IoT devices are often vulnerable to security threats such as hacking and malware attacks, which can compromise the confidentiality, integrity, and availability of health data.
2- Data fragmentation: It might be challenging to manage and evaluate health data obtained from various IoT devices because of the possibility of data fragmentation and distribution among devices and servers.
3- Interoperability: IoT devices may use different data formats and protocols, making it difficult to integrate and share data across different devices and systems.
4- Scalability: The amount of health data generated by IoT devices is growing rapidly, which can make it challenging to store, manage, and analyze the data in a timely and efficient manner.

Overall, managing health data on the IoT requires addressing these challenges to ensure that health data is securely and efficiently managed to support healthcare delivery and improve patient outcomes. Using blockchain technology to safeguard medical records has several advantages:

1- Security: Blockchain technology provides a high level of security for health data by using advanced cryptographic algorithms and distributed consensus mechanisms to ensure that data cannot be tampered with or deleted without authorization. This makes it more difficult for hackers to breach the system and compromise health data.
2- Privacy: Blockchain technology enables privacy-preserving data sharing by using advanced encryption algorithms and smart contracts to ensure that only authorized parties can access and use health data. This helps to protect the privacy and confidentiality of patient's health information.
3- Transparency: With the immutability and transparency provided by blockchain technology, the provenance and validity of health records may be more easily tracked and verified. This has the potential to boost healthcare systems' credibility and transparency.
4- Efficiency: By facilitating instantaneous and error-free health data exchange and processing, blockchain technology has the potential to boost the effectiveness of healthcare systems. This

can help to reduce costs and improve patient outcomes.

5- Interoperability: Blockchain technology can facilitate interoperability between different healthcare systems and providers by providing a secure and standardized platform for data exchange. This can help to improve the coordination and continuity of care for patients.

Using blockchain technology for health data protection can provide a range of benefits, including improved security, privacy, transparency, efficiency, and interoperability. These benefits can help to improve the quality of care and outcomes for patients while also reducing costs and increasing trust in healthcare systems.

The main contribution of this paper is the proposal of a new system for the secure storage of medical data using Chaskey cryptography and blockchain technology. The system provides a highly secure and scalable solution for healthcare organizations seeking to protect patient privacy and comply with regulatory requirements. It is hoped that this work will inspire further research in this area and lead to the development of even more innovative and effective solutions for secure medical data storage.

The remainder of this article is organized as follows: In the second section, provide an overview of relevant work in the field of secure medical data storage, highlighting the limitations and challenges of current solutions. In the third section, introduce the technical background of the proposed system, including Chaskey cryptography, blockchain technology, Bflow hashing, column hashing, and smart contracts. In the fourth section, describe the architecture and design of the proposed system in detail, including its components, data flow, and security features. In the fifth section, evaluate previous studies. The sixth section presented the implementation and evaluation of the system, including performance criteria, security analysis, and comparison with existing solutions and discuss the strengths and weaknesses of the proposed system, as well as its limitations and future work. Finally, Section seven, conclude the article with a summary of the contributions, implications, and future directions of the proposed system.

Background

The secure storage of medical data has become increasingly important in recent years due to the growing use of electronic health records (EHRs) and the increasing number of cyber-attacks on healthcare organizations. EHRs allow healthcare providers to access patient information quickly and easily, but they also present new risks to patient privacy and data security. Sensitive patient data may be stolen in the event of a cyberattack on a healthcare provider, which can be used for identity theft, insurance fraud, or other criminal activities.

To address these risks, healthcare organizations must implement robust security measures to protect patient data. Traditional approaches to data security, such as firewalls and encryption, are no longer sufficient in the face of sophisticated cyber-attacks. New technologies, such as blockchain and smart contracts, offer the potential for more secure and decentralized storage of medical data. By leveraging these technologies, healthcare organizations can enhance the security and privacy of patient data while also improving the efficiency of data management and sharing.

Blockchain Overview

Blockchain technology is a decentralized, distributed ledger that allows for secure and transparent transactions without the need for a central authority. Each block in a blockchain contains a record of transactions that are added to the chain in chronological order. The transactions are verified by a network of nodes through a consensus algorithm, ensuring that the information is accurate and tamper-proof, Fig. 1.

The immutability of blockchain data is a crucial feature. A newly added block cannot be modified or removed from the chain without the agreement of all nodes in the system. Because of this, storing and transmitting data using it is risk-free and dependable.

Another important characteristic is transparency. All blockchain transactions are accessible to all participants, making it impossible for any one person or organization to influence the system. Blockchain technology is also highly resistant to hacking and cyber-attacks due to its decentralized nature. Because there is no central point of failure, it is much harder for hackers to gain control of the network.

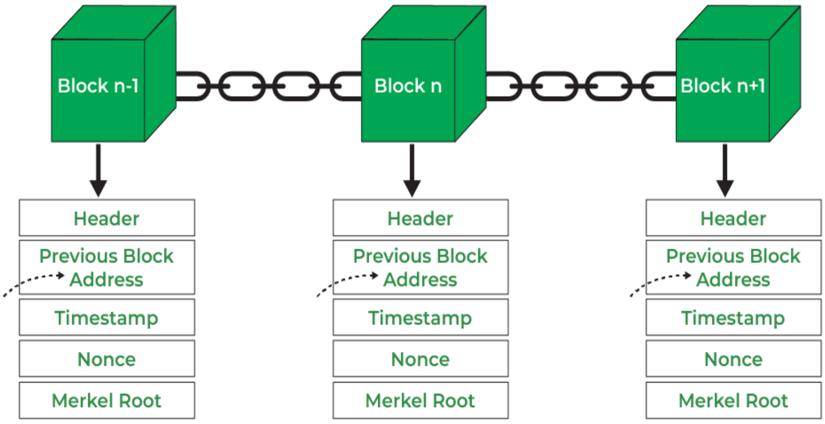


Figure 1. Blockchain Structure

Blockchain technology is being used in healthcare to ensure the security and privacy of sensitive patient data, improve the efficiency of data sharing between healthcare providers and patients, and enhance the accuracy and transparency of clinical trials. One example of this is MedRec, a blockchain-based electronic medical record (EMR) system developed by researchers at MIT. MedRec uses blockchain technology to create a decentralized, secure, and transparent system for storing and sharing patient medical records[7,8]. Patients can permit healthcare providers to access their records, and all transactions are recorded on the blockchain, ensuring that the data is accurate and tamper-proof.

Another example is the use of blockchain technology in clinical trials. The pharmaceutical industry is using blockchain to create a decentralized ledger of clinical trial data that can be accessed by researchers, regulators, and patients. This allows for greater transparency and accountability in the clinical trial process, as well as improved data sharing and analysis. Several features of blockchain technology make it suitable for health data protection[9]:

1- Decentralization: Blockchain technology is decentralized, which implies that no one entity controls the data. Because there is no single point of failure, hackers have a more difficult time gaining access to the data.
2- Immutable records: Once data is recorded on the blockchain, it cannot be altered or deleted. This ensures that the data is secure and tamper-proof.
3- Encryption: Data on the blockchain is encrypted, which means that it is protected from unauthorized access. This makes it more difficult for hackers to steal or modify the data.
4- Transparency: Blockchain technology allows for transparent and auditable records, which means that everyone can see the history of the data. This provides an additional layer of security and accountability.
5- Permissioned access: Blockchain technology allows for permission access to the data, which means that only authorized parties can view or modify the data. This ensures that the data is only accessed by those who have a legitimate reason to do so.

All these features make blockchain technology an ideal solution for protecting health data, as it provides a high level of security, transparency, and accountability.

The Lightweight Encryption algorithms

Lightweight encryption algorithms are designed to provide secure encryption and decryption of data with minimal computational resources. They are ideal for use in low-power devices such as sensors, wearables, and IoT devices that have limited processing capabilities and memory. One example of a lightweight encryption algorithm is the SIMON cipher. SIMON is a block cipher that uses a key size of 64, 96, or 128 bits and a block size of 64 bits. It is designed to be fast and efficient while providing strong encryption[10]. SIMON uses a round-based structure with a key schedule that is based on the Feistel network.

Another lightweight encryption algorithm is SPECK. SPECK is a block cipher that uses a key size of 64, 96, or 128 bits and a block size of 64 bits. It is designed to be secure and efficient on both software and hardware platforms. SPECK uses a round-based structure with a key schedule that is based on the ARX operation[11].

Both SIMON and SPECK are lightweight encryption algorithms that are suitable for use in low-power devices that require secure communication. They provide strong encryption while minimizing the computational resources required for encryption and decryption.

The Data Fragmentation

Data fragmentation is the process of dividing data into smaller, more manageable pieces. This can be done for a variety of reasons, such as improving performance, increasing security, or facilitating data management. In my article, data fragmentation may refer to the practice of breaking up large data sets into smaller, more manageable chunks. This can be useful in situations where the entire data set cannot be processed at once, or where different parts of the data set need to be accessed by different users or applications. Data fragmentation can be implemented in several ways, such as through the use of partitions, subsets, or shards. Each of these approaches involves dividing the data into smaller pieces, but they may differ in terms of how the data is organized and accessed[12].

There are several types of data fragmentation, including:

1- *Horizontal fragmentation:* This involves dividing a table into multiple smaller tables based on rows. Each smaller table contains a subset of the original table's rows, typically based on specific criteria, such as a range of values or a particular attribute[13].
2- *Vertical fragmentation:* This involves dividing a table into multiple smaller tables based on columns. Each smaller table contains a subset of the original table's columns, typically based on a specific criterion, such as a group of related attributes.
3- *Directory fragmentation:* This involves creating a master directory that contains information about the location and contents of smaller data fragments. Each fragment is stored in a separate file or database, and the directory provides a way to locate and access the data.
4- *Replication fragmentation:* This involves creating multiple copies of the same data, which are stored on different servers or devices. This can improve performance and availability but also requires additional storage and management.

