An Integrated Privacy Preservation and Blockchain Mode for Secured Data Transmission in Medical Applications

1st E. Samatha Sree Chaturved
Research Scholar
School of Computing
Sathyabama Institute of science and Technology(SIST)
Tamilnadu, India
eschaturvedi@gmail.com

2nd L. Mary Gladence
Professor
School of Computing
Sathyabama Institute of science and Technology(SIST)
Tamilnadu, India
marygladence.it@sathyabama.ac.in

Abstract

Keeping medical data safe and private has become a big challenge with the fast-growing digital healthcare systems. Old security methods are not strong enough to stop hacking and unauthorized access. This paper introduces an Integrated Privacy Preservation and Blockchain (IPPB) model to make medical data sharing secure. The model uses blockchain to create a decentralized and unchangeable record that ensures data accuracy, precise tracking, and controlled access. It also applies strong encryption methods like homomorphic encryption and zero-knowledge proofs (ZKP) to protect patient information while allowing safe data sharing between healthcare providers. A lightweight approval method is used to make the system faster, which lowers the usual heavy processing of blockchain networks, making it better for real-time medical use. An intelligent contract-based access system ensures that only allowed users can see the data while keeping track of who accessed it. Tests show that the IPPB model works better than current security methods by improving speed, maintaining private data, and defending against cyber threats. The results prove that adding blockchain to privacy systems can make medical data more secure, trustworthy, and easy to share, making it useful for future healthcare systems.

Keywords: Privacy Preservation, Blockchain, Medical Data Security, Homomorphic Encryption, Smart Contracts, Secure Data Transmission, Cybersecurity in Healthcare.

Introduction

With the development of the digital healthcare system, medical data transmission has become one of the most essential parts of modern healthcare infrastructure. The growth of electronic health records (EHR), telemedicine, and the Internet of Medical Things (IoMT) have played a significant role in seamless data exchange between the healthcare sector and improved operational efficiency and patient care. Yet, with digitization, various security and privacy issues emerge, such as data breaches, unauthorized access, cyber threats, and so on. Usually, traditional security mechanisms, such as encryption-based storage and centralized access control systems, can't have the ability to provide end-to-end transparency, data integrity and confidentiality to the model. So, there is a need for an advanced model to improve the security mechanism.

Blockchain has become a very useful technology for securing medical data transmission because it is decentralized, cannot be altered, and is fully transparent. Blockchain removes specific critical points of failure and guarantees high data sovereignty while providing efficient and transparent access control. However, the traditional blockchain implementation has some issues, such as scalability, high computation overhead problems and potential privacy issues that are not very appropriate for real-time medical applications. So, the challenges need to be identified to enhance the privacy and security system while transferring healthcare data.

To address these challenges, this paper introduced an advanced Integrated Privacy Preservation and Blockchain (IPPB) Model for secure data transmission in medical applications. It builds based on tamper-proof and decentralized blockchain technology while using advanced cryptography techniques, mainly zero-knowledge proofs (ZKP) and homomorphic encryption, which are widely used to ensure transaction privacy. Incorporating a lightweight consensus mechanism in this healthcare system reduces the processing overhead and makes blockchain deployable in healthcare environments. In addition, it also introduced smart contract-based access control, which helps to provide automated, secure and auditable data-sharing policies between healthcare entities.

The proposed IPPB framework's primary aim is to offer an efficient security framework to strengthen integrity, privacy, and reliability while transmitting medical data. Its overall efficacy is evaluated by experimenting with it using real-time applications. The experimental result stated that it performs better and faster than the existing privacy preservation and transmission efficiency

frameworks and provides better resilience against cyber-attacks. The findings also stated that combining blockchain with privacy-preserving cryptographic schemes has significantly improved the security, trustworthiness and interoperability of medical data sharing, which makes this model more suitable for the next-generation healthcare system.

Contribution of The Paper

This paper contributes the following steps of procedures to the entire performance of data collection, preprocessing, and secured transmission from a source to a destination.

