Journal of Harbin Engineering University Vol 44 No. 8
ISSN: 1006-7043 August 2023

Secure-Donation: A Blockchain-Based Secure and Privacy-Enhanced Healthcare Monetary Donation Management System

Walzade Arti Krushnarao and Dr. Pradnya Ashish Vikhar
Department of Computer Science and Engineering
Dr. A. P. J. Abdul Kalam University, Indore (M. P.) – 452010

Abstract:-Monetary donations play a crucial role in the healthcare industry by serving as financial contributions made by individuals, organizations, or institutions to support various healthcare initiatives such as funding medical research, enhancing patient care, expanding healthcare facilities, and assisting underprivileged individuals in accessing healthcare services. The primary objective of these donations is to advance the overall well-being and development of the healthcare sector, ultimately leading to improved healthcare delivery and patient outcomes. Managing monetary donations in the healthcare industry is a critical task, with traditional systems facing disadvantages such as a lack of transparency, security vulnerabilities, and privacy concerns. To address these challenges, this paper presents SECURE-DONATION, a blockchain-based healthcare monetary donation management system that ensures enhanced security and privacy. The system incorporates various advanced techniques, including multi-factor authentication, ECC-ChaCha20 cryptography, image watermarking, steganography, HmacBLAKE2 hash generation, and patient consent-based access control. These techniques collectively safeguard sensitive medical data and enhance the privacy of donor-recipient interactions. Experimental results validate the efficiency and effectiveness of SECURE-DONATION. Hash generation is performed quickly, taking only 23 milliseconds for 100 blocks. The ECC-ChaCha20 cryptography used in SECURE-DONATION outperforms other cryptography combinations, demonstrating encryption and decryption times of 0.005 seconds for 96-bit data. These results highlight the system's efficiency in securely sharing medical data and images. The experimental evaluation confirms that SECURE-DONATION is a reliable and robust solution for secure monetary donation management in healthcare environments.

Keywords: Blockchain, Two-Factor Authentication, ECC-ChaCha20 Cryptography, Image Watermarking, Steganography, HmacBLAKE2 Hash Generation, Patient's Consent

1. Introduction

In the healthcare industry, managing monetary donations plays a vital role in supporting patients' medical treatments and improving their overall well-being [1]. However, traditional systems employed for healthcare donation management often face significant challenges, including a lack of transparency, security vulnerabilities, and privacy concerns [2]. To address these shortcomings, this paper presents SECURE-DONATION, a blockchain-based secure and privacy-enhanced healthcare monetary donation management system.

Traditional donation management systems suffer from several disadvantages that hinder their effectiveness and compromise the donation process. Firstly, the lack of transparency in these systems creates uncertainty among donors and recipients regarding how their contributions are utilized and whether they directly impact the intended recipients [3]. This opacity hampers trust and reduces the willingness of potential donors to contribute.

Secondly, security vulnerabilities pose a considerable risk in traditional donation management systems [4]. Centralized databases and storage systems are susceptible to unauthorized access, data breaches, and manipulations, jeopardizing the confidentiality and integrity of sensitive donor and recipient information. Such security breaches can lead to identity theft, fraudulent activities, and the misuse of donated funds [5]. Thus, ensuring the security of the donation process is crucial to maintain the trust of donors and protect the interests of recipients.

Moreover, privacy concerns are prevalent in the context of healthcare donation management [6]. Donors and recipients are required to share personal and medical information, which may include sensitive details. Without robust privacy

measures, this information is at risk of unauthorized access, misuse, or even exploitation. Protecting the privacy of individuals involved in the donation process is essential to build trust and encourage active participation.

To tackle these disadvantages and provide a robust solution, the SECURE-DONATION system is introduced. Leveraging blockchain technology, SECURE-DONATION offers enhanced security and privacy, ensuring transparency and trustworthiness in healthcare monetary donation management.

SECURE-DONATION incorporates various advanced techniques to address the shortcomings of traditional systems. Two-factor authentication is implemented to strengthen the security of the system, requiring donors and recipients to authenticate their identities using multiple factors such as email, hash-based authentication, and fingerprint images. This multi-layered authentication process reduces the risk of unauthorized access and enhances the overall system security.

ECC-ChaCha20 cryptography is utilized to safeguard the confidentiality and integrity of sensitive data, such as medical records and images. This encryption technology ensures that only authorized individuals can access and decipher the information, mitigating the risk of data breaches and unauthorized tampering.

Furthermore, SECURE-DONATION employs image watermarking and steganography techniques to protect the privacy of medical records and images. Watermarking adds a unique identifier to patient images, ensuring their authenticity and preventing unauthorized alterations. Steganography hides sensitive information within the images using LSB substitution, further safeguarding the privacy and confidentiality of medical records.

To enhance the integrity of the system, SECURE-DONATION utilizes HmacBLAKE2 hash generation, which is faster and more secure than existing hash algorithms. This approach ensures the integrity of donation records and detects any tampering attempts, providing an additional layer of security.

Patient consent-based access control is a crucial aspect of SECURE-DONATION, empowering patients to control access to their healthcare data. Patients can specify who can access their information and under what conditions, ensuring their privacy preferences are respected and comply with relevant regulations.

The contributions of this paper can be summarized as follows:

- Development of SECURE-DONATION, a blockchain-based secure and privacy-enhanced healthcare monetary donation management system.
- Implementation of two-factor authentication, ECC-ChaCha20 cryptography, image watermarking, steganography, HmacBLAKE2 hash generation, and patient consent-based access control to address the limitations of traditional systems.
- Experimental evaluation showcasing the efficiency and effectiveness of SECURE-DONATION for secure medical data and image sharing.
- Demonstration of the reliability and robustness of SECURE-DONATION in managing monetary donations within healthcare environments.

This paper aims to present a comprehensive and reliable solution for secure and privacy-enhanced healthcare monetary donation management. The proposed system finds application in various areas, including hospitals, healthcare organizations, and medical research institutions, where the secure management of monetary donations is crucial.

The remainder of this paper is organized as follows. Section 2 provides an overview of related work in the field of healthcare donation management systems. Section 3 presents the design and architecture of SECURE-DONATION, detailing the various techniques employed. Section 4 describes the experimental setup and presents the results and analysis. Finally, Section 5 concludes the paper and outlines future research directions in this domain.