Related works

The research paper[14], that proposes a blockchain-based data-sharing scheme for the industrial Internet of Things (IIoT). The paper addresses the issue of secure and efficient data sharing in the IIoT, which is critical for the success of Industry 4.0. The proposed scheme uses a hybrid consensus model that combines proof of work (PoW) and proof of authority (PoA) to ensure both security and efficiency. The PoW mechanism is used to prevent double-spending and ensure the integrity of the blockchain, while the PoA mechanism is used to ensure fast transaction processing and minimize delays. The scheme also uses data sharding to improve the scalability of the system, allowing the data to be divided into smaller pieces and stored on different nodes within the network. This helps to ensure that the system can handle large amounts of data without compromising its security or efficiency.

Another related work to Blockchain-Enabled Health Data Protection. The article[15] proposes a blockchain-based system for privacy-preserving healthcare data management in the cloud. The system uses blockchain technology to ensure the integrity and security of healthcare data while also providing privacy-preserving features such as data encryption and access control. The proposed system uses a combination of hash-based and elliptic curve-based encryption techniques to protect the privacy of healthcare data. It also uses smart contracts to enforce access control policies and ensure that only authorized parties can access the data. The system is designed to be scalable and efficient, with low computational overhead and high throughput. It can be deployed in a cloud environment, which allows for easy access and sharing of healthcare data among different healthcare providers.

In article[16], It proposes a blockchain-enabled access control system to maintain privacy in IoMT. The system includes an intelligent contract-based access control mechanism and a privacy-preserving data sharing mechanism, which allows data owners to define access policies for their data and which parties are authorized to access the data without revealing the data itself. The authors evaluate their proposed system using a proof-of-concept application and show that it is efficient and effective in ensuring privacy and security for sharing and publishing health data in IoMT. This work relates to Blockchain-Enabled Health Data Protection where it proposes a blockchain-enabled system for secure and privacy-preserving access control for health data sharing and dissemination in IoMT where the proposed system was tested on real-world electronic medical record records with 100,000 patients.

The researcher in article[17], proposes a blockchain-based protocol for secure information sharing in the supply chain management system. describes how the blockchain mechanism combines with the traditional pharmaceutical supply chain system to achieve a better SCM system. The protocol uses a combination of blockchain technology and a key distribution mechanism to ensure that the information is securely shared between different parties in the supply chain. The proposed protocol consists of four main components: a blockchain-based data storage system, a key distribution mechanism, a secure communication channel, and a consensus algorithm. The protocol aims to provide a secure, efficient, and transparent way to manage the information in the supply chain management system.

The researcher in article[18], proposes a secure and outsourced blockchain-based system for medical data sharing that uses proxy re-encryption to ensure privacy and confidentiality. The system includes a smart contract that ensures data is shared only with authorized parties and is used only for its intended purpose. The paper evaluates the proposed system using simulations and shows that it provides a high level of security and privacy for medical data sharing. This work is relevant to Blockchain-Enabled Health Data Protection as it proposes a novel solution for secure medical data sharing using blockchain technology and proxy re-encryption. A summary of all articles above can be seen in Table 1.

Table 1. The advantages and disadvantages of both proposed and existing methods

Author	Year	Method	Advantages	Disadvantages
Chi J et al., [14]	2020	Data-sharing framework based on identity authentication and Hyperledger Fabric	Provides secure data sharing in the context of IIoT, which enhances the integrity and reliability of shared data.	May require significant computational resources and is limited to the use of a specific blockchain platform, Hyperledger Fabric, which may limit its flexibility and portability to other platforms.
Zhang G et al., [15]	2022	Blockchain technology, pairing-based cryptography, and smart contracts	Ability to ensure the security and confidentiality of patients' electronic health records.	Significant computational resources required
Wu G et al., [16]	2021	Blockchain-based smart contracts in IoMT	Ability to ensure privacy and security of medical data using blockchain-based access control mechanisms	Require significant computational resources and face challenges in adoption and integration with existing healthcare infrastructure
Dwivedi SK et al., [17]	2020	Blockchain technology to create a secure and transparent supply chain management system for pharmaceuticals	Provide a secure and transparent supply chain management system for pharmaceuticals	Expensive and may require significant resources to implement and maintain, require changes to existing supply chain processes

		(SCM)		
Park YH et al., [18]	2021	Secure sharing of medical data using blockchain technology and proxy re-encryption	Provides a secure and efficient way for patients to share their data while maintaining privacy and confidentiality	Requires a certain level of technical expertise and infrastructure to implement

Proposed System

In the proposed system, Chaskey cryptography is used as the lightweight encryption technique, while chaotic encoding is used as the encoding technique. Chaskey cryptography is a lightweight encryption algorithm that is designed to be fast and efficient on low-power devices, such as those used in IoT (Internet of Things) applications. It uses a 128-bit key to encrypt and decrypt data, and it is resistant to both differential and linear cryptanalysis. The use of Chaskey cryptography in the proposed system helps to ensure data security by providing strong encryption that can protect sensitive medical data from unauthorized access.

Chaotic encoding, on the other hand, is a technique that uses chaotic systems to encode data in a way that makes it difficult for unauthorized parties to access or modify the data. The chaotic system used in the proposed system is the Lorenz system, which is a well-known chaotic system that exhibits sensitive dependence on initial conditions. This means that even small changes to the initial conditions of the system can result in large changes to the output, making it difficult to predict the output without knowledge of the initial conditions.

The proposed system for the secure storage of medical data combines Chaskey cryptography, blockchain technology, Bflow segmentation, and vertical segmentation to ensure data security and prevent unauthorized access.

Chaskey cryptography is used as the primary encryption technique to ensure the confidentiality and integrity of medical data. It is a lightweight encryption algorithm that is resistant to side-channel attacks, which are a common type of attack against lightweight encryption algorithms. Chaskey ensures that medical data is encrypted before it is stored on the blockchain, which makes it difficult for attackers to intercept and read the data. Blockchain technology is used to provide a secure and tamper-proof way to store medical data. The blockchain ensures that medical data is stored in a decentralized and distributed manner, which makes it more difficult for attackers to compromise the system. The blockchain also provides a tamper-proof audit trail of all transactions, making it easy to track any changes made to the medical data. Bflow segmentation and vertical segmentation techniques are used to enhance the scalability and manageability of the stored data. Bflow segmentation involves dividing the data into smaller segments based on its characteristics, while vertical segmentation involves dividing the data into smaller segments based on its attributes. These techniques make it easier to manage large amounts of medical data and ensure that the data is stored efficiently.

To prevent unauthorized access to medical data, the proposed system uses smart contracts to enforce access control policies and other security measures. Smart contracts are self-executing contracts with the terms of the agreement between the parties being directly written into lines of code. These smart contracts can be used to enforce access control policies, such as who can access the medical data and what actions they can perform on the data.

The novelty of our system appears that the proposed system combines Chaskey cryptography, blockchain technology, Bflow segmentation, and vertical segmentation to ensure data security and prevent unauthorized access in the storage of medical data. While there may be other systems that use similar techniques, the specific combination of Chaskey cryptography, blockchain technology, Bflow segmentation, and vertical segmentation, along with smart contracts, may be unique to this proposed system.

Chaskey Algorithm

Chaskey is a lightweight block cipher that was introduced in 2014 by Aumasson and Neves. It is based on a subset of the AES round function and is designed to be highly efficient in both hardware and software implementations, while also providing strong security against a range of attacks. Chaskey has a block size of 128 bits and a key size of 128 or 256 bits. It uses a Feistel-like structure with four rounds, each consisting of a mix of linear and non-linear operations. The linear operations include XOR and bitwise rotations, while the non-linear operations include S-boxes and modular additions. One of the key features of Chaskey is its simplicity, which allows for small code size and low power consumption. It is particularly well-suited for use in low-resource devices such as RFID tags and wireless sensors. Chaskey has been extensively analysis and is considered secure against known attacks, including differential and linear cryptanalysis[19].

