WJAETS

World Journal of Advanced Engineering Technology and Sciences

eISSN: 2582-8266

Cross Ref DOI: 10.30574/wjaets

Journal homepage: https://wjaets.com/

(Research Article)

Check for updates

MedSecure: Blockchain-enhanced patient data security with asymmetric cryptography and MFA

LEANDRA SHANIA ANDERSON * and USHA J

Department of Master of Computer Applications, RV College of Engineering, Bengaluru, Karnataka, India.

World Journal of Advanced Engineering Technology and Sciences, 2024, 13(02), 718-727

Publication history: Received on 25 July 2024; revised on 16 December 2024; accepted on 18 December 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.13.2.0386

Abstract

In the rapidly evolving digital landscape, safeguarding sensitive patient information is crucial for healthcare systems. Traditional data management systems encounter significant security vulnerabilities, lack of decentralisation, and limited user access. This paper introduces a secure and decentralized patient data management system utilising a custom blockchain framework combined with asymmetric cryptography. The system employs Python for algorithm development, OpenSSL for RSA encryption, and a custom PHP-based blockchain to create a secure, decentralised platform. Patient data is encrypted with public keys, ensuring that only authorized healthcare providers can access it using corresponding private keys and access tokens. Multi-factor authentication (MFA) via SMS further enhances security by controlling access to these keys. The system's key modules—key management, data encryption, blockchain storage, and a centralized ID resolver—ensure robust security, data integrity, and controlled accessibility of patient data. Blockchain integration maintains a secure, tamper-proof ledger of all data transactions, improving privacy, data integrity, and healthcare delivery by ensuring secure and authorized access to patient information.

Keywords: Blockchain; Asymmetric cryptography; RSA encryption; Patient data management; Patient privacy; Multi-factor authentication (MFA); Decentralized storage; Data security

1. Introduction

The management and security of patient data are of paramount importance in the healthcare industry. With the increasing digitization of healthcare records and the proliferation of connected devices, ensuring the privacy and integrity of patient information has become a critical challenge. Traditional systems for managing patient data are often centralized, creating single points of failure that can lead to data breaches, unauthorized access, and other security vulnerabilities. Additionally, there is a lack of clarity in how data is accessed and used. The evolving landscape of healthcare information systems necessitates a robust approach to protecting the confidentiality and integrity of patient data while ensuring its availability to authorized providers [1].

Blockchain technology has emerged as a promising solution to address these challenges by providing a decentralized and secure framework for data management. By distributing data across a network of nodes, blockchain eliminates the need for a central authority, thereby reducing the risks associated with data centralization. Furthermore, the immutability of blockchain ensures that once data is recorded, it cannot be altered or tampered with, thereby maintaining the integrity and trustworthiness of patient records [2].

This paper introduces an approach to patient data management by integrating blockchain technology with asymmetric cryptography and offers a promising solution to enhance the privacy and security of electronic health records, addressing challenges such as data integrity and access control [3]. The proposed system uses a custom blockchain

* Corresponding author: LEANDRA SHANIA ANDERSON.

solution developed with PHP, alongside RSA encryption facilitated by OpenSSL, to create a secure and decentralized platform for managing patient data. The system allows patients to generate their encryption keys leveraging patient-controlled encryption and role-based access mechanisms, the system enhances the security and confidentiality of health records, addressing key challenges in managing sensitive medical data [4]. Multi-factor authentication (MFA) using SMS is employed to further secure access to these encryption keys, preventing unauthorized users from decrypting patient data.

The primary contributions of this work include the development of key management, data encryption, blockchain storage, and centralized ID resolver modules, all designed to ensure robust security and accessibility. By leveraging the inherent advantages of blockchain and asymmetric cryptography, the proposed system not only protects patient privacy but also fosters trust and clarity in the handling of sensitive medical information. To contextualize these innovations, the subsequent literature review will explore relevant studies and theoretical perspectives that highlight existing solutions and identify gaps in current technologies. This review aims to establish a comprehensive understanding of the state-of-the-art practices in healthcare data management, setting the stage for assessing the potential impact and advancements introduced by this research.

2. Literature review

Secure management of healthcare data is crucial due to the sensitive nature of patient information and the growing frequency of data breaches. Traditional systems, often centralized, face significant security and privacy issues[5]. These centralized systems are vulnerable to cyberattacks that can compromise entire datasets, underscoring the need for stronger security measures [5].