- A figurative explanation is demonstrated to understand how healthcare records become high-dimensional data and the need for an advanced database mechanism to secure the data instead of normal encryption-decryption.
- An immutable ledger system is created and deployed as a decentralized ledger to improve data security regarding integrity, traceability, and transparency for healthcare and medical data.
- A Homomorphic Encryption model is implemented to apply computation on encrypted healthcare data without affecting sensitive information.
- A Zer-Knowledge Proof is integrated to examine user authentication to preserve privacy without exploring all the data.

This paper provides a novel security framework integrating data generation, preparation, and implementation of blockchain and other interrelated security processes. It provides an advanced cryptographic method to preserve privacy and scalable healthcare data transmission.

Literature Survey

Combining blockchain technology and advanced encryption methods is a promising way to protect medical data. This survey looks at recent progress in this area, mainly focusing on keeping medical information private and secure in healthcare. In 2009, blockchain technology received a wide reputation in all kinds of decentralized computing applications due to the emergence of Bitcoin [1]. The IoMT has changed healthcare by allowing smart devices to create and share large amounts of personal medical records. However, keeping this sensitive data safe from unauthorized access is a big challenge. One study introduced a triple-subject purpose-based access control (TSPAC) model that securely uses blockchain to share medical data in IoMT systems [2]. This model improves security by ensuring that only approved users can access specific medical data based on its intended purpose. A homomorphic encryption technique is applied to encrypt the data to ensure privacy during data transmission [3]. Research has shown that this method helps hospitals work together on encrypted medical data without exposing patient details. For example, hospitals can analyze encrypted data to improve treatment methods while keeping patient information private. The author in [4] explained that zero-knowledge proofs (ZKPs) allow one party to prove they have specific information without revealing it. In healthcare, ZKPs help verify user identities when accessing electronic health records (EHRs) without showing personal details, increasing privacy. Studies have shown that ZKPs can be useful for security in different fields, including healthcare. Traditional blockchain methods require a lot of computing power, which can slow down real-time medical processes. To fix this, researchers have developed lightweight blockchain systems for IoMT. These systems use better algorithms to lower delays and reduce resource use, making them more efficient for smart medical devices [5]. Smart contracts help automate and enforce rules for data access on blockchain networks [6]. In healthcare, they ensure that only authorized people can access medical data based on patient consent and legal requirements. One method combines blockchain with attribute-based encryption to give medical institutions more control over data sharing while protecting patient privacy.

Some research has focused on developing advanced cryptographic mechanisms to tighten the security level of healthcare data. Shraiyash Pandey et al. [7] presented ZKP and post-quantum cryptography for securing and improves the examination of proof authentication. The author also explored the evolution of the healthcare data analytics industry processes from Healthcare 1.0 to 5.0 by updating the technologies for data and technological transformations. Similarly, S. Bharath Babu and K. R. Jothi [8] proposed a framework comprising blockchain technology, ZKP, and Homomorphic encryption methods for improving data security, privacy preservation and balancing data usage during healthcare data analysis and transmission. Combining the above three approaches allows stakeholders to derive insights from healthcare data without exploring sensitive data. Thus, this model facilitates research and the collection of personalized healthcare data. Earlier studies also focused on using blockchain technology to implement high-level healthcare and medical data transmission security. For example, Hao Jin et al. [9] reviewed the recent advances in methods used for security and preserving the application's user data. The author classifies permissionless and permission-based blockchain methods with merits and demerits. Various potential methods related to blockchain-based healthcare data security are discussed in detail. Ranaweera T.A.V.Y et al. [10] have developed a security model for improving digitalized EHR systems by integrating advanced cryptographic methods. The author's target was protecting healthcare data from cyberattacks to safeguard the patient's sensitive information. Homomorphic encryption, ZKPs, and blockchain

models are integrated to enhance the security and privacy of EHRs. The integration of advanced cryptographic methods ensures confidential and temper-proof patient data.