2. Related Works

Existing research in healthcare donation management systems has shed light on various limitations and challenges that necessitate careful consideration and innovative solutions. In this section, we will explore the disadvantages outlined in the literature and underscore the pressing need for a transformative approach to overcome these hurdles.

Muhammad et al. [7] introduced an enterprise resource planning (ERP)-based blood donation management system designed for hospitals and donors. While their system presented a promising avenue for improving the efficiency of blood donation processes, it exhibited potential drawbacks. Specifically, the lack of transparency and robust security measures within their system could engender privacy concerns and compromise the integrity of donor information. Without adequate safeguards, the confidentiality and trustworthiness of sensitive data may be at risk.

Chandler et al. [8] conducted a study during the COVID-19 pandemic to examine donors' motivations across European countries. Although their research offered valuable insights into the factors driving blood donation behavior, it primarily focused on motivational aspects rather than addressing the specific security vulnerabilities and privacy concerns inherent in traditional donation management systems. To ensure the confidentiality of donor information and mitigate potential risks, an innovative solution is required that tackles these security and privacy challenges head-on.

Jayawardena et al. [9] proposed a model aimed at assessing the risk of transfusion-transmitted syphilis and enhancing testing strategies. While their work contributed to the improvement of testing protocols, it may not have fully encompassed the broader challenges associated with transparency, security, and privacy in healthcare donation management systems. Robust security measures and privacy-enhancing mechanisms are crucial to instill confidence in the donation process and safeguard sensitive donor and patient data.

Lim et al. [10] explored the factors influencing patients' attitudes toward organ and tissue donation. Their study shed light on the psychological aspects shaping donation decisions. However, it may not have explicitly addressed the security vulnerabilities and privacy concerns prevailing in conventional donation management systems. Given the sensitive nature of healthcare monetary donations, an innovative solution is needed to protect donor privacy and secure the confidentiality of financial transactions.

Soni and Kumar [11] proposed a blockchain-based system for organ donation, highlighting the potential of this technology in enhancing transparency and trust in the organ donation process. While their work focused on the transparency aspect of organ donation, it may not have directly addressed the broader challenges related to managing healthcare monetary donations. Ensuring the secure and privacy-enhanced management of healthcare monetary donations necessitates an integrated approach that encompasses the specific requirements and complexities of financial transactions in the healthcare sector.

Hawashin et al. [12] proposed a blockchain-based management system for organ donation and transplantation, emphasizing transparency and traceability. While their solution holds promise for enhancing accountability and visibility in the organ donation domain, it may not have explicitly concentrated on the challenges associated with monetary donations in healthcare. Establishing a robust framework that specifically addresses the intricacies of managing healthcare monetary donations is imperative to ensure the integrity and confidentiality of financial transactions.

Kenang and Gosal [13] examined the factors influencing online donation intentions in donation-based crowdfunding platforms. Although their research focused on online platforms, it may not have comprehensively addressed the specific challenges and requirements unique to managing healthcare monetary donations. Healthcare donation management necessitates specialized security measures and privacy-enhancing mechanisms tailored to the healthcare industry's sensitive nature and regulatory frameworks.

Bin-Nashwan et al. [14] investigated fundraising campaigns and donors' attitudes during the COVID-19 outbreak, highlighting the importance of social solidarity. While their study provided insights into donor behavior and the impact of societal events on donation patterns, it may not have explicitly addressed the security vulnerabilities and privacy concerns associated with traditional healthcare donation management systems. Safeguarding donor information and financial transactions is crucial to ensure the trust and integrity of the donation process.

Shi et al. [15] reported on the first organ donation in Wuhan following the COVID-19 lockdown. Their study offered a unique perspective on organ donation in exceptional circumstances. However, it may not have thoroughly examined the broader challenges of transparency, security, and privacy in managing healthcare monetary donations. An innovative solution is required to address these challenges effectively and ensure the secure and privacy-enhanced management of monetary donations in the healthcare sector.

Hawashin et al. [16] proposed a blockchain-based management system for blood donation, aiming to enhance transparency and traceability. While their work primarily focused on the blood donation domain, it may not have explicitly concentrated on the challenges associated with monetary donations in healthcare. Addressing the specific requirements and complexities of managing healthcare monetary donations demands a comprehensive solution that encompasses not only transparency and traceability but also robust security measures and privacy-enhancing mechanisms.

Overall, the existing literature on healthcare donation management systems has identified several limitations, including issues related to transparency, security vulnerabilities, and privacy concerns. While various studies have made valuable contributions in specific areas such as blood donation, organ donation, and online donation platforms, they may not have holistically tackled the challenges associated with managing healthcare monetary donations. To overcome these disadvantages and ensure the secure and privacy-enhanced management of healthcare monetary donations, an innovative solution that integrates transparency, security, privacy, and tailored features for monetary transactions is needed.

3. Methodologies

Managing monetary donations in the healthcare industry is a critical task, with traditional systems facing disadvantages such as a lack of transparency, security vulnerabilities, and privacy concerns. To address these limitations and ensure a secure and privacy-enhanced healthcare monetary donation management system, this section proposes the SECURE-DONATION system. The SECURE-DONATION system is an innovative solution that addresses the limitations of traditional healthcare donation management systems. It provides a secure and privacy-enhanced platform for managing monetary donations in the healthcare industry. The system incorporates advanced technologies such as multi-factor authentication, cryptography, image watermarking, steganography, HmacBLAKE2 hash generation, and patient consent-based access control. These features ensure transparency, security, and trust in donation processes, while also protecting sensitive information and enabling real-time tracking of donations.

This section presents the methodology employed in the development of the SECURE-DONATION system. It describes the design and implementation of the system. The methodology encompasses the system architecture design, multi-factor authentication, cryptography, image watermarking, steganography, HmacBLAKE2 hash generation, and patient consent-based access control.

3.1 System Architecture of SECURE-DONATION system:

In the SECURE-DONATION system, the system architecture is designed to overcome the limitations and challenges of traditional healthcare donation management systems. The architecture consists of several components, including the Admin, Blockchain, Authentication Server, Certification Authority, Doctor, Nurse, Pharmacist, Patient (Recipient), and Donor. These components work together to ensure secure registration, authentication, encryption, and sharing of medical records.