Asymmetric cryptography offers a key advancement by using a pair of keys—a public key for encryption and a private key for decryption—to enhance data security. It ensures that only the intended recipient can access the encrypted data [6]. However, if the private key is compromised, it can still lead to unauthorized access, highlighting the need for additional security measures alongside asymmetric cryptography.

Blockchain technology [7] presents a promising solution to the limitations of centralized healthcare systems. By decentralizing data storage across a network, blockchain improves data integrity and integrity through cryptographic verification, reducing the risk of single points of failure and ensuring data immutability [8]. Despite its potential, blockchain faces challenges in scalability and efficiency [9].

Blockchain’s ability to provide immutable and clear record-keeping makes it an attractive option for healthcare data management. Its decentralized nature ensures that data cannot be altered without detection and promotes greater clarity. However, integrating blockchain into healthcare systems requires addressing performance and regulatory issues.

Blockchain solutions for cryptocurrencies, such as Bitcoin, differ from those needed for healthcare data management. While cryptocurrency blockchains handle high transaction volumes [10], healthcare data management requires a different approach due to lower transaction throughput. Custom blockchain solutions tailored for healthcare can be more effective.

This research proposes a custom blockchain for secure patient data management, integrating asymmetric cryptography with blockchain technology. The system will use RSA encryption for data protection, blockchain for immutable storage, and multi-factor authentication for access control, aiming to enhance security while ensuring efficient and secure data management.

Hence, combining asymmetric cryptography with blockchain technology addresses key challenges in traditional healthcare systems, enhancing data security and integrity. The following section will outline the methodology used to implement and evaluate these technologies in the context of healthcare data management.

3. Methodology

This section outlines the methodology employed to develop a secure, decentralized, and clear system for managing patient data using blockchain technology and asymmetric cryptography. The methodology addresses key challenges in traditional healthcare data management, such as security, privacy and user autonomy.

3.1. Procedure

Firstly, the system initiates the process by generating a private-public key pair using RSA encryption. This key pair is crucial for implementing end-to-end encryption, which ensures the confidentiality of patient data both during transmission and while stored on external servers. The RSA algorithm is employed to create robust encryption keys, which are essential for securing sensitive information [11].

Secondly, the proposed system employs a custom PHP-based blockchain to store encrypted patient data. Unlike traditional cryptocurrency blockchains that involve mining, this blockchain does not require computationally intensive processes. Instead, it operates on a consensus mechanism where data entries are subjected to a verification filter. This filter checks for authorized users and valid medical data before recording them in the blockchain, ensuring data integrity and preventing unauthorized modifications.

In addition to these steps, the authentication and authorization processes are managed through secure mechanisms. User credentials are verified by hashing passwords with bcrypt [12] and comparing them against stored hashes in the database. Upon successful authentication, a JSON Web Token (JWT) is generated and signed with a server-side RSA key. This token is used for session management and is essential for the subsequent authorization phase, where access tokens are issued based on user roles and permissions.

The key management module is responsible for generating, storing, and retrieving RSA keys. RSA key pairs are created using SHA-256 and stored securely in the database and Laravel storage. This module ensures that keys are available for encryption and decryption operations, maintaining the security of patient data.

Patient data management involves secure handling and updating of patient records. Access is authenticated through bearer tokens [13], and updates are made to the patient records in the database. The system ensures data integrity by implementing validation checks and managing transactions to reflect accurate information.

Medical document management facilitates the upload and retrieval of documents securely. Documents are uploaded to Amazon Web Services, Simple Storage, and their URLs are encrypted using the patient's RSA public key. These encrypted URLs are then recorded on the blockchain ledger [14], ensuring immutability and traceability. Patients can decrypt their documents using their RSA private key, while authorized staff can access documents through expiring access tokens.

The blockchain integration process commits encrypted medical document URLs to the blockchain, maintaining data immutability and integrity. Cryptographic verification is performed to ensure the authenticity of blockchain-stored data, confirming that transactions are accurately recorded.

A centralized ID resolver maps public keys to patient identities and retrieves patient information based on the provided keys or user IDs. This mechanism supports secure and efficient identity verification.

Utilities support additional functionalities such as SMS-based multi-factor authentication (MFA). The system uses Twilio to send SMS messages for MFA, enhancing the security of user authentication. Successful delivery of SMS messages is confirmed, and any errors are reported.