Shifting from earlier cryptographic methods to blockchain technology with other advanced cryptographic methods increases the robustness and enhanced privacy preservation in healthcare data security. Current research and real-time implementations of emerging healthcare and medical data systems focus on using blockchain with advanced cryptographic methods to improve security outputs. The above survey shows that blockchain frameworks used earlier are highly expensive in computation and proof-of-concept, making them unsuitable for real-time healthcare applications. They also struggled with latency and less throughput due to network scalability. They have found many issues and challenges, like interoperability, susceptibility and scalability. Thus, to overcome the problems and challenges of the existing blockchain frameworks, this paper is motivated to integrate advanced cryptographic techniques with blockchain technology, explained in detail below.

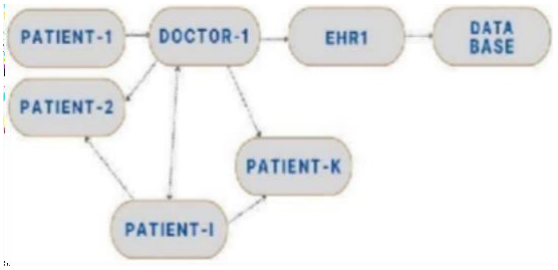
Problem Statement

Let the hospital $H1$has N number of doctors $D = \{D1, D2, \ldots Di, \ldots DN\}$ is committed with K number of patients. Each patient's medical and health data are maintained in EHR and persisted in a local data server for fast access and processors. $EHR = \{EHR1, EHR2, \ldots EHRi, \ldots EHRK\}$ is maintained by doctor 1. It is assumed that a similar scenario is available in M number of hospitals, then $H = \{H1, H2, \ldots . Hi, HM\}$ and $E\ H\ Ri\ j^{k}$ denotes that it is the electronic healthcare record of i^{th}patient, monitories by j^{th}doctor in K^{th}hospital. The overall complexity of medical data generation is represented in Figure 2.

Proposed IPPB

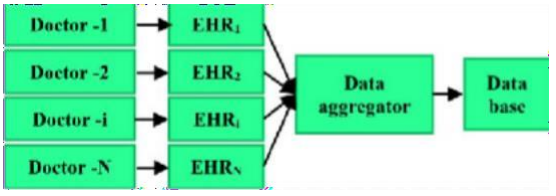
This paper proposes an Integrated Privacy Preservation and Blockchain (IPPB) model to make medical data sharing secure by analysing the electronic health records (***EHRs***) of patients diagnosed by doctors in multiple hospitals. The primary objective of this study is to simplify the complexity of analysing large-scale EHR data and transmit it to the destination node with high security and privacy. The input EHR data includes all the sensitive details of the patients, such as name, age, gender, current health condition, and other medical history. So, tightening the data security system between the source and destination device is essential.

Figure-1(a) depicts the workflow of the proposed IPPB framework for analysing and storing the EHR of patients in the database (***DB***). Generally, the doctor diagnoses and provides Multiple ***EHR1*** data includes medicines, health reports, current health conditions, previously provided treatments, diet, diagnosis results, and other personal details of each patient. To simplify the data analysis process, the proposed deep learning model collects the Multiple ***EHR1*** of the ***K*** number of patients (***P***) generated by the doctor (***D1***) and transmitted and stored into the DB based on individual ID.