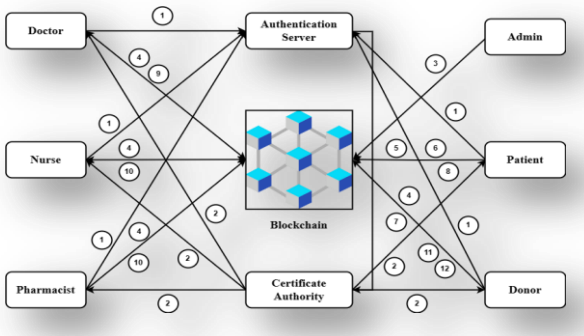

Figure 1: Architecture of the SECURE-DONATION system

The workflow of the SECURE-DONATION system is as follows:

1. **Registration:**The registration process with the Authentication Server involves doctors, nurses/pharmacists, patients (recipients), and donors providing necessary personal and professional information, including name, contact details, and credentials. The authentication server verifies this information to ensure the authenticity of the users.
2. **Digital Certificate:**After successful registration, a certification authority issues digital certificates to registered healthcare professionals, patients, and donors. These digital certificates serve as proof of identity and are used for encryption and decryption purposes within the system.
3. **Create and maintain blockchain:**An administrator is responsible for creating and maintaining a blockchain, which functions as a decentralized and distributed ledger. This secure platform records transactions and information across multiple nodes, ensuring the secure storage and management of encrypted professional information, donation requests, and medical data, including medical images.
4. **Encrypt and upload personal and professional information:** Doctors, nurses, and pharmacists can encrypt and upload their professional information, such as qualifications, certifications, and work history, onto the blockchain. Additionally, donors can encrypt and upload their personal information onto the blockchain. This information is securely stored within the blockchain and can only be accessed by authorized parties.
5. **Encrypt and upload medical data and images:** Patients can encrypt and upload their medical data, which typically includes their medical history, diagnoses, treatments, medical images, and other relevant health information, onto the blockchain. This encryption ensures the privacy and security of the medical data.
6. **Donation Requests:**Patients create specific donation requests outlining their medical needs, associated costs, and any supporting documentation. These requests are recorded on the blockchain, ensuring transparency, immutability, and traceability of the information.Donation requests are listed on the blockchain, making them visible to potential donors. Recipients can share their donation requests through blockchain to raise awareness and attract donors.
7. **Consent Request:**Donors interested in supporting a recipient browse through the list of donation requests available on the blockchain.But donors must send a consent request to see the patient's medical records to determine if they are indeed suffering from the disease.
8. **Consent preferences:** Patients have control over their medical data through the use of a digital certificate and an expiry date. They can specify their consent preferences regarding who can view and update their medical data. With their digital certificate, patients can provide explicit consent for specific healthcare providers, such as doctors, nurses, pharmacists, and donors to access their medical data within a specified timeframe.
9. **View and Update medical records:**Doctors registered in the system can view and update the medical data of their patients securely. This allows them to access and modify their patients' medical records to provide appropriate healthcare services.
10. **View medical records:**Nurses, pharmacists, and donors registered in the system can only view patient medical data and do not have the authority to make changes. This ensures that nurses, pharmacists, and donors have access to relevant patient information for quality care while maintaining the integrity of the medical data.
11. **Donation Processing:**After checking patient medical records with medical images, donors contribute Ether (ETH), a cryptocurrency, as the donation amount for a specific request. The blockchain platform facilitates the secure transfer of Ether from the donor's wallet to the recipient's wallet, ensuring transparency and eliminating intermediaries.
12. **Communication and Updates:**The donation management system enables communication between the recipient and donors. Recipients can provide updates on their medical

condition, and treatment progress, and express gratitude to the donors. Donors may also have the option to communicate with the recipient, ask questions, or offer words of support.Recipients can generate reports or statements showcasing the impact of the donations received and how the funds were utilized.

The key components and features of the SECURE-DONATION system are explained in the following subsections.

3.2 Multi-factor authentication:

Multi-Factor Authentication (MFA) is a crucial component of the SECURE-DONATION system, designed to enhance the security of user access. It incorporates multiple factors to verify the identity of individuals attempting to register or log into the system.

The multi-factor authentication mechanism employed by SECURE-DONATION consists of the following factors:

- **Email ID Verification:** During the registration and login process, users are required to verify their email ID. This verification step helps ensure that the provided email address is valid and belongs to the individual seeking access.
- **Hashed Value (HmacBLAKE2):** The authentication server generates a unique hashed value using the HmacBLAKE2 algorithm during the registration process. This hashed value serves as an additional factor for authentication and is associated with the user's account.
- **Fingerprint Image Verification:** Various user roles, including doctors, nurses/pharmacists, patients, and donors undergo fingerprint image verification. This process involves capturing and verifying the fingerprint image of individuals during registration and login. Only authorized individuals with valid fingerprints can gain access to the system.

By combining these multiple factors, SECURE-DONATION ensures that only authorized individuals can access the system and perform actions within their designated roles. The use of email ID verification, hashed values (HmacBLAKE2), and fingerprint image verification significantly enhance the security of user access, reducing the risk of unauthorized entry or data breaches.Algorithm 1 shows the working process of multi-factor authentication.

Algorithm 1: Multi-factor authentication

Input	**:**	User Email ID Hashed value (HmacBLAKE2) provided by the authentication server during registration Fingerprint image (for doctors, nurses/pharmacists, patients, and donors)
Output	**:**	Authentication status (whether the user is authorized or not)
Step 1	**:**	The user initiates the authentication process by providing their email ID, hashed value, and fingerprint image.
Step 2	**:**	The system verifies the provided email ID against the registered email ID to ensure its validity.
Step 3	**:**	The system retrieves the corresponding hashed value associated with the user's email ID during registration.
Step 4	**:**	The system compares the provided hashed value with the stored hashed value to authenticate the user's identity.
Step 5	**:**	If the hashed values match, the system proceeds to the fingerprint verification step.
Step 6	**:**	The system analyzes the provided fingerprint image and matches it with the stored fingerprint data associated with the user's role (doctor, nurse/pharmacist, patient, or donor).
Step 7	**:**	If the fingerprint image matches the stored fingerprint data, the system grants authentication and considers the user as authorized.
Step 8	**:**	If any of the authentication steps (email ID verification, hashed value verification, or fingerprint verification) fail, the system denies authentication and considers the user unauthorized.
Step 9	**:**	The system provides the authentication status as the output, indicating whether the user is authorized or not.