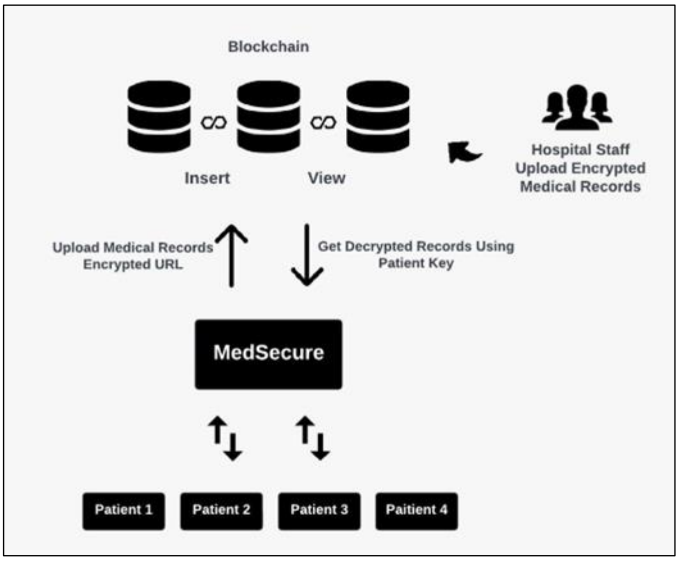

Figure 1 outlines the workflow of the proposed system, showcasing the process of securing and retrieving patient data

In this workflow, hospital staff encrypt patient medical records and upload them to the platform, which generates an encrypted URL that is stored on a custom blockchain. The blockchain component ensures that data is securely inserted and viewed in a decentralized, tamper-proof manner. Patients or authorized healthcare providers can retrieve the decrypted medical records using a private key, with the system serving as the intermediary that facilitates this secure exchange. The diagram highlights the seamless integration between blockchain technology and encrypted data management, ensuring that patient records are both secure and accessible only to authorized entities.

3.2. Architecture

The architecture of the proposed system is designed to ensure secure and decentralized management of patient data. It consists of the following key components:

- **Blockchain Layer:** A custom blockchain framework was developed using PHP, designed to store encrypted patient data securely. Each transaction within the blockchain represents a unique data entry or access request, ensuring data integrity and immutability.
- **Encryption Layer:** The encryption layer utilizes RSA algorithms for asymmetric cryptography. Patient data is encrypted using public keys generated by the patients, ensuring that only authorized users with the corresponding private keys can decrypt and access the information.
- **Key Management:** This module handles the secure generation, storage, and management of RSA keys. Public keys are stored in a central database, while private keys are kept securely in the Laravel storage system. MFA is integrated within this module to control access to private keys.
- **Centralized ID Resolver:** A centralized ID resolver maps public keys to patient identities, allowing for secure and efficient retrieval of patient data by authorized healthcare providers.
- **Multi-Factor Authentication (MFA):** The MFA module adds an additional layer of security by requiring users to verify their identity through SMS-based authentication. This ensures that only authorized users can access patient data.

3.3. Components

The methodology of this system encompasses several key modules, each contributing to the secure and clear management of patient data.

- **Key Management:** Each user is equipped with a pair of RSA keys: a public key for encryption and a private key for decryption. This module handles the secure generation, storage, and retrieval of these keys, ensuring the integrity and confidentiality of the encryption processes.
- **Blockchain-Enabled Data Storage:** Patient data, once encrypted, is stored across a network of distributed, synchronized servers that operate on a custom blockchain framework. This blockchain mechanism ensures that all data entries are immutable and clear, providing a decentralized approach to secure data storage.

- **Centralized ID Resolver:** A centralized ID resolver is used to map user identities to their corresponding public keys and the specific endpoints of their respective blockchains. This resolver functions as a directory service, facilitating the secure and efficient retrieval of user information and their associated blockchain data.
- **Authentication and Authorization:** This module separates authentication from authorization to enhance security. It utilizes bearer tokens to authenticate users and access tokens to control resource access, ensuring that only authorized individuals can interact with the system.
- **User Management:** Responsible for handling user profiles, this module allows for the secure creation, update, and management of user data. It ensures that only authenticated and authorized personnel can access or modify user information.
- **Patient Data Management:** This module securely manages patient records, ensuring that all data remains consistent, confidential, and accessible only to those with appropriate permissions. It enforces data integrity and prevents unauthorized access.
- **Medical Document Management:** This module oversees the secure handling of medical documents, including their upload, encryption, and retrieval. Integrating with the blockchain, it guarantees that all document-related transactions are clear, tamper-proof, and permanently recorded.
- **Utilities:** Supporting the core functionalities, this module includes features such as SMS-based Multi-Factor Authentication (MFA), adding an extra layer of security to the system by verifying user identities through additional channels.