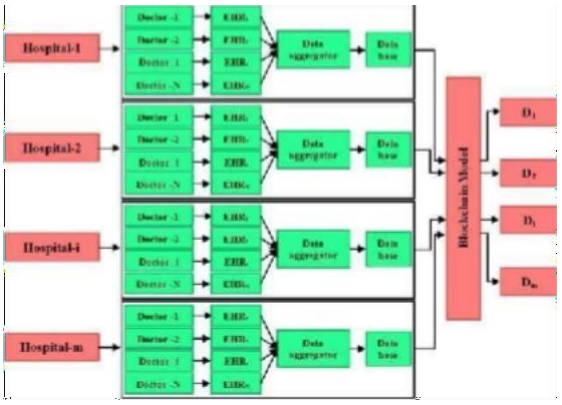
(a). Doctor Vs. Patients

Figure-1(b) shows the structure of the IPPB model on handling ***N*** number of (**EHRs**) generated by ***N*** number of doctors (***DN***). That is each (***D***) in hospital (***H***) have handling (***P***)**,** for each (***p***)**,** set of (**EHRs**) are generated. Similarly, in a single (***H***), (***DN***)have to work, and every day, they are diagnosing and generating ***EHRN*** of data, all these data are gathered and transmitted into a single pathway and stored in the **(DB)** using the proposed DL model and a unique patient ID.



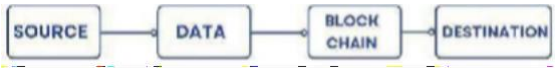
(b). Doctor Vs. EHRs

Figure-1(c) shows how the proposed model is suitable for processing the data gathered from multiple Hospitals (***HM***). In figure-1(c), the variable {(***b1***), (***b2***), … , (***bi***), … (***bn***)} indicates the blocks, representing the proposed model's workflow discussed in figure-1(b). The input data are generated by the (***DN***) in (***HM***), from the source point, all the ***EHR11*** are collected by the DL model using data aggregators.



(c). Hospital Vs. Healthcare Data Generation

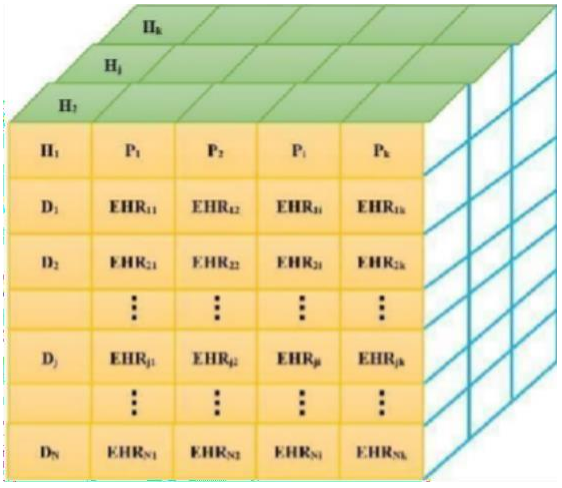
The data collected through the data aggregators is either stored in the (***DB***) are transmitted to the destination device through the blockchain (***BC***)**.** Figure 1 (d) shows the proposed model's overall workflow.



(d). Overall Process

Figure 1. Workflow of IPPB Framework

Here, the (***BC***) model is implemented to tighten the security system of the healthcare application. Because, gathering (**EHRs**) of every individual from (***Dn***) in (***Hm***), converts the input (***1D***) data into multidimensional data (***MD***), as shown in Figure 2. In that case, an advanced security system is required to transmit the patient data from the source device to the destination device. Thus, this paper proposes and implements a blockchain-integrated deep learning model to analyse and secure data transmission.



Blockchain (BC) is a decentralized model used to store and verify transactions over a network of computers. It is also termed distributed ledger technology (DLT). The BC includes multiple blocks; each block has a chain of connection. The BC blocks' data are not removed or modified without authorised users' knowledge. It creates an immutable ledger for tracking transactions, payments, orders, etc. To prevent the input of sensitive data from unauthorized users, it has built-in mechanisms which share the copy of the ledger (authorized and unauthorized transaction entries) to all the blocks. This technique will reduce the need for third parties between the source and destination device. BC is fully transparent for the verification and monitoring of every individual. Each block in the BC network is connected with previous blocks using a specific cryptographic hash value. Each block contains a unique header and body to process large-scale input data. The total number of blocks is created based on the input data. In each block, the header blocks include the hash value of the current and previous blocks, nonce, timestamp, Merkle root, and difficulty target. The body block contains distributed ledgers, representing the hash value and overall details of transactions. Through BC, highly sensitive data are secured, stored, and transmitted. So, it is widely used in many applications to perform secure data transmission. Similarly, this BC is implemented to handle the large set of patient EHRs collected from various hospitals. Each transaction in the network is verified using the cryptographic hash function (H). This make the distributed HER data into fixed-size output.