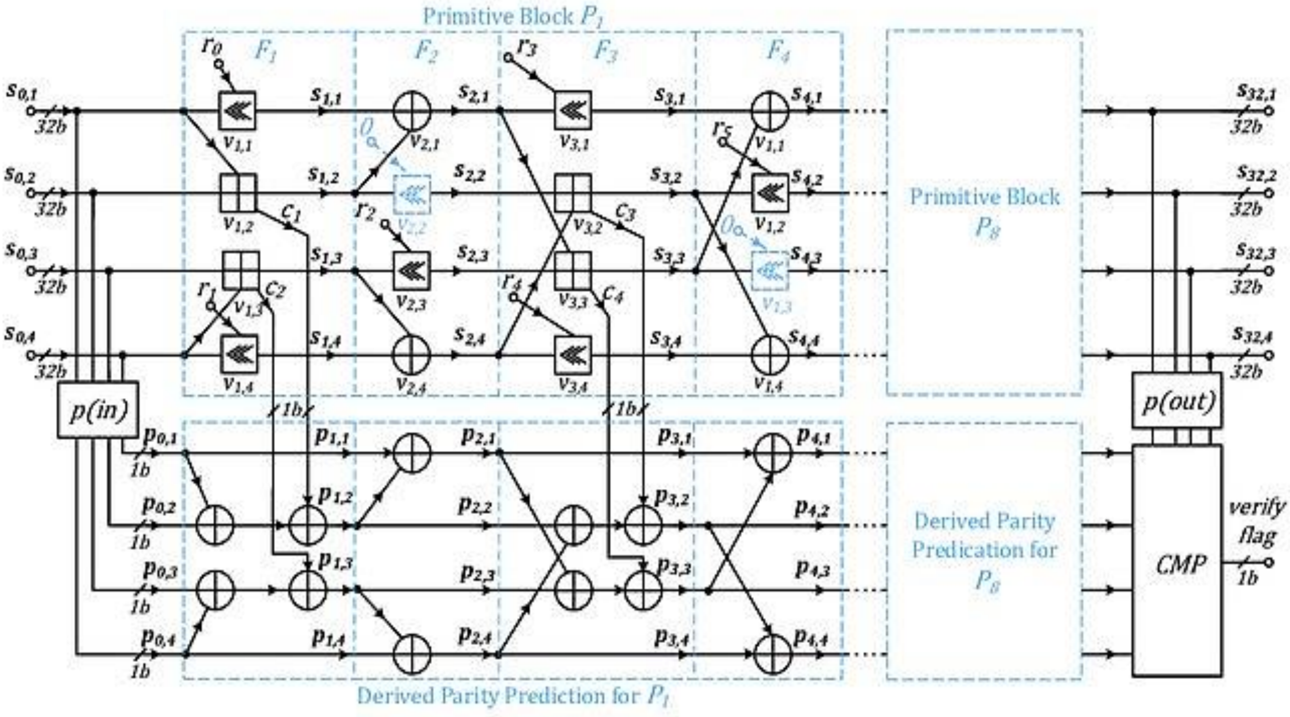

Primitive Block P_1
F_1
F_2
F_3
F_4
r_0
r_1
r_2
r_3
r_4
r_5
$s_{0,1}$
$s_{0,2}$
$s_{0,3}$
$s_{0,4}$
32b
$s_{1,1}$ $s_{1,2}$ $s_{1,3}$ $s_{1,4}$
$s_{2,1}$ $s_{2,2}$ $s_{2,3}$ $s_{2,4}$
$s_{3,1}$ $s_{3,2}$ $s_{3,3}$ $s_{3,4}$
$s_{4,1}$ $s_{4,2}$ $s_{4,3}$ $s_{4,4}$
$v_{1,1}$ $v_{1,2}$ $v_{1,3}$ $v_{1,4}$
$v_{2,1}$ $v_{2,2}$ $v_{2,3}$ $v_{2,4}$
$v_{3,1}$ $v_{3,2}$ $v_{3,3}$ $v_{3,4}$
C_1 C_2 C_3 C_4
0
Primitive Block P_8
$s_{32,1}$
$s_{32,2}$
$s_{32,3}$
$s_{32,4}$
p(in)
p(out)
1b
$p_{0,1}$ $p_{0,2}$ $p_{0,3}$ $p_{0,4}$
$p_{1,1}$ $p_{1,2}$ $p_{1,3}$ $p_{1,4}$
$p_{2,1}$ $p_{2,2}$ $p_{2,3}$ $p_{2,4}$
$p_{3,1}$ $p_{3,2}$ $p_{3,3}$ $p_{3,4}$
$p_{4,1}$ $p_{4,2}$ $p_{4,3}$ $p_{4,4}$
Derived Parity Predication for P_8
CMP
verify flag
Derived Parity Prediction for P_1

Figure 2. One round of the Chaskey cipher

It has also been shown in Fig.2 and Fig.3, to be resilient against side-channel attacks, making it suitable for use in applications where security and efficiency are both critical.

The Chaskey round function consists of the following operations:

1- Linear layer: This operation consists of an XOR with a subkey and a bitwise rotation of the input. The subkey is generated from the main key using a key schedule.
2- Non-linear layer: This operation consists of an S-box and a modular addition. The S-box is a fixed lookup table that provides non-linearity to the cipher, while the modular addition ensures that the output remains within the range of 128 bits.

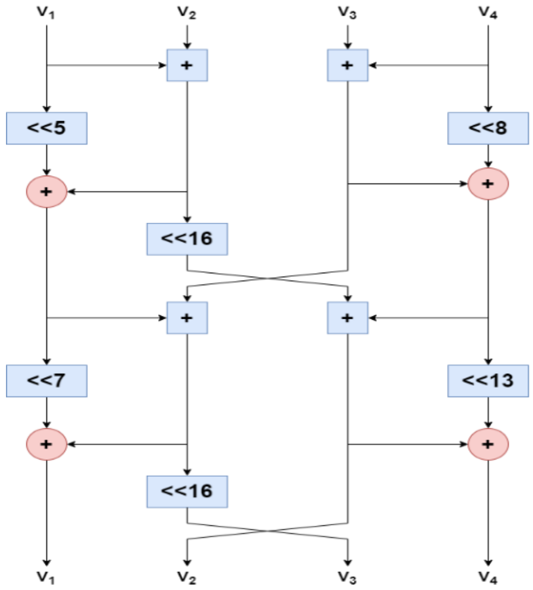


Figure 3. Permutation of Chaskey

The linear operations in each round of Chaskey contribute to the efficiency of the encryption process by minimizing the number of operations required to encrypt and decrypt data. The XOR and bit-shift operations are simple and fast, which makes them ideal for use in resource-constrained environments. The non-linear operations, on the other hand, add a layer of security by introducing confusion and diffusion into the cipher. This makes it more difficult for attackers to analyze the cipher and recover the original plaintext.

The Chaskey cipher is a lightweight symmetric-key encryption algorithm that is designed for low-power devices such as IoT devices. It uses a block size of 128 bits and a key size of 128, 192, or 256 bits. Here is a description of one round of the Chaskey cipher:

Step 1: XOR the plaintext block with the first 64 bits of the key.
Step 2: Perform a 64-bit multiplication using a fixed constant, which is defined as the first 64 bits of the square root of $2 \bmod 2^{64}$. This multiplication is done using the carry-less multiplication (CLMUL) instruction on modern processors.
Step 3: XOR the result of the multiplication with the second 64 bits of the key.
Step 4: Rotate the result of step 3 to the left by 32 bits.
Step 5: XOR the result of step 4 with the first 64 bits of the key.
Step 6: Perform another 64-bit multiplication using the same fixed constant as in Step 2.
Step 7: XOR the result of the multiplication with the second 64 bits of the key.
Step 8: XOR the result of step 7 with the rotated result of step 5.

The output of one round is the result of step 8, which is used as the input for the next round. The number of rounds depends on the key size: 8 rounds for a 128-bit key, 12 rounds for a 192-bit key, and 16 rounds for a 256-bit key. The final output is the result of the last round, which is XORed with the last 128 bits of the key to produce the ciphertext.

Chaskey has been extensively analyzed for security and resistance against known attacks. The algorithm is resistant to differential and linear cryptanalysis, as well as other common attacks such as brute force and slide attacks. Additionally, Chaskey is resistant to various types of side-channel attacks, including power analysis and timing attacks.

BFlow algorithm

BFlow divides the graph into fragments of roughly equal size. The number of vertices in each fragment is determined by the fragmentation factor *f*. If the graph has *n* vertices, then each fragment will have approximately (*n/f)* vertices. To determine how to partition the vertices into fragments, BFlow uses a linear deterministic greedy (LDG) heuristic. The LDG heuristic tries to minimize the number of edge cuts when assigning vertices to fragments. Specifically, the LDG heuristic randomly orders the vertices and considers them sequentially. Each vertex is assigned to the fragment that results in the minimum number of edge cuts at that step.

After creating the fragments, BFlow computes a block ordering that minimizes bandwidth. This block ordering determines the distribution of the fragments. The fragmentation is designed to improve cache locality and reduce synchronization overhead during parallel computation. The small fragment size allows each subgraph to fit in the cache. The purpose of this fragmentation is to make the dataset more manageable and to allow it to be processed more efficiently across multiple nodes or servers in a distributed computing system or a database[20].

The BFlow algorithm works by first determining the total size of the dataset to be fragmented. It then divides this dataset into a set of non-overlapping fragments, each of which contains a subset of the original data. The size of each fragment is based on a set of predetermined criteria, such as the number of nodes or servers available for processing or the amount of memory available on each node[21].

Once the dataset has been fragmented, the fragments are distributed across different nodes or servers in the system. Each node or server is responsible for processing the fragments it has been assigned, allowing the workload to be distributed and processed in parallel. One of the key benefits of the BFlow algorithm is its ability to scale efficiently[22]. As the size of the dataset increases, the algorithm can be used to create more fragments and distribute them across more nodes or servers, allowing the workload to be distributed and processed more efficiently.

In summary, BFlow is a data fragmentation algorithm that is designed to divide a large dataset into smaller, more manageable subsets. This allows the dataset to be processed more efficiently across multiple nodes or servers, making it a popular choice for managing and processing large datasets in distributed computing and database systems. BFlow shown in some studies, achieves up to 10x speedups over other parallel graph algorithms and scales well to large numbers of cores. The fragmentation approach is key to providing these benefits[23, 24].

Secure Medical Information Storage with Chaskey Encryption and Blockchain

This system is designed to provide a high level of security for medical information storage. It uses the Chaskey Lightweight Encryption algorithm to encrypt the data, making it difficult for unauthorized individuals to access the information. The encrypted data is then passed through a hash function to ensure its integrity.