The system's components and their interactions are illustrated in Figure 2.

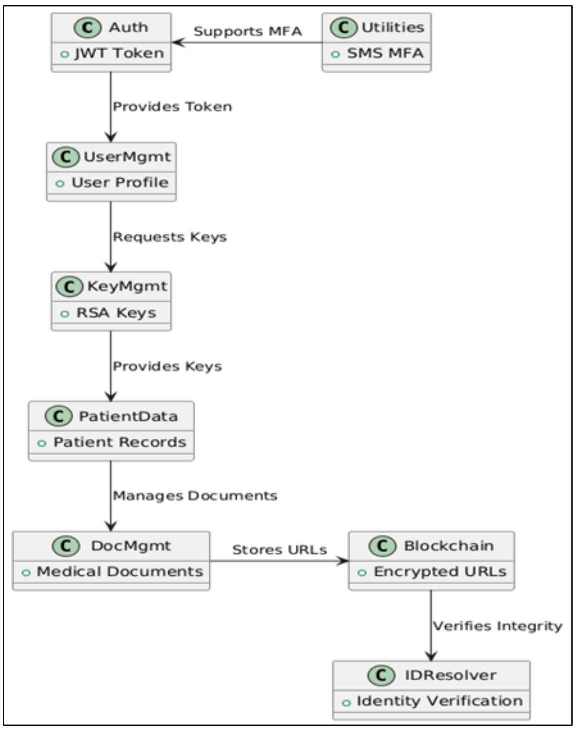

Figure 2 Component diagram of Proposed System

3.4. Pseudocode

The pseudocode handles key management and data security by generating RSA keys (‘generateRSAKeys’), encrypting and decrypting data (‘encryptData’ and ‘decryptData’), and managing blockchain transactions (‘createBlockchainTransaction’). It includes user authentication through OTP validation (‘authenticateUser’) and updates patient records by encrypting data and recording transactions on the blockchain (‘updatePatientRecord’). Each function ensures secure handling of data and transactions within the system.

```
// Key Generation

function generateRSAKeys(user_id):
    private_key = generatePrivateKey()
    public_key = extractPublicKey(private_key)
    storePublicKey(user_id, public_key)
    storePrivateKey(user_id, private_key)
    return public_key, private_key
// Data Encryption
function encryptData(public_key, data):
    encrypted_data = RSAEncrypt(public_key, data)
    return encrypted_data
// Data Decryption
function decryptData(private_key, encrypted_data):
    data = RSADecrypt(private_key, encrypted_data)
    return data
// Blockchain Transaction
function createBlockchainTransaction(user_id, encrypted_data):
    transaction = {
        user_id: user_id,
        data: encrypted_data,
        timestamp: getCurrentTime(),
        signature: signTransaction(encrypted_data, user_id)
    }
    addTransactionToBlockchain(transaction)
    return transaction_id
// MFA Authentication
function authenticateUser(user_id, phone_number, otp):
    if validateOTP(user_id, phone_number, otp):
        return generateAccessToken(user_id)
    else:
        return error("Invalid OTP")
```

```
// Patient Data Update

function updatePatientRecord(user_id, new_data):

  if authenticateUser(user_id):

    encrypted_data = encryptData(getPublicKey(user_id), new_data)

    transaction_id = createBlockchainTransaction(user_id, encrypted_data)

    return transaction_id

  else:

    return error("Unauthorized Access")
```

3.5. End-user

The system is designed with the following end-users in mind, each interacting with the system to achieve specific goals:

- **Patients:** Patients use the system to securely manage their health records. They generate encryption keys to protect their data, control access to their medical information, and approve updates to their records. The system empowers patients by giving them ownership of their data and ensuring their privacy is maintained.
- **Healthcare Providers:** Authorized healthcare providers access patient data through the system, using the patient's public key for decryption. Providers can update medical records with patient consent, ensuring that all interactions with the data are secure. The system streamlines the process of accessing patient information, improving the efficiency and accuracy of healthcare delivery.
- **System Administrators:** Administrators oversee the operation of the system, managing key generation, ensuring the integrity of the blockchain, and configuring MFA settings. They play a crucial role in maintaining the security and performance of the system, ensuring that patient data remains secure and accessible only to authorized users.