$$H(X) = h$$

Here, H indicates the has function, x illustrates the input EHR data, and h indicates hash digest. To verify all the input entities are secured and authorized entities, the digital signature signed before the transaction is ensured by the proposed model.

$$S = H(x)^d \ mod \ n$$

Here, x is the HER data, (x) denotes hashed HER value, d denotes the sender's private key, and n denotes data encryption modulus. Once the signature is generated, it is verified using its public and private key, which is stored in the BC database.

$$H(X) = S^e \ mod \ n$$

Here, S^e indicates the public key of the input entities. If the signed key value matches the stored key value in the database, then the BC allows the entities to perform the transaction. Once the model

successfully logs in to the network, the input data are encrypted using data encryption techniques like RSA or ECC before the transaction. The source or sender node encrypts the data using a unique public key value and transmits it to the destination device.

$$C = X^e \ mod \ n$$

Where, X is the plain patient EHR data, e indicates the receiver's public key and C denotes the ciphertext. Using the unique private key value, the recipient decrypts the transaction. It is expressed as:

$$Y = C^d \ mod \ n$$

Here, Y represent the decrypted data, C represent the input encrypted EHR data, and d represents the receiver's private key value.

Zero-Knowledge Proof (ZKP) in Blockchain for Medical Data Security

Zero-knowledge proof lets one person, called the prover, show another person, called the verifier, that something is true without sharing the details. In medical data security, ZKP helps doctors and hospitals check patient information without revealing personal medical records. ZKP in blockchain follows three main ideas. First, completeness means a fair verifier will believe a fair prover if the statement is true. Second, soundness means a dishonest prover cannot trick a fair verifier into accepting something false. Third, zero-knowledge means no extra details are shared except that the statement is true. For example, a ZKP-based method in blockchain can help verify patient records without showing any medical data. Let x be the patient's encrypted medical data and (x) be its cryptographic hash. A prover (hospital) wants to prove knowledge of x (valid medical record) without revealing it. The prover generates a secret random number r and computes a commitment:

$$C = H(x \| r)$$

Where C is the commitment stored on the blockchain as an immutable reference, the verifier (another hospital or insurance provider) selects a random challenge c and sends it to the prover. The prover computes a response R

$$R = f(x, r, c)$$

A typical function f could be

$$R = x \,.\, c + r \ mod \ p$$

Where p is a large prime to ensure security, the verifier checks if:

$$H(x \| r) = C$$

If the verification is valid, the prover has shown awareness of x without exposing accurate medical information. Smart contracts should use Zero-Knowledge Proof (ZKP) verification to ensure that only authorized people can check medical data while keeping it private. Homomorphic Encryption (HE) should be combined with ZKP to do calculations on encrypted medical data without decrypting it. To reduce computing effort, a lightweight approval method should be used with efficient cryptographic techniques like Schnorr or Bullet-proofs, making real-time use easier.

Homomorphic Encryption

In addition to the ZKP method, the proposed IPPB framework also includes a homomorphic encryption technique for verifying input medical data. This method is mainly used for key generation, data encryption, and decryption during medical data transmission from the source device to the destination device. The homomorphic encryption method-based authentication system is performed by referring to the step discussed in the study [18].

The IPPB model is designed and implemented by integrating the above three technologies, and the performance is verified.