Step 10 : The user can proceed with accessing the SECURE-DONATION system if the authentication is successful, or they may be prompted to retry the authentication process if it fails.

The implementation of multi-factor authentication in SECURE-DONATION plays a vital role in establishing a robust and secure access control mechanism. By requiring users to provide multiple factors for authentication, the system significantly strengthens the security posture and mitigates the risk of unauthorized access.

One of the key advantages of multi-factor authentication is that it adds an extra layer of protection beyond the traditional username and password combination. In SECURE-DONATION, users not only need to provide their credentials but also undergo additional verification steps, including email ID verification and fingerprint image verification.

The email ID verification step ensures that the provided email address is valid and belongs to the user seeking access. This verification process helps prevent unauthorized individuals from registering or logging into the system using fabricated or invalid email addresses.

The utilization of a hashed value (HmacBLAKE2) as an authentication factor adds a layer of security. This hashed value, generated by the authentication server during registration, serves as a unique identifier associated with the user's account. It helps ensure that only individuals with the correct hashed value can proceed with the authentication process, further reducing the risk of unauthorized access.

The inclusion of fingerprint image verification is particularly significant in enhancing the security of SECURE-DONATION. By capturing and verifying the fingerprint image of users during registration and login, the system verifies the physical presence of authorized individuals. This biometric authentication factor adds an extra level of assurance that only legitimate users can gain access to the system.

Overall, the implementation of multi-factor authentication in SECURE-DONATION significantly enhances the overall security of the system. By combining multiple authentication factors, such as email ID verification, hashed values, and fingerprint image verification, the system establishes a stringent access control mechanism. This approach reduces the risk of unauthorized access, strengthens user authentication, and ensures that only authorized individuals can perform actions within their designated roles. Ultimately, the robust multi-factor authentication in SECURE-DONATION fosters trust, confidentiality, and data integrity within the system, safeguarding sensitive information and enhancing the overall security posture.

3.3 ECC-ChaCha20 Cryptography:

ECC-ChaCha20 cryptography refers to the combination of two cryptographic techniques: elliptic curve cryptography (ECC) and the ChaCha20 encryption algorithm. This hybrid approach is used to ensure the confidentiality and integrity of sensitive information in the SECURE-DONATION system.

Elliptic curve cryptography (ECC) is a public-key cryptography method that utilizes the mathematics of elliptic curves to provide secure encryption and digital signatures. It offers a higher level of security compared to traditional cryptographic algorithms while requiring smaller key sizes. In ECC, a pair of keys, consisting of a public key and a corresponding private key, is used to encrypt and decrypt data.

The ChaCha20 encryption algorithm is a symmetric encryption algorithm that is known for its speed and security. It operates on 256-bit key and nonce inputs to generate a stream of pseudorandom data, which is then used to encrypt and decrypt the plaintext. ChaCha20 is widely regarded as a secure and efficient encryption algorithm.

In the context of SECURE-DONATION, ECC-ChaCha20 cryptography is employed to protect various types of sensitive information, such as professional information of doctors, nurses/pharmacists, patient electronic health records (EHR), and patient images like ECG and MRI scan images. The ECC public key is used to encrypt the medical data, producing Ciphertext 1. Subsequently, the ChaCha20 secret key is used to encrypt Ciphertext 1, resulting in Ciphertext

When authorized users with appropriate access permissions need to access the encrypted data, they can download Ciphertext 2 and perform the

decryption process in reverse. First, the ChaCha20 decryption step decrypts Ciphertext 2, revealing Ciphertext 1. Then, the ECC decryption step decrypts Ciphertext 1 using the ECC private key, recovering the original medical data in its plaintext form.

Algorithm 2 shows the working process of the ECC-ChaCha20cryptography.

Algorithm 2: ECC-ChaCha20 Cryptography

Input : Medical data (plaintext)
ECC public key
ECC private key
ChaCha20 secret key

Output : Encrypted ciphertext (Ciphertext 2)
Decrypted plaintext (original medical data)

Step 1 : Generate ECC public and private keys along with the ChaCha20 secret key during the registration process. These keys are provided by a certification authority to ensure secure communication and data protection.

Step 2 : **Encryption:**
a. Encrypt the medical data (plaintext) using the ECC public key. This encryption step produces Ciphertext 1.
b. Encrypt Ciphertext 1 using the ChaCha20 secret key. This encryption step results in Ciphertext 2.

Step 3 : **Uploading to the blockchain:**
- Upload the encrypted Ciphertext 2 to the blockchain, ensuring its secure storage and immutability.

Step 4 : **User Download and Decryption:**
- An authorized user with access permission can download the encrypted Ciphertext 2 from the blockchain.

Step 5 : **Decryption:**
a. Decrypt Ciphertext 2 using the ChaCha20 secret key. This decryption step retrieves Ciphertext 1.
b. Decrypt Ciphertext 1 using the ECC private key. This decryption step yields the original medical data (plaintext).

Step 6 : **Accessing the decrypted data:**
- The authorized user can now access and utilize the decrypted medical data for the intended purposes.

By utilizing ECC-ChaCha20 cryptography, SECURE-DONATION ensures secure communication, data confidentiality, and integrity, protecting sensitive medical information from unauthorized access or tampering.

3.4 Image Watermarking:

Image watermarking is a technique used to embed information or a visual mark, called a watermark, into a digital image. The watermark can be used to indicate ownership, authenticity, or to protect against unauthorized use or tampering of the image. It serves as a form of digital signature that helps identify the source or author of the image.

Image watermarking typically involves modifying the pixel values or metadata of an image to embed the watermark. The process aims to make the watermark visually imperceptible while maintaining the quality and integrity of the original image. Various algorithms and techniques, such as LSB (Least Significant Bit) substitution, spread spectrum, and frequency domain methods, are used to embed the watermark into the image.

Watermarks can be visible or invisible. Visible watermarks are often overlaid on top of the image and can include text, logos, or patterns. They are easily detectable by visual inspection. Invisible watermarks, on the other hand, are embedded within the image data itself and are not immediately visible to the naked eye. They require specialized techniques or software to extract and verify their presence.