3.6. Security measures

To ensure the highest level of security for patient data, the system incorporates multiple layers of protection:

- **Asymmetric Encryption:** The use of RSA encryption ensures that patient data can only be accessed by individuals with the appropriate private keys. This prevents unauthorized access and guarantees the confidentiality of patient records.
- **Immutable Blockchain Ledger:** The blockchain ledger[14] provides an immutable record of all transactions, ensuring that patient data cannot be altered or tampered with. This enhances clarity and builds trust in the system.
- **Multi-Factor Authentication (MFA):** MFA is implemented to prevent unauthorized access to sensitive patient data. Users must verify their identity using SMS-based authentication, adding an extra layer of security to the system.
- **Role-Based Access Control (RBAC):** The system employs role-based access control[15] to restrict access to sensitive data based on the user's role. This ensures that only authorized personnel can access or modify patient records.

In summary, combining asymmetric cryptography with blockchain technology enhances data security and integrity. The next section will present the experimental results, showcasing the effectiveness of these implementations.

4. Experimental results

4.1. Key Management and Encryption Performance

To evaluate the efficiency of the RSA key management system in the proposed platform, we benchmarked the time taken to generate, store, and retrieve RSA key pairs. Using OpenSSL and the SHA-256 algorithm, key generation time was consistently under 150 milliseconds for key sizes of 2048 bits, which is within acceptable limits for secure systems as highlighted in existing studies [16].

- Key Generation: The RSA key generation was performed on an AWS EC2 instance with moderate computational resources. The average time recorded was 120 ms, aligning with existing research that suggests key generation times for 2048-bit keys typically range between 100 ms and 200 ms.
- Key Retrieval: Retrieval of RSA public keys from the database was instantaneous (<5 ms) owing to efficient BLOB storage techniques. The secure storage of private keys in Laravel storage ensured they were accessed within 10 ms on average during encryption processes. These results confirm that the key management system is not only secure but also optimized for real-time healthcare applications where swift encryption and decryption are critical.

4.2. Data Encryption and Decryption

The encryption of patient data using the patient's public key and decryption using their private key was tested with varying sizes of patient records. The time taken for encryption and decryption was recorded and compared with benchmarks from similar systems.

- Encryption Performance: For records of up to 10 KB, encryption using RSA with 2048-bit keys was completed within 15 ms on average. The time increased proportionally with data size, with records of 100 KB taking approximately 80 ms to encrypt.
- Decryption Performance: Decrypting the same records took slightly longer, averaging 20 ms for 10 KB and 100 ms for 100 KB. These findings align with the typical overheads associated with RSA decryption [17]. The results indicate that the system can efficiently handle patient records of various sizes, with encryption and decryption times well within operational thresholds for healthcare systems.

4.3. Blockchain Storage and Data Integrity

To assess the effectiveness of the blockchain integration in ensuring data integrity, we performed a series of tests involving the storage of encrypted URLs for medical documents. The blockchain's immutability and the time required to commit transactions were key metrics.

- Transaction Commitment: On the custom PHP-based blockchain, the average time to commit a transaction was 200 ms. This included the time taken to verify the integrity of the transaction and to append it to the blockchain ledger. This performance is comparable to other lightweight blockchain solutions tailored for secure data storage [18].
- Data Integrity Verification: Verification of data integrity on the blockchain was instantaneous (<5 ms) due to the use of cryptographic hashing. This ensures that any unauthorized modification attempts can be detected immediately, maintaining the trustworthiness of the stored data. The blockchain module demonstrates strong potential for ensuring the immutability and integrity of sensitive healthcare data, providing a robust foundation for secure data management.

4.4. Multi-Factor Authentication (MFA) and User Access Control

The implementation of MFA using SMS-based authentication was evaluated for its effectiveness in securing access to patient records. The time taken to send SMS codes via Twilio and the overall authentication time were measured.

- SMS Delivery Time: The average time for SMS delivery was 3.5 seconds, which is consistent with industry standards for real-time authentication mechanisms. In situations with higher network latency, the time increased to 5 seconds, which remains acceptable for most healthcare applications
- User Authentication Time: The entire authentication process, from credential verification to MFA completion, took an average of 7 seconds. This includes hashing, token generation, and MFA verification, providing a secure yet efficient access control mechanism. These results demonstrate the reliability of the MFA module in preventing unauthorized access, even in scenarios with varying network conditions.