Result and Discussion

This paper implements the Integrated Privacy Preservation and Blockchain (IPPB) model for secure healthcare data transmission. The model was experimented using the simulation software installed in the Windows OS system with the Intel i7 processor 12th Gen, 1TB HDD, and 64 GB RAM. The proposed IPPB framework analyses the digital signature of the input transaction using its private and public keys and permits the authorized device or entities to process data transmission. The proposed IPPB framework efficacy is analysed using mutiple parameters like data transmission speed, delay time, throughput, encryption and decryption time, etc. This section discusses the proposed framework's simulation and graphical results in detail using the dataset explained below.

Dataset

The performance of the IPPB framework is evaluated by training and testing on real-time Electronic Health Records (EHR) datasets. The

dataset contains about 50,000 patient records for different types of diseases. The patient records are taken from publicly available databases such as Kaggle and MIMIC—-111 databases. It also contains sensitive attributes such as diagnosis, prescription, patient demographics, and lab results. Finally, the dataset was tokenized and anonymized before blockchain storage and encryption.

Performance Metrics

The efficiency and effectiveness of the model were analysed using various quantitative metrics, which include security analysis, encryption and decryption time, data transmission speed, throughput value, effectiveness of access control, and blockchain latency. Security analysis used resistance to main-in-the-middle attacks, blockchain tampering, and unauthorized access. Encryption and decryption time were calculated by the performance of the homomorphic encryption in data sharing, which was calculated in seconds (s). Data transmission speed was evaluated by the time taken to transfer the medical data securely over the blockchain technology, which was estimated in (ms). The throughput value was evaluated by the number of transactions successfully done per second. The effectiveness of the access control was evaluated by the success rate of the role-based access control, which was evaluated in (%). Finally, blockchain latency was evaluated by validating the transaction and finalization time in the network.

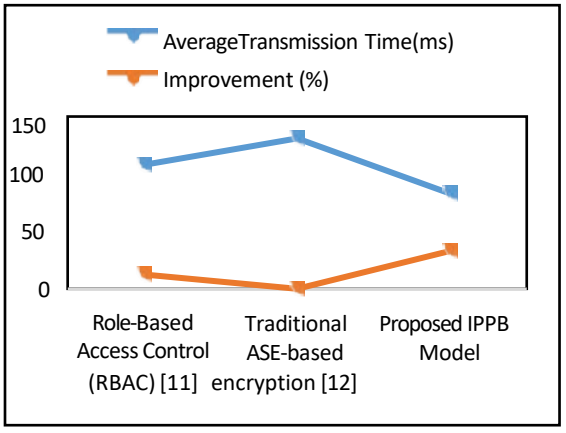


Figure-3 Data Transmission Speed Analysis

Figure-3 shows the average data transmission speed to the proposed IPPB and existing models: RBAC [11] and AES-based encryption [12]. This result is observed by transmitting the data across different network conditions. The result shows that the proposed IPPB model transmits the data with 83 ms, which is 33% faster than the traditional models. It is because of the lightweight consensus mechanism and optimized data verification technique, which minimize the overall time taken for authentication verification and transaction.

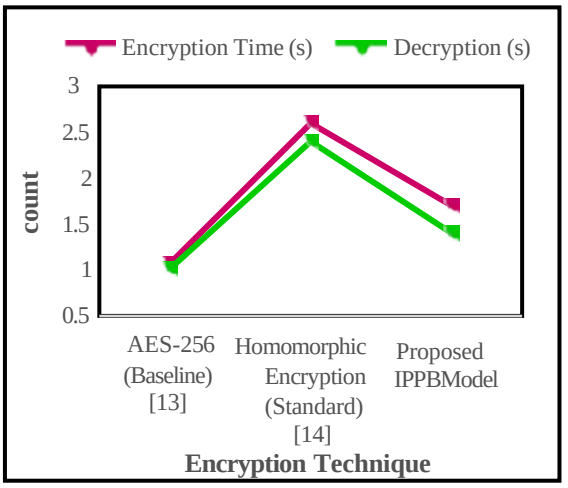


Figure-4 Data Encryption And Decryption Time Analysis

The total time taken for data encryption and decryption over the proposed and existing model (AES-256 [13] and Homomorphic encryption [14]) is analysed, and the result is illustrated in figure-4. The comparison result shows the AES model has consumer 1.07s for encryption and 1.01s for decryption, and the homomorphic method utilized 2.6s for encryption and 2.4s for decryption. The proposed model consumes 1.7s and 1.4s for data encryption and decryption, 24 times faster than the traditional methods. Implementing the zero-knowledge proofs (ZKP) method minimizes computational complexity and ensures secure data transmission.