In the context of SECURE-DONATION, image watermarking is employed to protect sensitive medical images, such as ECG and MRI scan images. Patient images, such as photos, are used as watermarks to add an additional layer of authenticity and prevent unauthorized use or tampering. This helps ensure the integrity, ownership, and traceability of the medical images within the SECURE-DONATION system.

Algorithm 3 shows the working process of image watermarking.

Algorithm 3: Image Watermarking		
Input	:	Original medical image (Plaintext image) Patient image (Watermark image)
Output	:	Watermarked medical image
Step 1	:	Read the original medical image and the patient image.
Step 2	:	Resize the patient image to an appropriate size for watermarking.
Step 3	:	Apply a watermarking algorithm, such as the Least Significant Bit (LSB) substitution technique, to embed the patient image as a watermark into the original medical image.
Step 4	:	Determine the embedding location within the original medical image where the watermark will be inserted.
Step 5	:	For each pixel in the patient image and the corresponding pixel in the original medical image, extract the least significant bit (LSB) from the original medical image pixel and replace it with the corresponding bit from the patient image pixel.
Step 6	:	Repeat the process for all pixels in the patient image, embedding the watermark into the original medical image.
Step 7	:	Save the watermarked image as the output.
Step 8	:	The resulting image is the watermarked medical image that contains the patient image as a watermark.
Step 9	:	The watermarked image can be used for verification, authentication, and ownership purposes within the SECURE-DONATION system, ensuring the integrity and authenticity of the medical images.

In SECURE-DONATION, the implementation of image watermarking plays a crucial role in safeguarding sensitive medical images. By embedding unique watermarks into these images, their integrity and authenticity are ensured. This prevents unauthorized use, tampering, or misrepresentation of medical images. Moreover, the watermarking technique enhances traceability within the system, allowing for easy identification of the source and ownership of the images. This provides an added layer of protection for sensitive medical data, instilling confidence in both patients and healthcare providers regarding the privacy and security of their information.

3.5 Steganography:

In the SECURE-DONATION system, steganography is a technique employed to enhance the privacy and security of sensitive medical records, specifically the concealment of medical image descriptions. Steganography allows for the hiding of confidential information within cover images in a way that is imperceptible to the human eye.

The process begins by encrypting the "secret data" (which can include sensitive medical information or image descriptions) using ECC (Elliptic Curve Cryptography) public key encryption. This encryption ensures the confidentiality of the data.

Next, the encrypted data, referred to as the "ciphertext," is embedded within the cover image using the LSB substitution steganography technique. LSB substitution involves replacing the least significant bits of the cover image pixels with the bits from the ciphertext, effectively hiding the encrypted data within the image.

Once the stego image is constructed, it undergoes an additional layer of encryption. The ChaCha20 secret key encryption algorithm is used to encrypt the stego image, resulting in a new ciphertext referred to as "ciphertext 2." This encryption adds another level of security to the concealed data.

The ciphertext 2, which represents the encrypted stego image, is then uploaded to the blockchain. This ensures the traceability and integrity of the concealed data, as the blockchain provides a transparent and tamper-proof record of the uploaded information.

Authorized and access-permitted users within the SECURE-DONATION system can then download and decrypt the original image. By utilizing the appropriate decryption keys and algorithms, they can extract the hidden information from the stego image and access the original medical data or image descriptions.

Algorithm 4 shows the working process of steganography.

Algorithm 4: Steganography

Input	:	Cover image (image file containing hidden information) Secret data (sensitive medical information or image description) ECC public key (for encryption), ECC private key (for decryption) ChaCha20 secret key (for both encryption and decryption)
Output	:	Stego image (the cover image with the hidden data embedded) Ciphertext 2 (encrypted stego image) Decrypted image (original image after decryption)
Step 1	:	Encrypt the secret data using the ECC public key to obtain the ciphertext 1.
Step 2	:	Load the cover image into memory.
Step 3	:	Iterate over each pixel in the cover image.
Step 4	:	For each pixel, extract the RGB values.
Step 5	:	Modify the least significant bit (LSB) of each color channel (R, G, B) to store a bit of the ciphertext 1.
Step 6	:	Repeat this process for all bits of ciphertext 1, distributing them across multiple pixels.
Step 7	:	After embedding the ciphertext 1, save the modified image as the stego image.
Step 8	:	Encrypt the stego image using the ChaCha20 secret key to obtain ciphertext 2.
Step 9	:	Upload the ciphertext 2 (encrypted stego image) to the blockchain for secure storage.
Step 10	:	Authorized users can download ciphertext 2 from the blockchain.
Step 11	:	Decrypt the ciphertext 2 using the ChaCha20 secret key to obtain the stego image.
Step 12	:	Extract the hidden ciphertext 1 from the stego image by reversing the LSB substitution process.
Step 13	:	Decrypt the extracted ciphertext 1 using the ECC private key to obtain the original secret data.
Step 14	:	Retrieve the original image if necessary.

Through the application of steganography techniques, SECURE-DONATION ensures an additional layer of protection for sensitive medical records. It safeguards the confidentiality, integrity, and ownership of the concealed data, allowing only authorized individuals to access and interpret the hidden information.

3.6 HmacBLAKE2 Hash Generation:

HmacBLAKE2 Hash Generation is a cryptographic algorithm employed in the SECURE-DONATION system to ensure secure verification, data integrity checks, and authentication processes. It offers faster hash generation with stronger security compared to other existing algorithms like HMAC-SHA3, HMAC-SHA256, and HMAC-SHA1.

In the SECURE-DONATION system, HmacBLAKE2 is used to generate hash values for various purposes, such as verifying the integrity of data, validating authenticity, and ensuring secure communication between different components of the system. The algorithm takes a plaintext message and a secret key as inputs and produces an HMAC (Hash-based Message Authentication Code) value as the output.

Algorithm 5 shows a detailed explanation of the HmacBLAKE2 Hash Generation algorithm within the SECURE-DONATION system.

Algorithm 5: HmacBLAKE2 Hash Generation

Input	:	Plaintext: The plaintext message. Key: The secret key used for HMAC.
Output	:	hmac: The HmacBLAKE2 hash value.
Step 1	:	If the length of the key is greater than the block size of the HmacBLAKE2 hash function, compute the hash of the key: key = BLAKE2(key).
Step 2	:	If the length of the key is less than the block size, pad it with zeros to match the block size.
Step 3	:	Create two variables, inner_key and outer_key, by XORing the key with specific constants: • inner_key = key XOR 0x3636...36 (the constant is

repeated to match the block size).
- outer_key = key XOR 0x5C5C...5C (the constant is repeated to match the block size).