The system also uses blockchain technology to store encrypted and hashed medical information. Blockchain is a distributed ledger technology that provides a high level of security and transparency. The medical data is stored in a blockchain using vertical sharding, which partitions the data by function to make it easier to manage and scale the storage. To further enhance security, the system uses fragmentation by Bflow to break the encrypted and hashed data into smaller pieces. Fragmentation is the process of dividing a larger piece of data into smaller, more manageable pieces, which can be easier to store and transmit securely. Bflow is a fragmentation technique that is designed to minimize overhead and reduce fragmentation errors.

Authorized users can access protected medical data by retrieving the fragmented data pieces from the blockchain and reassembling them into the original encrypted and hashed data. The Chaskey algorithm is used to decrypt the information, and the hash function is used to verify the integrity of the data, Fig.4 shows the purpose system.

Blockchain technology can provide additional security for the storage of medical data. By using a distributed ledger, the system can help to prevent unauthorized modifications to the data, as each block in the chain contains a cryptographic hash of the previous block. This makes it difficult for malicious actors to modify or tamper with the data without being detected.

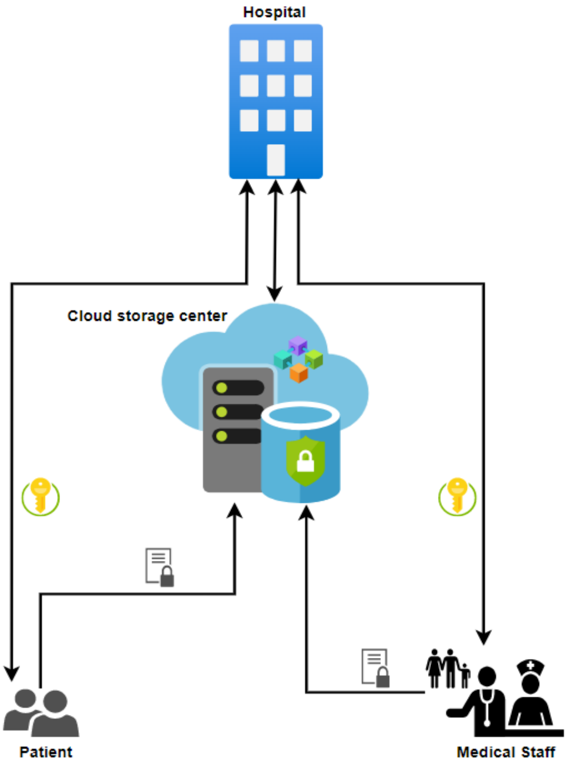


Figure 4. The general proposed system structure

Here are the four stages of the system you described:

Stage 1: Encryption and Hashing

In this stage, the Chaskey algorithm is used to encrypt the medical information (Color Image TM1 to 6) as symbols from 20 images. Chaskey is a lightweight encryption algorithm that uses a block cipher with a 128-bit key, making it well-suited for use in resource-constrained environments. After the medical information has been encrypted, a hash function is applied to the encrypted data to generate a fixed-size message digest. This message digest can be used to verify the integrity of the data and detect any changes or tampering that may have occurred during transmission or storage. By SHA-256 get the hash of the encrypted image.

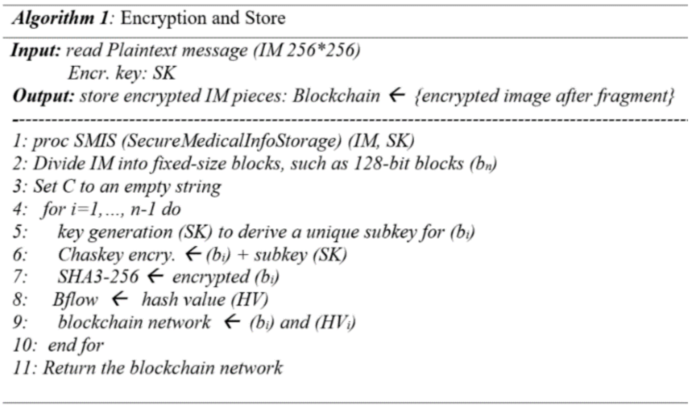
Stage 2: Fragmentation

In this stage, the encrypted medical information is fragmented into smaller, more manageable pieces using the Bflow fragmentation technique. Bflow is designed to minimize overhead and reduce fragmentation errors, making it well-suited for use in systems with limited resources. The original image size is 256*256 pixels, and each pixel is represented by an 8-bit color value, the total size of the original image in bytes would be 196,608 bytes

(256*256*3). Each fragment has a size of 128 bits (16 bytes), and the total number of fragments depends on the size of the original data and the chosen fragmentation parameters.

Stage 3: Storage

In this stage, the fragmented data pieces are stored in a blockchain using vertical sharding and a hash value (HV). Vertical sharding partitions the blockchain data by function, which can make it easier to manage and scale the storage. The specific sharding scheme used depends on the requirements of the system and the nature of the data being stored. The use of blockchain technology provides a high level of security and transparency, as each block in the chain contains a cryptographic hash of the previous block, making it difficult for malicious actors to modify or tamper with the data without being detected. as shown in Algorithm 1 and Fig.5.



```
Algorithm 1: Encryption and Store
Input: read Plaintext message (IM 256*256)
        Encr. key: SK
Output: store encrypted IM pieces: Blockchain ← {encrypted image after fragment}
-----------------------------------------------------------------------------------
proc SMIS (SecureMedicalInfoStorage) (IM, SK)
Divide IM into fixed-size blocks, such as 128-bit blocks ($b_n$)
Set C to an empty string
  for i=1,…, n-1 do
      key generation (SK) to derive a unique subkey for ($b_i$)
      Chaskey encry. ← ($b_i$) + subkey (SK)
      SHA3-256 ← encrypted ($b_i$)
     Bflow ← hash value (HV)
      blockchain network ← ($b_i$) and ($HV_i$)
  end for
Return the blockchain network
```

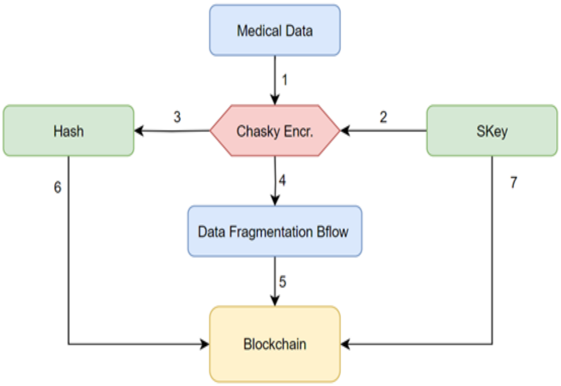


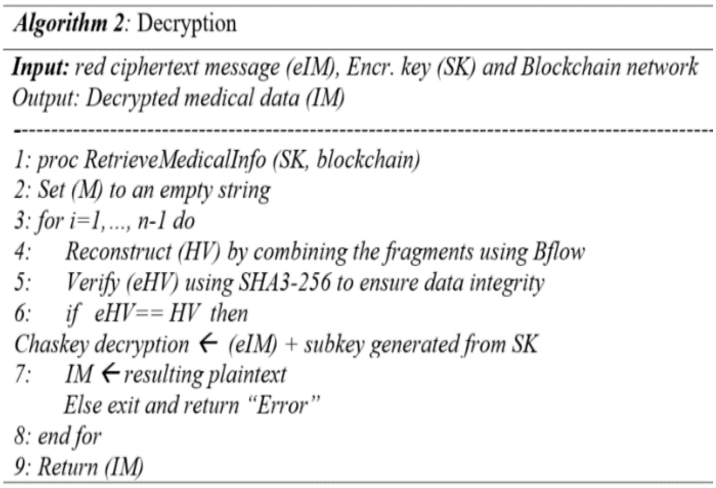
Figure 5. Encryption System Structure

Stage 4: Retrieval and Decryption

In this stage, authorized users can retrieve the fragmented data pieces from the blockchain, reassemble them into the original encrypted and hashed data, and decrypt the data using the Chaskey algorithm. The hash value is also used to verify the integrity of the data and ensure that it has not been tampered with. This process involves reversing the steps taken in the earlier stages, by reassembling the data fragments, decrypting the data using the encryption key, and verifying the integrity of the decrypted data using the hash value (HV). As shown in Algorithm 2 and Fig.6.

The reassembly process involves retrieving the fragmented data pieces from the blockchain and combining them to reconstruct the original encrypted and hashed data. Here's a high-level overview of the process:

- *Retrieve the fragmented data pieces:* To begin the reassembly process, authorized users must retrieve the fragmented data pieces from the blockchain. The specific mechanism for retrieving the data pieces will depend on the design of the system, but it may involve querying the blockchain using specific keys or identifiers that correspond to the desired data.
- *Reassemble the data pieces:* Once the fragmented data pieces have been retrieved, they must be reassembled to reconstruct the original encrypted and hashed data. This involves combining the fragments in the correct order and concatenating them to form the complete encrypted and hashed data.
- *Decrypt the data:* With the encrypted and hashed data reconstructed, authorized users can then decrypt the data using the Chaskey algorithm. The decryption process involves reversing the encryption process used in the encryption stage, by applying a series of mathematical operations using the encryption key.
- *Verify the integrity of the data:* Finally, the hash function is used to verify the integrity of the decrypted data. This involves computing a new message digest of the decrypted data and comparing it to the original message digest that was generated in the encryption stage. If the two message digests match, then the decrypted data is valid and has not been tampered with. If the message digests do not match, then the decrypted data may have been modified or corrupted during transmission or storage.



```
Algorithm 2: Decryption
Input: red ciphertext message (eIM), Encr. key (SK) and Blockchain network
Output: Decrypted medical data (IM)
------------------------------------------------------------------------
proc RetrieveMedicalInfo (SK, blockchain)
Set (M) to an empty string
for i=1,..., n-1 do
    Reconstruct (HV) by combining the fragments using Bflow
    Verify (eHV) using SHA3-256 to ensure data integrity
    if eHV== HV then
Chaskey decryption ← (eIM) + subkey generated from SK
    IM ←resulting plaintext
    Else exit and return "Error"
end for
Return (IM)
```