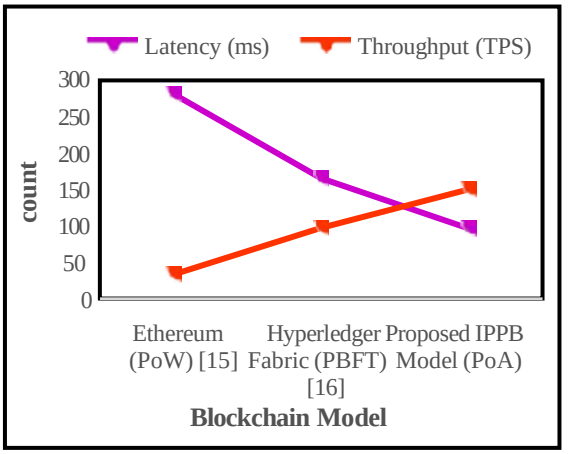


Figure-5 Through and Latency Analysis

The model's efficiency in analysing and creating a secure data transmission platform is evaluated based on throughput (TH) and Latency (ms) time. Thus, the throughput and latency time of the proposed and existing models (Ethereum (PoW)

[15] and Hyperledger Fabric (PBFT) [16]) are analysed, and the result is shown in Figure 5. The comparison proves that the proposed IPPB model performs better with a throughput of 150 TH and a latency time of 96ms compared to other models. The proposed model has achieved 40% improvements in throughput, illustrating that the proposed PoA algorithm increases transaction throughput with minimised latency.

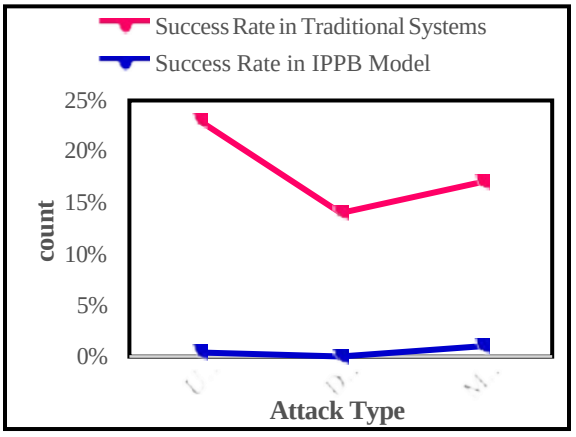


Figure-6 Security And Privacy Analysis Results

Figure-6 depicts the proposed and existing model [17] security and privacy analysis results regarding unauthorised access, man-in-the-middle, and data tampering. The analysis shows that by integrating a smart contract system and a cryptographic authentication system, unauthorised access, man-in-the-middle, and data tampering are reduced to 0.4%, 1%, and 0%, respectively. The proposed IPPB framework provides a tamper-proof, decentralized, and highly privacy-preserving platform for securing medical data.

Conclusion

An Integrated Privacy Preservation using a Blockchain model is proposed to secure healthcare data transmission. It aims to overcome the existing issues and challenges of earlier blockchain frameworks and cryptographic techniques. The main objective of this paper is to integrate multiple advanced cryptographic techniques, such as homomorphic encryption and zero-knowledge proofs, for increasing privacy preservation, decentralized healthcare data maintenance, and tamper-proof while data sharing and transmission. The IPPB model is implemented in Python and obtained 32% faster transmission speed than AES, 27% decreased encryption-decryption time than homomorphic method, and 38% increased throughput than the existing blockchain models used in healthcare applications. It also obtained 45% less blockchain latency than POW and 22% less than the Hyperledger fabric method. From the output, it is concluded that the IPPB framework performs better than other models. The blockchain model will be integrated with deep learning-based healthcare data analytics to improve data security in healthcare data processing.