Step 4 : Concatenate inner_key with the plaintext to form the inner message: inner_msg = inner_key || plaintext.

Step 5 : Compute the hash of the inner message using the HmacBLAKE2 hash function: inner_hash = BLAKE2(inner_msg).

Step 6 : Concatenate outer_key with the inner_hash to form the outer message: outer_msg = outer_key || inner_hash.

Step 7 : Compute the final HmacBLAKE2 hash by computing the hash of the outer message: hmac = BLAKE2(outer_msg).

Step 8 : Return the hmac as the output.

The HmacBLAKE2 Hash Generation algorithm ensures the integrity and authenticity of data within the SECURE-DONATION system. It is used for verifying the integrity of sensitive information, validating the authenticity of messages, and enabling secure communication between different entities involved in the system. By employing HmacBLAKE2, the system enhances the overall security and trustworthiness of the data and interactions within the SECURE-DONATION system.

3.7 Patient's Consent-Based Access Control:

To ensure that patient privacy preferences and consent are respected, SECURE-DONATION incorporates a Patient's Consent-Based Access Control algorithm. This algorithm takes inputs such as the patient's digital certificate containing consent preferences and access permissions, along with the credentials of doctors, nurses, pharmacists, and donors for authentication. Based on the consent preferences and access permissions specified in the digital certificate, authorized access to view and/or update patient medical data and images is granted. The algorithm continuously monitors access and updates to ensure compliance with the patient's consent preferences.

Algorithm 6 shows the working process of the Patient's Consent-Based Access Control.

Algorithm 6: Patient's Consent-Based Access Control

Input : Patient's digital certificate containing consent preferences and access permissions with an expiry date.
Doctor, nurse, pharmacist, and donor credentials for authentication.
Patient medical data and images.

Output : Authorized access to view and/or update patient medical data and images based on consent preferences and access permissions.

Step 1 : **Specify Consent Preferences:**
- The patient uses their digital certificate to specify consent preferences, indicating who can view and update their medical data and images. The digital certificate also includes an expiry date.

Step 2 : **Authenticate User Credentials:**
- Authenticate the credentials of doctors, nurses, pharmacists, and donors to ensure their registration and appropriate access permissions.

Step 3 : **Verify Digital Certificate:**
- Verify the validity and compatibility of the patient's digital certificate with their consent preferences. Check if the certificate is active and has not expired.

Step 4 : **Grant Access to Doctors:**
- If the doctor's credentials are authenticated and the digital certificate grants access permissions, allow the doctor to view and update the patient's medical data and images until the expiry date.

Step 5 : **Grant Access to Nurses:**
- If the nurse's credentials are authenticated and the digital certificate grants access permissions, permit the nurse to view the patient's medical data and images without updating them until

the expiry date.

Step 6 : Grant Access to Pharmacists:

- If the pharmacist's credentials are authenticated and the digital certificate grants access permissions, enable the pharmacist to view the patient's medical data and images without updating them until the expiry date.

Step 7 : Grant Access to Donors:

- If the donor's credentials are authenticated and the digital certificate grants access permissions, enable the donor to view the patient's medical data and images without updating them until the expiry date.

Step 8 : Deny Unauthorized Access:

- Deny access to patient medical data and images if the user credentials are not authenticated or if the digital certificate does not indicate access permissions.

Step 9 : Log Changes:

- Log any attempted changes to the patient's medical data and images for auditing purposes.

Step 10 : Monitor Access and Updates:

- Continuously monitor access and updates to ensure compliance with consent preferences and access permissions.

Step 11 : Terminate Algorithm:

- Terminate the algorithm when authorized users complete their tasks or log out of the system.

Overall, the Patient Consent-Based Access Control algorithm in SECURE-DONATION provides a systematic approach to managing access to patient medical data and images. It considers the patient's consent preferences, the credentials of authorized personnel, and the validity of digital certificates to determine the appropriate level of access. This ensures that patient privacy is respected, access is granted based on consent, and unauthorized access attempts are prevented.

Overall, the SECURE-DONATION system addresses the disadvantages of traditional healthcare donation management systems by incorporating multi-factor authentication, ECC-ChaCha20 cryptography, image watermarking, steganography, HmacBLAKE2 hash generation, and a patient's consent-based access control algorithm. These features collectively ensure the security, privacy, integrity, and transparency of healthcare monetary donations, providing a comprehensive and innovative solution for efficient donation management in the healthcare industry.

4. Experimental Results and Discussions

The efficiency of the SECURE-DONATION system was thoroughly evaluated in this section, employing a Java-based blockchain for experimenting. The experiment incorporated a diverse range of elements within a data string, including Ethereum-style smart contracts. The primary focus of the evaluation was on two key criteria: the time taken for hash generation and the time taken for encryption and decryption processes.

To quantify the time difference between pre and post-hash generation in the blockchain network, a metric called Hash Generation Time (HGT) was defined. HGT, expressed in milliseconds, is calculated as the difference between the current time (in milliseconds) before and after the hash generation processin Eq. (1):

$$HGT = AH - BH \quad (1)$$

Here, BH denotes the initial time before hash generation, while AH represents the subsequent time after hash generation.

A comparative analysis of hash generation time was conducted across various algorithms implemented in the blockchain network. The algorithms under consideration included the Algorithm by Shynu et al. [17], the Algorithm by Abunadi et al. for BSF-EHR [18], the Algorithm by Abunadi et al. for BBPM [19], and the SECURE-DONATION system. The results of this analysis are presented in Table 1, shedding light on the performance differences among these algorithms in terms of hash generation time.

Table 1: Hash generation time comparison

Number of Blocks	Shynu et al. [17]	Abunadi et al. [18]	BBPM [19]	SECURE-DONATION
10	22	20	16	3
25	38	36	32	13
50	60	42	37	14
75	90	78	71	22
100	130	118	110	23
Average	68	58.8	53.2	15

The analysis presented in Table 1 reveals that the SECURE-DONATION system consistently outperforms the other algorithms in terms of hash generation time across different block sizes. This signifies that the SECURE-DONATION system excels in generating hashes efficiently, leading to quicker processing and enhanced computational performance. Efficient hash generation time holds significant importance in blockchain applications as it directly impacts the overall system performance and responsiveness. With its shorter hash generation times, the SECURE-DONATION system enables faster transaction processing and boosts the overall efficiency of the system.