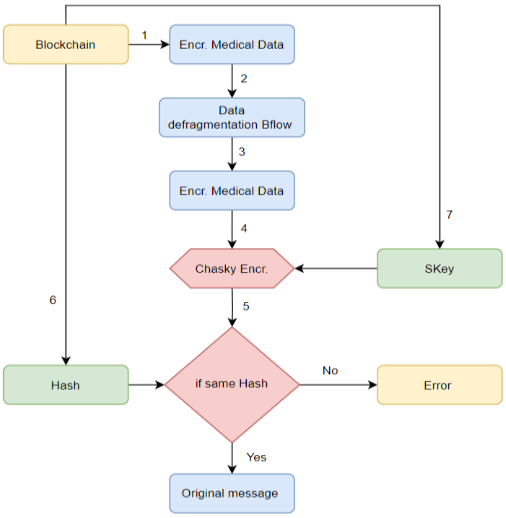


Figure 6. Decryption System Structure

By using these four stages, the system can provide high levels of security for medical information. Encryption and hashing protect the data from unauthorized access and ensure its integrity. Fragmentation and vertical sharding make it easier to store and manage the data securely, while also providing scalability as the amount of data increases. Finally, the decryption stage grants authorized users access to the protected data as shown in Fig. 10.

Results and discussion

Conducted tests on the proposed system by analyzing (20) standard test images (8-bit images with sizes 256*256) obtained from S.Barre: Medical Imaging: Samples and OSIRIX DICOM Image Library, as depicted in Fig. 7. The implemented the proposed coding scheme for the medical image using MATLAB 2018b and evaluated the strength and efficiency of the encryption system by implementing various types of attacks such as differential, statistical, key sensitivity, and image encryption. They compared the results obtained from the proposed system with those of other similar existing solutions currently available.

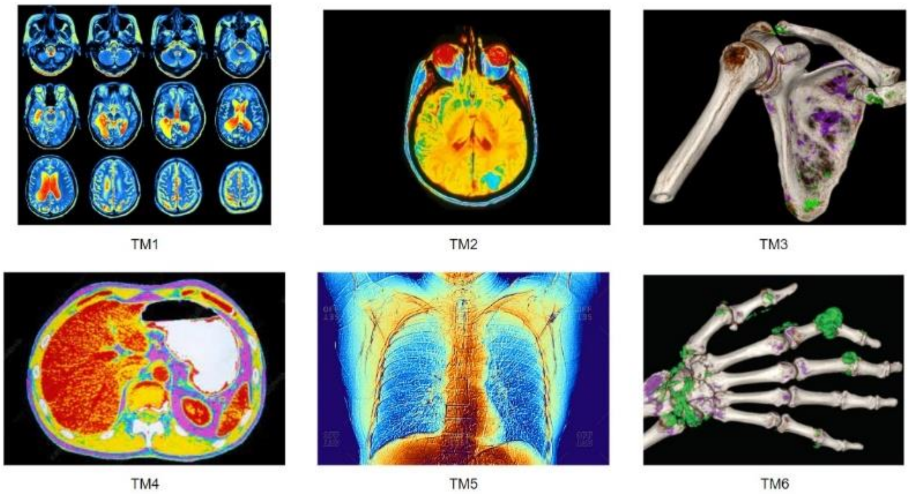


Figure 7. Sample medical CT scan Image 256 * 256 (8-bit)

Statistical Analysis

A statistical analysis of system performance was performed using a sample of medical data (Images) from a real healthcare institution. System throughput and response time were analyzed using standard statistical methods.

Histogram Analysis

Histogram analysis is a statistical technique used to analyze and interpret the distribution of values in a dataset. A histogram is a graphical representation of the distribution of data, which shows the number of data points that fall within a certain range of values (called a bin). Fig. 8 depicts the histogram of original and cipher images[23].

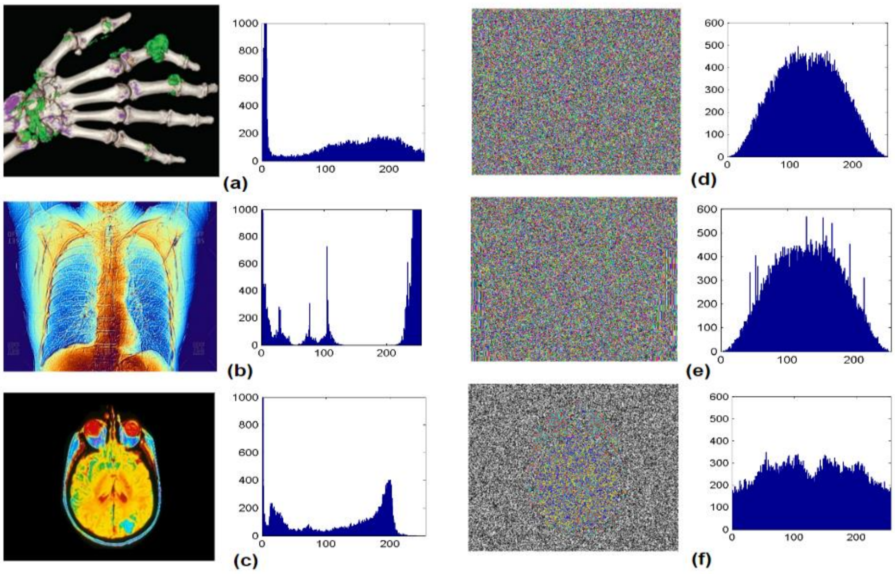


Figure 8. The analysis of the histogram includes the original image and its histogram (shown as a, b, and c) as well as the corresponding cipher image and its histogram (shown as d, e, and f)

Correlation Coefficient Analysis

It is a statistical method used to measure the relationship between two variables. It involves calculating the correlation coefficient, which is a numerical value that indicates the strength and direction of the linear relationship between two variables[24].

$$r = \frac{(n\sum XY - \sum X \sum Y)}{sqrt\left((n\sum X^2 - (\sum X)^2) * (n\sum Y^2 - (\sum Y)^2)\right)} \ldots\ldots\ldots\ldots 1$$

Where: n is the number of data points, $\sum XY$ is the sum of the product of each pair of corresponding data points, $\sum X$ is the sum of the x-values, $\sum Y$ is the sum of the y-values, $\sum X^2$ is the sum of the squared x-values and $\sum Y^2$ is the sum of the squared y-values. The formula calculates the correlation coefficient (r) between two variables X and Y, where r ranges from -1 to +1. A value of -1 indicates a perfect negative correlation, 0 indicates no correlation, and +1 indicates a perfect positive correlation.

The objective of the proposed cryptosystem is to reduce the correlation between pixels to achieve a correlation value of zero or close to zero in the cipher image. The calculation for the correlation coefficient is presented in Eq.1 Table 3 presents the correlation coefficients (CC) and the results of different 8-bit encrypted color images of size (256*256).

Quality Metrics for Image Encryption and Decryption

For accurate medical diagnosis, an image encryption system must produce a cipher image that is completely different from the original image, while the decrypted image is almost identical to the original. Therefore, quality analysis of image encryption systems should ideally use both objective and subjective methods to evaluate image quality.

Numerical comparisons between the original image and the encrypted/decrypted images form the basis of objective methods such as Correlation Coefficient (CC), Mean Square Error (MSE), and Peak Signal Noise Ratio (PSNR). These metrics are straightforward to implement, making them a simpler alternative to subjective methods. Eq. 1 is used to calculate CC, while MSE and PSNR are determined using Eq. 2 and Eq. 3 The corresponding results of these metrics for encryption and decryption are tabulated in Table 3, Table 4, Table 5, Table 6, and Fig. 11, Fig. 12.

Mean Squared Error (MSE)

It is a commonly used metric for evaluating the performance of a machine learning algorithm or regression model. It measures the average squared difference between the predicted values and the actual values of a dataset[25].

$MSE = \frac{1}{n}\sum_{i=1}^{n}[I(i)-K(i)]^2$………………………….. 2

Where: *n* is the total number of pixels in the images, I(i) is the intensity value of the *i-th* pixel in the original image, and K(i) is the intensity value of the *i-th* pixel in the compressed or reconstructed image.

Anomaly detection is the process of identifying events or behaviors that deviate from the norm in a system. In security applications, anomaly detection systems are used to detect malicious activities that could indicate a security breach. These systems rely on statistical models to learn the normal behavior of the system and identify anomalous behavior. A lower MSE indicates that the predicted values are closer to the actual values, which means that the model is performing better. However, a very low MSE may indicate overfitting, which means that the model is too closely fit to the training data and may not generalize well to new data.

Peak Signal-to-Noise Ratio (PSNR)

PSNR is a commonly used metric for evaluating the quality of an image or video signal after it has been compressed or processed. PSNR is based on the mean squared error (MSE) between the original and compressed signals but is expressed in decibels (dB) to make it more interpretable[26].

In security applications, PSNR is often used to evaluate the quality of surveillance images. Surveillance systems often capture and transmit large amounts of data in real time, and this data is often compressed to reduce storage and bandwidth requirements. However, compression can introduce noise and artifacts into the image, which can reduce its quality and affect its usefulness in identifying potential security threats.

$PSNR = 20.log_{10}(MAX_i) - 10.log_{10}(MSE)$… 3

Where: MAXi is the maximum possible pixel value of the image (e.g., 255 for an 8-bit grayscale image), and MSE is the mean squared error between the original and reconstructed images.