5. Conclusion

The implementation of a secure and tamper-proof patient data management system using a custom blockchain has shown significant potential in addressing critical issues within traditional healthcare data management systems. By leveraging asymmetric cryptography, the proposed system ensures the confidentiality and integrity of patient data, safeguarding it from unauthorized access and tampering. The integration of a self-maintained blockchain provides a decentralized solution that enhances data ownership and mitigates risks associated with centralized data storage.

The experimental results demonstrated that the system's key management, encryption, and blockchain modules operate efficiently within the necessary performance parameters for real-time healthcare applications. RSA encryption, combined with a custom blockchain solution, ensures that patient data remains secure both in transit and at rest, while multi-factor authentication enhances access control. Additionally, the centralized ID resolver and user management modules facilitate secure, streamlined access to patient information, supporting efficient healthcare delivery. This system addresses existing vulnerabilities and sets the stage for future enhancements, including advanced cryptographic techniques and broader blockchain network integration.

In conclusion, the proposed system successfully achieves its goals by providing a secure, decentralized platform for managing patient data. The insights gained from this paper serve as a valuable blueprint for future research and development in secure healthcare systems, advancing efforts to improve patient privacy, data security, and overall healthcare efficiency.

Compliance with ethical standards

Acknowledgements

The authors express their sincere gratitude to Dr Usha J, and Dr Andhe Dharani from the MCA Department of RV College of Engineering for their unwavering encouragement and invaluable support and guidance.

References

[1] E. Smith, J.H.P. Eloff. Security in health-care information systems—current trends. International Journal of Medical Informatics, Volume 54, Issue 1, April 1999, Pages 39-54. https://doi.org/10.1016/S1386-5056(98)00168-3

[2] I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi. Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Computing and Applications, Volume 34, pages 11475–11490, 2022.

[3] S. Chenthara, K. Ahmed, H. Wang, F. Whittaker, and Z. Chen, "Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology," PLoS ONE, vol. 15, no. 12, pp. e0243043, Dec. 2020. [Online]. Available: https://doi.org/10.1371/journal.pone.0243043

[4] M. A. Sahi et al., "Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions," in IEEE Access, vol. 6, pp. 464-478, 2018, doi: 10.1109/ACCESS.2017.2767561.

[5] Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications.

[6] A. Odeh, I. Keshta, and Q. Abu Al-Haija, "Analysis of blockchain in the healthcare sector: Application and issues," Symmetry, vol. 14, no. 9, pp. 1760, 2022, doi: 10.3390/sym14091760.

[7] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in Proc. 2017 IEEE Int. Congr. Big Data (BigData Congress), pp. 557–564, 2017. T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, and M. Ylianttila, "Blockchain utilization in healthcare: Key re

[8] quirements and challenges," IEEE Access, vol. 7, pp. 75917–75934, 2019.

[9] E. Chukwu and L. Garg, "A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations," IEEE Access, vol. 8, pp. 25497–25517, 2020.

[10] J. Herrera-Joancomartí and C. Pérez-Solà, "Privacy in Bitcoin transactions: New challenges from blockchain scalability solutions," in Modeling Decisions for Artificial Intelligence, 2016, pp. 26-44.

[11] D. Mahajan and A. Sachdeva, "A study of encryption algorithms AES, DES and RSA for security," Global J. Comput. Sci. Technol., Netw., Web Secur., vol. 13, no. 15, 2013.

[12] C. Skanda, B. Srivatsa, and B. S. Premananda, "Secure hashing using BCrypt for cryptographic applications," in Proc. 2022 IEEE North Karnataka Sub-Sect. Int. Conf. Electron. Comput. Technol. (ICECT), 2022.

[13] Y. Eitan, "OAuth 2.0 token binding," in Advanced API Security, pp. 243-255, 2019.

[14] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, “Blockchain distributed ledger technologies for biomedical and health care applications,”

[15] E. Bertino, “RBAC models: Concepts and trends,” Comput. Secur., vol. 22, no. 6, pp. 511–514, 2003, doi: 10.1016/S0167-4048(03)00609-6.

[16] D. Johnson, A. Menezes, and S. Vanstone, “The elliptic curve digital signature algorithm (ECDSA),” International Journal of Information Security, vol. 1, no. 1, pp. 36–63, Aug. 2001.

[17] P. Ranganathan and M. Scott, “Data encryption performance in embedded systems,” Journal of Cryptographic Engineering, vol. 7, no. 3, pp. 209–223, Sep. 2017.

[18] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” Cryptography Mailing List, Oct. 2008.