Considering the findings presented in Table 1, it can be concluded that the SECURE-DONATION system stands out as the optimal choice among the compared algorithms. Its consistent achievement of shorter hash generation times showcases superior efficiency and accelerated processing capabilities. By selecting the SECURE-DONATION system, organizations can benefit from improved performance and streamlined operations. For a visual representation of the hash generation time comparison, refer to Figure 2, which presents a pictorial diagram illustrating the performance differences among the algorithms.

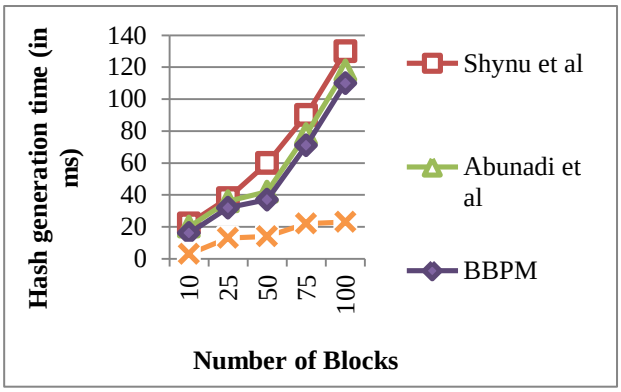

Figure 5: Hash generation time comparison

Moreover, Table 2 compares the times required for encryption and decryption using two-hybrid cryptography combinations, AES - RSA and RSA - ECC, as documented in reference [20], with the proposed hybrid cryptography technique (ECC-ChaCha20).

Table 2: Comparison of Encryption and Decryption Times (in seconds) for the ECC-ChaCha20 Cryptography Technique and Two Existing Hybrid Cryptography Combinations

Data size (bits)	AES - RSA	RSA - ECC	ECC-ChaCha20 Cryptography
48	10.2493	8.3266	0.004
64	14.7360	14.8445	0.005
80	21.8297	17.1274	0.003
96	34.0297	21.6842	0.005

Analyzing the data presented in Table 2, it becomes apparent that the ECC-ChaCha20 Cryptography technique surpasses both AES-RSA and RSA-ECC in terms of encryption and decryption times across various data sizes. This demonstrates the superior performance and efficiency of the ECC-ChaCha20 Cryptography technique in securing sensitive information.

For instance, at a data size of 48 bits, the ECC-ChaCha20 Cryptography technique achieves encryption and decryption in just 0.004 seconds, while AES-RSA and RSA-ECC require significantly more time, taking 10.2493 and 8.3266 seconds, respectively. Similarly, at larger data sizes such as 96 bits, the ECC-ChaCha20 Cryptography technique exhibits impressive encryption and decryption times of only 0.005 seconds,

outperforming AES-RSA (34.0297 seconds) and RSA-ECC (21.6842 seconds) by a substantial margin.

Based on these compelling results, it is evident that the ECC-ChaCha20 Cryptography technique offers unparalleled speed and efficiency in encryption and decryption operations when compared to the alternative combinations. Its ability to optimize cryptographic processes makes it the ideal choice among the options presented in Table 2. To visually illustrate the comparison of these techniques in terms of encryption and decryption time, refer to Figure 3.

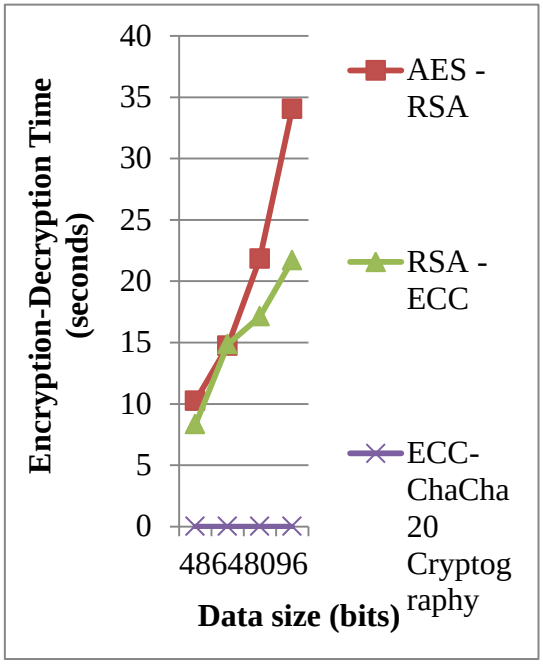

Figure 3: Data Size vs. Encryption-Decryption Time Comparison: ECC-ChaCha20 Cryptography vs. Two Existing Hybrid Cryptography Combinations

In the realm of secure data management, the SECURE-DONATION system has established its prominence by exhibiting faster hash generation times compared to alternative algorithms. This achievement can be attributed to the utilization of the HmacBLAKE2 hash-generating technique. By employing HmacBLAKE2, the SECURE-DONATION system effectively generates hashes in a timely and efficient manner, leading to enhanced overall performance and reduced processing durations.

Moreover, the ECC-ChaCha20 Cryptography technique employed within the system showcases efficient encryption and decryption times across various data sizes. This technique integrates different encryption algorithms and strategies to optimize performance. Through meticulous selection and combination of these encryption components, the ECC-ChaCha20 technique maximizes efficiency and minimizes computational overhead. As a result, encryption and decryption operations can be swiftly executed while consuming minimal computational resources.

The efficiency of the ECC-ChaCha20 Cryptography technique is particularly notable when considering different data sizes. Table 2 presents compelling evidence of the technique's consistent outperformance compared to other combinations like AES-RSA and RSA-ECC in terms of encryption and decryption times. Regardless of the data size at hand, the ECC-ChaCha20 Cryptography technique consistently delivers faster processing times, highlighting its effectiveness and superiority in real-world applications. This efficiency translates to improved data security and faster cryptographic operations within the SECURE-DONATION system, reinforcing its capabilities in safeguarding sensitive information.