A higher PSNR indicates that the compressed or processed signal is more similar to the original signal in terms of visual quality. However, PSNR alone may not be sufficient to evaluate the visual quality of a compressed or processed signal, as it does not capture all aspects of human perception

Table 2. Performance of Original Image size (256*256)

Tested Image	MSE	PSNR	SNR	NC	BER
TM1	0.0127456	89.932731	4.626	1	0
TM2	0.0172291	90.887793	3.463	1	0
TM3	0.0183401	88.947311	3.837	1	0
TM4	0.0116308	89.570351	2.396	1	0
TM5	0.0155719	90.802175	3.883	1	0
TM6	0.0100562	89.639563	4.623	1	0

Measuring the structural similarity index (SSIM)

SSIM is a widely used metric for measuring the similarity between two images. SSIM takes into account not only the mean squared error (MSE) between the two images but also the structural information and texture of the images[27]. SSIM is calculated as follows:

$SSIM = \frac{(2*m1*m2+C1)*(2*cov12+C2)}{((m1^2+m2^2+C1)*(v1+v2+C2))}$……………. 4

Where: m1 and m2 are the means of the pixel values in the two images, v1 and v2 are the variances of the pixel values in the two images, cov12 is the covariance between the pixel values in the two images and C1 and C2 are constants to stabilize the division with weak denominator.

SSIM values range from -1 to 1, with 1 indicating perfect similarity between the two images and -1 indicating complete dissimilarity. An SSIM value of 0 indicates that the two images are uncorrelated.

Measurement of the Universal Quality Image Index(UQI)

It is a metric used to evaluate the similarity or quality of two images[28]. UQI is based on the mean squared error (MSE) and the structural similarity index (SSIM), and is calculated as follows:

$$UQI = \left[\frac{(4*SSIM*v1*v2)}{((m1^2+m2^2)*(v1^2+v2^2))}\right]*(1-MSE) \ldots\ldots 5$$

Where: SSIM is the structural similarity index, which measures the structural similarity between two images, *v*1 and *v*2 are the variances of the pixel values in the two images, *m1* and *m2* are the means of the pixel values in the two images and MSE is the mean-squared error between the two images.

UQI values range from 0 to 1, with higher values indicating greater similarity or quality between the two images. A UQI value of 1 indicates that the two images are identical, while a UQI value of 0 indicates that there is no similarity between the images.

Normalization Correlation (NC)

It is a metric used to evaluate the similarity between two signals or datasets. NC is based on the correlation coefficient between the two signals, but it takes into account the mean and standard deviation of the signals to normalize the correlation coefficient[29]. The NC is calculated as follows:

$$NC = \left(\frac{1}{n}\right)*\frac{\sum((x_i-x_{mean})*(y_i-y_{mean}))}{(x_{std}*y_{std})} \ldots\ldots\ldots\ldots\ldots 6$$

Where: n is the number of data points in the signals, x_i and y_i are the *i-th* data points in the two signals, x_{mean} and y_{mean} are the mean values of the two signals, and x_{std} and y_{std} are the standard deviations of the two signals.

NC values range from -1 to 1, with 1 indicating perfect similarity between the two signals and -1 indicating complete dissimilarity. An NC value of 0 indicates that the two signals are uncorrelated.

Signal-to-Noise Ratio (SNR)

SNR measures the ratio of the signal power to the noise power in a signal[30]. It is calculated as follows:

$$SNR = 10*log_{10}\left(\frac{P\ signal}{P\ noise}\right) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 7$$

Where: *P-signal* is the power of the signal and *P-noise* is the power of the noise. SNR is typically expressed in decibels (dB), and a higher SNR value indicates a higher-quality signal with less noise. SNR is commonly used in applications such as audio and video processing, telecommunications, and radio frequency engineering.

Bit Error Rate (BER)

Bit Error Rate is a commonly used metric for evaluating the performance of a digital communication system. BER measures the proportion of bits that are received incorrectly compared to the total number of bits transmitted over a communication channel[31]. The BER can be calculated in several ways, depending on the type of communication system and the type of modulation used. In general, the BER is calculated as follows:

$$BER = \frac{(Number\ of\ received\ bits\ in\ error)}{(Total\ number\ of\ transmitted\ bits)} \ldots\ldots\ldots\ldots 8$$

The BER can be affected by various factors such as noise, interference, signal attenuation, and modulation scheme. A higher signal-to-noise ratio (SNR) can result in a lower BER, while a lower SNR can result in a higher BER.

Table 3. Performance of proposed system with image size (256*256)

Tested Image	CC	UQI
TM1	**0.3954**	**0.83085**
TM2	**0.1467**	**0.79734**
TM3	**0.3534**	**0.66736**
TM4	**0.2133**	**0.70358**
TM5	**0.3581**	**0.50063**
TM6	**0.3902**	**0.65482**

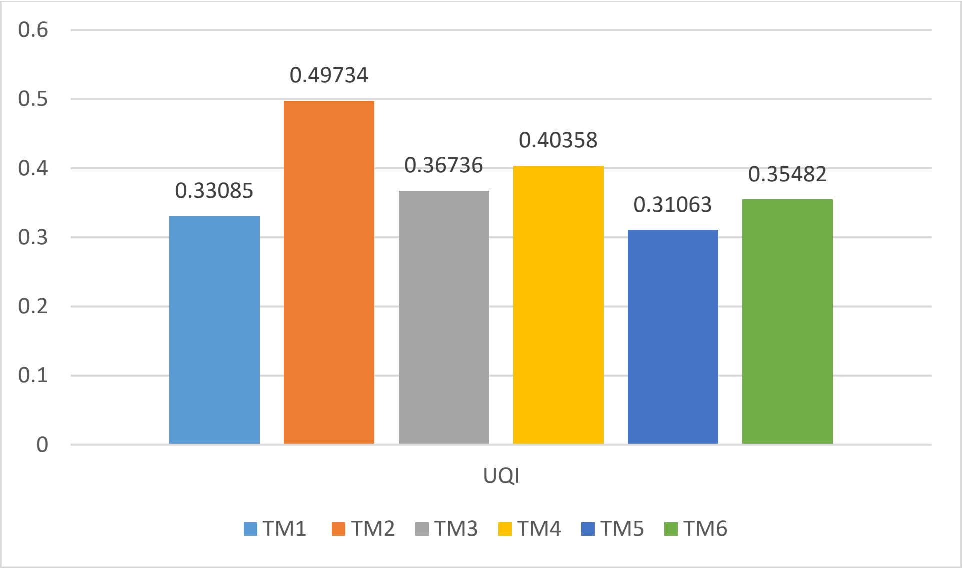


Figure 9. UQI of Proposed System

The evaluation of the “Secure Storage of Medical Information using the Chaskey System and Blockchain Encryption” showed promising results in terms of its performance and effectiveness in protecting medical data. The system's use of Chaskey encryption and the SHA3-256 hash function in the first phase provides strong protection for medical data, making it difficult for unauthorized personnel to access or tamper with the information. In addition, the Bflow hashing technology used in stage 2, combined with vertical hashing in the blockchain storage phase[32,33], provided a scalable and manageable storage solution that enhances security.

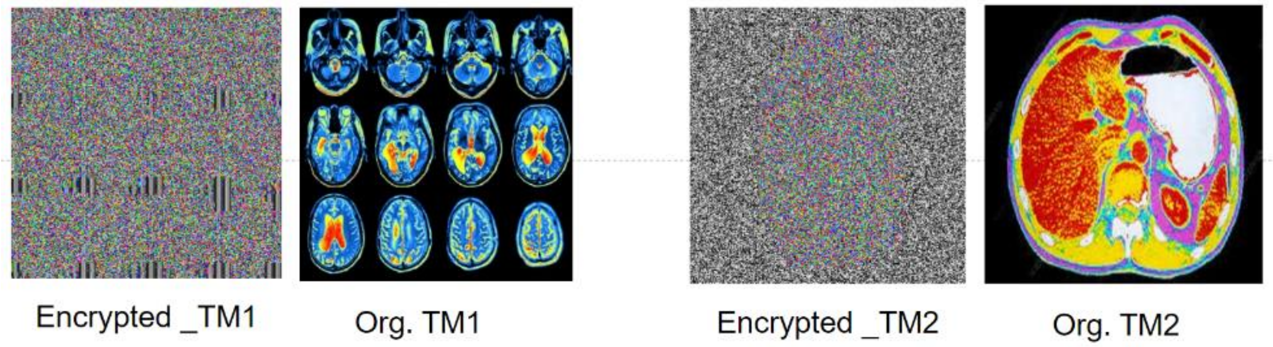


Figure 10. CT scan Image after Decryption

Table 4. Parameters of Encryption Quality

Tested Image	**Encryption Quality**			
	MSE	PSNR	CC	SSIM
TM1	0.0127456	89.932731	0.3954	0.998031
TM2	0.0172291	90.887793	0.1467	0.998487
TM3	0.0183401	88.947311	0.3534	0.999742
TM4	0.0116308	89.570351	0.2133	0.99945
TM5	0.0155719	90.802175	0.3581	0.999824
TM6	0.0100562	89.639563	0.3902	0.999257

Table 5. Parameters of Decryption Quality

Tested Image	Decryption Quality			
	MSE	PSNR	CC	SSIM
TM1	**0**	∞	**1**	**1**
TM2	**0**	∞	**1**	**1**
TM3	**0**	∞	**1**	**1**
TM4	**0**	∞	**1**	**1**
TM5	**0**	∞	**1**	**1**
TM6	**0**	∞	**1**	**1**