References

1. Wu, G., Wang, S., & Ning, Z. (2021). Blockchain-enabled privacy-preserving access control for data publishing and sharing in the internet of medical things. *IEEE Internet of Things Journal*, *9*(11), 8091-8104.
2. Scheibner, J., Ienca, M., & Vayena, E. (2022). Health data privacy through homomorphic encryption and distributed ledger computing: an ethical-legal qualitative expert assessment study. *BMC Medical Ethics*, *23*(1), 121.
3. Jayodya Methma, (2023), "Zero Knowledge Proofs: A Comprehensive Review of Applications, Protocols, and Future Directions in Cybersecurity", Computer Security and Reliability, DOI:10.13140/RG.2.2.11606.22080.
4. Li, C., Dong, M., Xin, X., Li, J., Chen, X. B., & Ota, K. (2023). Efficient privacy-preserving in IoMT with blockchain and lightweight secret sharing. *IEEE Internet of Things Journal*.
5. Xu, G., Qi, C., Dong, W., Gong, L., Liu, S., Chen, S., ... & Zheng, X. (2022). A privacy-preserving medical data-sharing scheme based on blockchain. *IEEE journal of biomedical and health informatics*, *27*(2), 698-709.
6. Pandey, S., Bhushan, B., Hameed, A.A. (2024). Securing Healthcare 5.0: Zero-Knowledge Proof (ZKP) and Post Quantum Cryptography (PQC) Solutions for Medical Data Security. In: Reddy, C.K.K., Sithole, T., Ouaissa, M., ÖZER, Ö., Hanafiah, M.M. (eds) Soft Computing in Industry 5.0 for Sustainability. Springer, Cham. https://doi.org/10.1007/978-3-031-69336-6_15.
7. Babu, S. B., & Jothi, K. R. (2024). A Secure Framework for Privacy-Preserving Analytics in Healthcare Records Using Zero-Knowledge Proofs and Blockchain in Multi-Tenant Cloud Environments. *IEEE Access*.
8. Jin, H., Luo, Y., Li, P., & Mathew, J. (2019). A review of secure and privacy-preserving medical data sharing. *IEEE Access*, *7*, 61656-61669.
9. Ranaweera, T. A. V. Y., Hewage, H. N. H., HKDWMCB, H., Preethilal, K. L. K. T., Senarathne, A., & Ruggahakotuwa, L. (2023, December). Ensuring Electronic Health Record (EHR) Privacy using Zero Knowledge Proofs (ZKP) and Secure Encryption Schemes on Blockchain. In *2023 5th International Conference on Advancements in Computing (ICAC)* (pp. 792-797). IEEE.

10. *S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2009, Available: http://bitcoin.org/bitcoin.pdf.*
11. Murthy, K. S. R., & Manikandan, V. M. (2022). A reversible data hiding through an encryption scheme for medical image transmission using AES encryption with key scrambling. Journal of Advances in Information Technology Vol, 13(5).
12. Garg, T., Kagalwalla, N., Puthran, S., Churi, P., & Pawar, A. (2023). A novel approach of privacy-preserving data sharing system through data-tagging with role-based access control. World Journal of Engineering, 20(1), 12-28.
13. Mohammed, Z. K., Mohammed, M. A., Abdulkareem, K. H., Zebari, D. A., Lakhan, A., Marhoon, H. A., ... & Martinek, R. (2024). A metaverse framework for IoT-based remote patient monitoring and virtual consultations using AES-256 encryption. Applied Soft Computing, 158, 111588.