5. Conclusions

The paper introduced SECURE-DONATION, a blockchain-based secure and privacy-enhanced healthcare monetary donation management system. The system addresses the challenges faced by traditional donation management systems, including lack of transparency, security vulnerabilities, and privacy concerns. By incorporating advanced techniques such as multi-factor authentication, ECC-ChaCha20 cryptography, image watermarking, steganography, HmacBLAKE2 hash generation, and patient's consent-based access control, SECURE-DONATION ensures the security and privacy of sensitive medical data and donor-recipient interactions. The experimental results demonstrated the efficiency and effectiveness of SECURE-DONATION. The hash generation process was performed quickly, taking only 23 milliseconds for 100 blocks, indicating the system's ability to process transactions rapidly. The ECC-ChaCha20 cryptography employed in SECURE-DONATION outperformed other cryptography combinations,

exhibiting encryption and decryption times of 0.005 seconds for 96-bit data. These results validate the system's efficiency in securely sharing medical data and images, contributing to improved privacy and confidentiality.

While SECURE-DONATION focuses on healthcare monetary donation management, its underlying principles and techniques can be extended to other domains beyond healthcare. Future work can explore the applicability of SECURE-DONATION in areas such as financial transactions, supply chain management, intellectual property protection, and document verification. By adapting and customizing the system to different industries, the security, privacy, and transparency in various sectors can be enhanced. Furthermore, ongoing research can focus on optimizing the system's performance and scalability. Investigating techniques to improve hash generation speed, exploring more efficient encryption algorithms, and enhancing the overall system architecture can contribute to faster transaction processing and accommodate larger-scale deployments. Additionally, incorporating machine learning and artificial intelligence techniques to identify patterns and detect anomalies in donation transactions can further enhance the system's security and fraud detection capabilities. Overall, SECURE-DONATION serves as a solid foundation for secure and privacy-enhanced donation management, and future work can extend its benefits to diverse industries and explore avenues for continual improvement and innovation.

References

[1] Bassani, G., Marinelli, N., &Vismara, S. (2019). Crowdfunding in healthcare. The Journal of Technology Transfer, 44, 1290-1310.

[2] Wu, H., & Zhu, X. (2020). Developing a reliable service system of charity donation during the covid-19 outbreak. Ieee Access, 8, 154848-154860.

[3] Moreno-Albarracín, A. L., Licerán-Gutierrez, A., Ortega-Rodríguez, C., Labella, Á.,& Rodríguez, R. M. (2020). Measuring what is not seen—Transparency and good governance nonprofit indicators to overcome the limitations of accounting models. Sustainability, 12(18), 7275.

[4] Muliawati, T., &Masya, F. (2019). Fundraising and donation application system. International Research Journal of Computer Science, 6(06), 639-653.

[5] Maulana, M. I., Kurniati, G., &Apriani, R. (2022). Legal Liability By Organs of Social and Humanitarian Foundations Against Misuse of Foundation Funds. WidyaYuridika: JurnalHukum, 6(1), 51-60.

[6] Harbinja, E. (2019). Posthumous medical data donation: the case for a legal framework. The ethics of medical data donation, 97-113.

[7] Muhammad, G., Asif, H., Abbas, F., Memon, I., &Fazal, H. (2020). An ERP-Based Blood Donation Management System for Hospitals and Donors. Sukkur IBA Journal of Emerging Technologies, 3(1), 44-54.

[8] Chandler, T., Neumann-Böhme, S., Sabat, I., Barros, P. P., Brouwer, W., van Exel, J.& Stargardt, T. (2021). Blood donation in times of crisis: early insight into the impact of COVID-19 on blood donors and their motivation to donate across European countries. VoxSanguinis, 116(10), 1031-1041.

[9] Jayawardena, T., Hoad, V., Styles, C., Seed, C., Bentley, P., Clifford, V., ...&Gastrell, T. (2019). Modeling the risk of transfusion-transmitted syphilis: a reconsideration of blood donation testing strategies. VoxSanguinis, 114(2), 107-116.

[10] Lim, K. J., Cheng, T. T. J., Jeffree, M. S., Hayati, F., Cheah, P. K., Nee, K. O., .&Tha, N. O. (2020, April). Factors influencing attitude toward organ and tissue donation among patients in primary clinic, Sabah, Malaysia. In Transplantation proceedings (Vol. 52, No. 3, pp. 680-686). Elsevier.

[11] Soni, A., & Kumar, S. G. (2021). Creating an organ donation system with blockchain technology. European Journal of Molecular and Clinical Medicine, 8(03).

[12] [Hawashin, D., Jayaraman, R., Salah, K., Yaqoob, I., Simsekler, M. C. E., &Ellahham, S. (2022). Blockchain-Based Management

for Organ Donation and Transplantation. IEEE Access, 10, 59013-59025.

[13] Kenang, I. H., &Gosal, G. (2021). Factors affecting online donation intention in donation-based crowdfunding. The Winners, 22(2), 97-104.

[14] Bin-Nashwan, S. A., Al-Daihani, M., Abdul-Jabbar, H., & Al-Ttaffi, L. H. A. (2022). Social solidarity amid the COVID-19 outbreak: fundraising campaigns and donors' attitudes. International Journal of Sociology and Social Policy, 42(3/4), 232-247.

[15] Shi, H., Xu, J., Li, X., Zhao, Y., Wei, L., Jiang, J., & Chen, Z. (2020). First organ donation in Wuhan after ending of the coronavirus lockdown. Transplant International, 33(9), 1149-1150.

[16] Hawashin, D., Mahboobeh, D. A. J., Salah, K., Jayaraman, R., Yaqoob, I., Debe, M., &Ellahham, S. (2021). Blockchain-based management of blood donation. IEEE Access, 9, 163016-163032.

[17] P. G. Shynu, V. G. Menon, R. L. Kumar, S. Kadry, and Y. Nam, "Blockchain-based secure healthcare application for diabetic-cardio disease prediction in fog computing," IEEE Access, vol. 9, pp. 45706–45720, 2021.

[18] I. Abunadi and R. L. Kumar, "BSF-EHR: blockchain security framework for electronic health records of patients," Sensors, vol. 21, no. 8, Article ID 2865, 2021.

[19] Abunadi, I., & Kumar, R. L. (2021). Blockchain and business process management in health care, especially for covid-19 cases. Security and Communication Networks, 2021.

[20] Subedar, Z., &Araballi, A. (2020). Hybrid cryptography: Performance analysis of various cryptographic combinations for secure communication. International Journal of Mathematical Sciences and Computing (IJMSC), 6(4), 35-41.