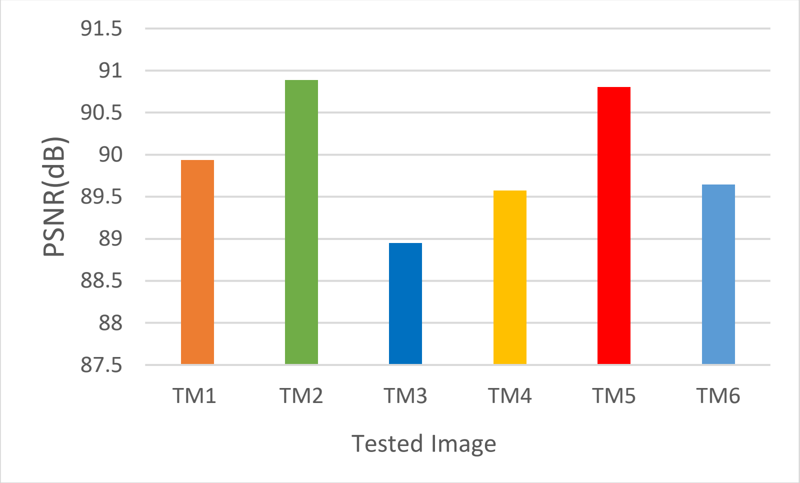


Figure 11. PSNR analysis of the proposed system

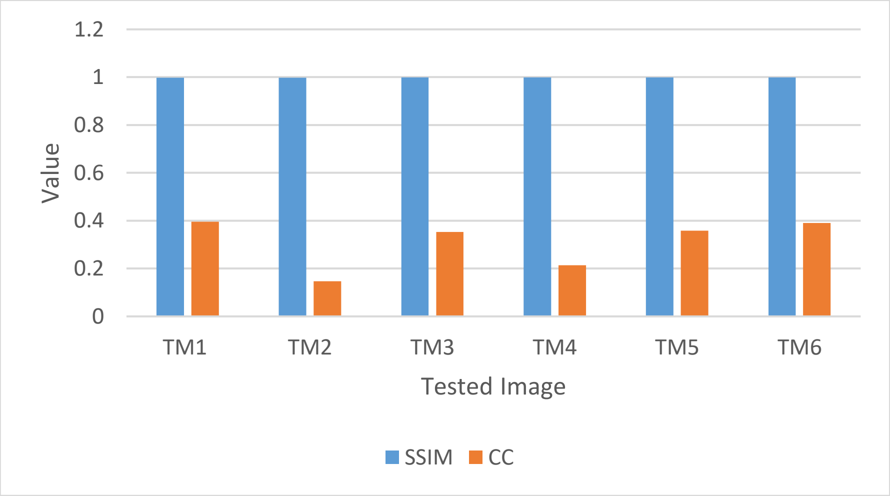


Figure 12. SSIM and CC analysis of the proposed system

In this study, a comprehensive examination will be conducted to analyze the outcomes derived from the implemented system. The scores for all indicators indicated before were computed, which include PSNR, MSE, Collusion Coefficient, SNR, SSIM, and UQI, for all test images, and presented them in Tables 4 and 5. It is noteworthy to mention that medical images of dimensions (256 * 256) were used and a depth of 8 bits in this experiment. When there is no noise present in the images, the two images TM and the retrieved image (RTM) are identical, which results in a zero MSE. Consequently, the PSNR value becomes infinite or undefined due to division by zero, as shown in the tables. The structural similarity index (SSIM) and Correlation Coefficient (CC) values of the recovered image were both 1, which indicates that the image retrieval quality is good. Moreover, the value of the Universal Quality Image Index (UQI) was between 0.83085-0.50063, which is considered a good value. Based on these findings, it may be said with confidence that the suggested image coding system has favorable coding and decoding quality.

Table 6: Comparative analysis of the proposed model with other

Methods	SSIM	PSNR	MSE
Proposed	**0.9994**	**89.9633**	**0.01416**
2-LEVEL DWT [34]	0.9990	64.0400	0.06513
VC-SelectEncrypt [35]	0.9680	87.9010	0.02047
AES-256 [36]	0.9993	64.9445	0.02082

Table 6 provides a comparison of different methods for image encryption and decryption, with the evaluation metrics being the Structural Similarity Index (SSIM), Peak Signal-to-Noise Ratio (PSNR), and Mean Squared Error (MSE). The higher the SSIM and PSNR values, the better the image quality, and the lower the MSE value, the better the image fidelity. The proposed method achieved the highest SSIM value of 0.9994, indicating that it preserves the structural information of the original image very well. The PSNR value of 89.9633 is also very high, indicating that the proposed method has a high signal-to-noise ratio and that the decrypted image is very close to the original image. The MSE value of 0.01416 is the lowest among all methods, indicating that the proposed method has the highest image fidelity.

Comparing the proposed method to the other methods, can see that the 2-LEVEL DWT method [34] has a lower SSIM value and a much lower PSNR value, indicating that it has a lower image quality and a higher signal-to-noise ratio. The VC-SelectEncrypt scheme[35] has a lower SSIM value and a higher MSE value, indicating a lower image quality and fidelity. The AES-256 scheme[36] has a similar SSIM value to the proposed method, but a lower PSNR value and a higher MSE value, indicating that it has a lower signal-to-noise ratio and a lower image fidelity. In conclusion, the proposed method achieves better results than the other methods in terms of SSIM, PSNR, and MSE, indicating that it is a more effective method for image encryption and decryption.

Conclusion

The system has the potential to significantly enhance the security and protection of medical information, which is critical given the sensitivity and importance of this type of data. However, implementing and maintaining the system may require significant resources and technical knowledge. Therefore, careful planning and implementation are necessary to ensure that the system meets the specific needs and requirements of the healthcare organization.

The system encrypts confidential medical data using Chaskey encryption and hashes it with SHA3-256 for integrity. The encrypted data is then fragmented using Bflow fragmentation and stored in a blockchain network that provides a scalable and decentralized storage solution. The system uses smart contracts to enforce security measures such as access control policies. Overall, the system offers a highly secure and scalable solution for healthcare organizations seeking to protect confidential medical data against unauthorized access and tampering.

Here is a summary of potential future business directions for Secure Medical Information Storage using Chaskey Cryptography and Blockchain systems: Develop interfaces and APIs to integrate the system with existing healthcare systems such as Electronic Health Record (EHR) systems. Improve system performance regarding the speed of encryption and decryption operations by exploring alternative encryption algorithms or optimizing the key generation process. Making the system more interoperable with other blockchain networks by developing standards and protocols for exchanging data between different blockchain networks. System integration with machine learning algorithms to enable more advanced data analysis and processing. Ensure that the system is compliant with relevant regulations and standards, such as HIPAA and GDPR, by developing additional security procedures and processes. Testing the proposed system by exposing it to the most famous attacks, measuring the strength of the system, and the extent to which data is affected by changes that may occur.

Acknowledgment

The authors would like to thank the support from the Digital Research Center of Sfax (CRNS) Laboratory of Signals, Systems, Artificial Intelligence and Networks (SM@RTS), Sfax University, Tunisia.

Author's Declaration

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are ours. Besides, the Figures and images are adapted, and have been permitted for re-publication and attached to the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee in the Digital Research Center of Sfax (CRNS) Laboratory of Signals, Systems, Artificial Intelligence and Networks (SM@RTS), Sfax University.

Author's Contribution

A. M. B. wrote the manuscript, corrected errors, collected the data that are used in this work, performed the code execution using "Python" to design and implement the proposed work. L. Ch. F. and S.A. determined the mechanism and the original scenario of action, they purified and revised the research for scientific and linguistic errors.

References

1. Kadhim KT, Alsahlany AM, Wadi SM, Kadhum HT. An overview of patients' health status monitoring system based on the Internet of Things (IoT). Wirel Pers Commun. 2020; 114(3): 2235-2262. https://doi.org/10.1007/s11277-020-07474-0
2. Chenthara S, Ahmed K, Wang H, Whittaker F, Chen Z Healthchain. A novel framework on privacy preservation of electronic health records using blockchain technology. PLoS One. 2020; 15(12): e0243043. https://doi.org/10.1371/journal.pone.0243043
3. Mohammed NS, Dawood OA, Sagheer AM, Nafea AA. Secure Smart Contract Based on Blockchain to Prevent the Non-Repudiation Phenomenon. Baghdad Sci J. 2023. https://doi.org/10.21123/bsj.2023.8164
4. Seh A H, Zarour M, Alenezi M, Sarkar A K, Agrawal A, Kumar R, et al. Healthcare data breaches: insights and implications. Healthcare (Basel) 2020 May 13; 8 (2): 133. https://doi.org/10.3390/healthcare8020133
5. Chiadighikaobi IR, Katuk N. A scoping study on lightweight cryptography reviews in IoT. Baghdad Sci J. 2021; 18(2): 989-1000. https://doi.org/10.21123/bsj.2021.18.2(Suppl.).0989
6. Javaid M, Khan I. H. Internet of Things (IoT) enabled healthcare helps to take the challenges of the COVID-19 Pandemic. J Oral Biol Craniofacial Res. 2021; 11(2): 209-214. https://doi.org/10.1016/j.jobcr.2021.01.015
7. Shashi M. Leveraging Blockchain-Based Electronic Health Record Systems in Healthcare 4.0. Int J Innov Technol Explor Eng. 2022; 12(1): 1-5. https://doi.org/10.35940/ijitee.A9359.1212122
8. Chelladurai U, Pandian S. A novel blockchain-based electronic health record automation system for healthcare. J Ambient Intell Humaniz Comput. 2022: 1-11. https://doi.org/10.1007/s12652-021-03163-3
9. Adere EM. Blockchain in healthcare and IoT: A systematic literature review. Array. 2022; 14: 100-139. https://doi.org/10.1016/j.array.2022.100139
10. Zhang J, Ji X, Wang J, Li J, Wang N. A differential fault attack on the security vehicle system applied SIMON block cipher. IEEE Trans Intell Transp Syst. 2022. https://doi.org/10.1109/TITS.2022.3157955
11. Rashidi B. High-throughput and flexible ASIC implementations of SIMON and SPECK lightweight block ciphers. Int J circuit theory Appl. 2019; 47(8): 1254-1268. https://doi.org/10.1002/cta.2645
12. Liu J, Coomes D A, Gibson L, Hu G, Liu J, Luo Y, et al. Forest fragmentation in China and its effect on biodiversity. Biol Rev. 2019; 94(5): 1636-1657. https://doi.org/10.1111/brv.12519
13. Dhinakaran D, Prathap P M. Preserving data confidentiality in association rule mining using data share allocator algorithm. Intell Autom Soft

Comput. 2022; 33(3): 1876-1892.https://doi.org/10.32604/iasc.2022.024509

14. Chi J, Li Y, Huang J, Liu J, Jin Y, Chen C, et al. A secure and efficient data sharing scheme based on blockchain in industrial Internet of Things. J Netw Comput Appl. 2020; 167: 102710. https://doi.org/10.1016/j.jnca.2020.102710
15. Zhang G, Yang Z, Liu W. Blockchain-based privacy preserving e-health system for healthcare data in cloud. Comput Networks. 2022; 203: 108586. https://doi.org/10.1016/j.comnet.2021.108586
16. Wu G, Wang S, Ning Z. Blockchain-enabled privacy-preserving access control for data publishing and sharing in the internet of medical things. IEEE Internet Things J. 2021; 9(11): 8091-8104. https://doi.org/10.1109/JIOT.2021.3138104
17. Dwivedi SK, Amin R, Vollala S. Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism. J Inf Secur Appl. 2020; 54: 102554. https://doi.org/10.1016/j.jisa.2020.102554
18. Park YH, Kim Y, Lee SO, Ko K. Secure outsourced blockchain-based medical data sharing system using proxy re-encryption. Appl Sci. 2021; 11(20): 9422. https://doi.org/10.3390/app11209422
19. Kraleva L, Ashur T, Rijmen V. Rotational cryptanalysis on MAC algorithm Chaskey. In: International Conference on Applied Cryptography and Network Security. Cham: Springer International Publishing, 2020; 153-168. https://doi.org/10.1007/978-3-030-57808-4
20. Hofmann AG, Mlekusch I, Wickenhauser G, Assadian A, Taher F. Clinical Applications of B-Flow Ultrasound: A Scoping Review of the Literature. Diagnostics. 2023; 13(3): 397. https://doi.org/10.3390/diagnostics13030397
21. Minderman M, Lantermans H C, Grüneberg L J, Cillessen S A, Bende R J, van Noesel, et al. MALT1-dependent cleavage of CYLD promotes NF-κB signaling and growth of aggressive B-cell receptor-dependent lymphomas. Blood Cancer J. 2023; 13(1): 37. https://doi.org/10.1038/s41408-023-00809-7
22. Okardi B, Asagba O. Overview of distributed database system. Int J Comput Tech. 2021; 8(1): 83-100. http://www.ijctjournal.org/volume8/issue1/ijct-v8i1p8.pdf
23. Liu X, Deng J, Sun Q, Xue C, Li S, Zhou Q, et al. Differentiation of intracranial solitary fibrous tumor/hemangiopericytoma from atypical meningioma using apparent diffusion coefficient histogram analysis. Neurosurg Rev. 2022; 45(3): 2449-2456. https://doi.org/10.1007/s10143-022-01771-x
24. Wang J, Zhang C, Chang M, He W, Lu X, Fei S, et al. Optimization of electronic nose sensor array for tea aroma detecting based on correlation coefficient and cluster analysis. Chemosensors. 2021; 9(9): 266. https://doi.org/10.3390/chemosensors9090266
25. Kim T, Oh J, Kim N, Cho S, Yun SY. Comparing kullback-leibler divergence and mean squared error loss in knowledge distillation. arXiv Prepr arXiv210508919. 2021. https://doi.org/10.48550/arXiv.2105.08919
26. Suriyan K, Ramaingam N, Rajagopal S, Sakkarai J, Asokan B, Alagarsamy M. Performance analysis of peak signal-to-noise ratio and multipath source routing using different denoising method. Bull Electr Eng Inform. 2022; 11(1): 286-292. https://doi.org/10.11591/eei.v11i1.3332
27. Setiadi DRIM. PSNR vs SSIM: imperceptibility quality assessment for image steganography. Multimed Tools Appl. 2021; 80(6): 8423-8444. https://doi.org/10.1007/s11042-020-10035-z
28. Sim K, Yang J, Lu W, Gao X. MaD-DLS: mean and deviation of deep and local similarity for image quality assessment. IEEE Trans Multimed. 2020; 23: 4037-4048. https://doi.org/10.1109/TMM.2020.3037482
29. Zhang X, Zhang W, Sun W, Sun X, Jha SK. A Robust 3-D Medical Watermarking Based on Wavelet Transform for Data Protection. Comput Syst Sci Eng. 2022; 41(3): 1043-1056. https://doi.org/10.32604/csse.2022.022305
30. Peng Y, Shi C, Zhu Y, Gu M, Zhuang S. Terahertz spectroscopy in biomedical field: a review on signal-to-noise ratio improvement. PhotoniX. 2020; 1: 1-18. https://doi.org/10.1186/s43074-020-00011-z
31. Trigui I, Agbogla EK, Benjillali M, Ajib W, Zhu WP. Bit error rate analysis for reconfigurable intelligent surfaces with phase errors. IEEE Commun Lett. 2021; 25(7): 2176-2180. https://doi.org/10.1109/LCOMM.2021.3071433
32. Ohyama Y, Naganuma H, Ishida H, Hoshino T. Portal vein gas in a patient with acute cholangitis: Report of a case with emphasis on B-flow imaging. J Med Ultrasound. 2022; 49(1): 107-108. https://doi.org/10.1007/s10396-021-01167-2
33. Hofmann A G, Mlekusch I, Wickenhauser G, Assadian A, Taher F. Clinical Applications of B-Flow Ultrasound: A Scoping Review of the Literature. Diagnostics, 2023; 13(3): 397. https://doi.org/10.3390/diagnostics13030397
34. Nazari H, Bidgoli M M, Ghasvari H. Integration of lightweight cryptography and watermarking with compression for high speed and reliable communication of digital images in IoT. IET Image Proces. 2023; 17: 2984-3001. https://doi.org/10.1049/ipr2.12849
35. Wu Z, Zhang K, Ren Y, Li J, Sun J, Wan W. Visual Security Assessment via Saliency-Weighted Structure and Orientation Similarity for Selective Encrypted Images. Secur Commun Netw. 2021; 2021: 1-16. https://doi.org/10.1155/2021/6675354

36. Elkandoz M T, Alexan W, Hussein H H. Double-layer image security scheme with aggregated mathematical sequences. Int Conf Adv Commun Control Comput. Technol. (CommNet), Rabat, Morocco. 2019; 1-7. https://doi.org/10.1109/COMMNET.2019.8742370

نظام جديد لتخزين البيانات الطبية السرية باستخدام تقنية تشفيرChaskey و Blockchain

ايمن مظهر بد [1،2]**، لمياء الفراتي**[1]**، سميحة اياد**[3]

[1]مركز البحوث الرقمية بصفاقس(CRNS) ، مختبر الإشارات والأنظمة والذكاء الاصطناعي والشبكات(SM @ RTS) ، جامعة صفاقس، صفاقس، تونس.
[2]قسم العلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة ديالى، ديالى، العراق.
[3]معهد شارل ديلوناي-إيرا، جامعة التكنولوجيا في تروا، فرنسا.

الخلاصة

يعد التخزين الآمن للمعلومات الطبية السرية أمرًا بالغ الأهمية لمنظمات الرعاية الصحية التي تسعى إلى حماية خصوصية المريض والامتثال للمتطلبات التنظيمية. في هذا البحث، نقدم نظامًا جديدًا للتخزين الآمن للبيانات الطبية باستخدام تقنية تشفير Chaskey و blockchain. يستخدم النظام تشفير Chaskey لضمان سرية وسلامة البيانات الطبية، وتكنولوجيا blockchain لتوفير حلول تخزين البيانات الطبية بحيث يكون قابل للتطوير ويتميز باللامركزية. يستخدم النظام أيضًا تقنيات Bflow للتجزئة ومنها التجزئة الرأسية لتعزيز قابلية التوسع وإدارة البيانات المخزنة. بالإضافة إلى ذلك، يستخدم النظام العقود الذكية لفرض سياسات التحكم في الوصول والتدابير الأمنية الأخرى. سنقدم وصف للنظام المقترح بالتفصيل ونقدم تحليلاً لخصائصه الأمنية والأداء. تظهر نتائجنا أن النظام يوفر حلاً آمنًا للغاية وقابل للتطوير لتخزين البيانات الطبية السرية، مع تطبيقات محتملة في مجموعة واسعة من إعدادات الرعاية الصحية.

الكلمات المفتاحية: Blockchain ، BFlow، Chaskey ، الرعاية الصحية ، إنترنت الأشياء ، الأمن.