**TRUSTWORTHY AI WITH BLOCKCHAIN: PREVENTING DATA POISONING IN DECENTRALIZED MODEL SHARING**

**Abstract**

The healthcare system has rapidly adopted digital techniques to manage sensitive patient information in recent years. However, ensuring data privacy, security, and trust in the multi-use environment is a significant challenge. Blockchain technology offers a decentralized and tamper-proof solution, but storing and processing sensitive healthcare data directly on-chain raises privacy concerns. This paper proposed a secure, privacy-preserving framework for healthcare data sharing using blockchain integrated with advanced cryptographic techniques. The proposed system Smart Contracts manage permissions and interactions while referencing encrypted data stored off-chain using the Inter Planetary File System (IPFS). Then, the leverages Homomorphic Encryption to Enable Computations (HESD) on Encrypted data without exposing the raw content, ensuring end-to-end data confidentiality. Zero-Knowledge Proofs (ZKPs) are used for privacy-preserving access control, allowing users to verify their access rights without revealing sensitive credentials. Together, these components form a scalable architecture that allows patients to control data sharing while enabling secure analytics by authorized users. The system is audit-friendly, with every transaction recorded irreversibly on the blockchain. The simulation results suggest that the proposed structure maintains high security and privacy standards, supporting efficient data in the distributed healthcare environment and supporting access. Integrating homomorphic encryption, ZKPs, and blockchain-based smart contracts significantly enhances trust, transparency, and compliance with healthcare data regulations.

**Keywords:** Blockchain, Healthcare, Privacy Preservation, Homomorphic Encryption, Zero-Knowledge Proofs, Smart Contracts, IPFS.

**1. Introduction**

Rapid digitization of healthcare systems has produced and exchanged vast amounts of sensitive medical data, diagnostic reports and real-time monitoring information. While it improves digital shift medical services and patient results, it also shows essential data privacy, security and trust challenges [1]. Traditional centralized healthcare data management systems are prone to data violations, unauthorized access and lack of transparency, making them insufficient to handle crucial patient information in today's mutual environment [2]. Blockchain technique has emerged as a promising solution to secure health data due to its decentralized, irreversible and transparent nature. By removing the requirement of a central authority, the blockchain ensures that all data interactions are traceable and tampering proofs [3]. However, storing direct medical data on-chains can highlight sensitive information and give rise to scalability issues [4]. The blockchain alone cannot apply fine rash control or protect users' privacy without integrating additional privacy-conservation technologies. To remove these challenges, a strong and privacy-focused structure is required that combines blockchain with advanced cryptographic methods [5].

This paper proposes Homomorphic encryption, ZKPS, and smart contracts using IPFS. HESD enables safe computations on encrypted data without highlighting the underlying content and also preserves data privacy during analysis. ZKPS allow users to prove access to sensitive credentials without disclosing the rights, ensuring privacy in a multi-user environment.

**2. Literature Survey**

In recent years, blockchain technology in healthcare systems has attracted significant attention due to its decentralized and tampering-proof architecture. Several studies have detected the ability of blockchain to increase the transparency of data, safety and control in medical data management [6]. Traditional centralized healthcare data systems are unsafe for data violations and single points of failure, increasing the risk of handling sensitive patient information. The blockchain provides an unchanged account book, providing a solution for permanently storing access and transactions, ensuring auditability and traceability [7].

The security vulnerabilities in traditional cloud-assisted EHR systems. However, although described as "limited," pairing-based cryptography is typically computationally expensive, especially for resource-limited users or devices [8].

This project introduces a blockchain-empowered security and privacy protection scheme specifically designed for CEMRs. The scheme focuses on secure sharing, user privacy, and fine-grained access control. However, the system manager is responsible for generating all private keys and system parameters, which introduces a central trust assumption—potentially a single point of failure or target [9].

The Blockchain-based Privacy-Preserving and Rewarding Private Data-Sharing Scheme (BPRPDS). However, framing attacks in anonymous networks are hard to handle—BPRPDS addresses it, but the problem remains complex [10].

The Attribute-Based Access Control (ABAC): Patients define who can access their records based on attributes (e.g., role, organization). However, Attribute-based access control requires effective management of user attributes and policies, which can be hard at scale [11].

The Privacy-Preserving Secure Ant Colony Optimization with Multi-Kernel Support Vector Machine (ACOMKSVM) However, partial data views may affect overall model generalizability if not carefully managed [12].

The Blockchain + Trusted Execution Environment (TEE) for privacy-preserving healthcare data sharing algorithm. However, TEE dependency means the scheme relies on specific hardware (like Intel SGX), which could limit deployment across diverse systems [13].

A Confidentiality-Privacy Preserving Blockchain-Based Scheme for Healthcare Cloud Applications-Elliptic Curve Cryptography (HCA-ECC) based digital signature framework for secure session key establishment. However, using multiple cryptographic techniques (ECC, RSA, AES) may increase system complexity and computational cost [14].

A more machine learning-focused proposal applied ACOMKSVM in conjunction with blockchain and Elliptic Curve Cryptography (ECC) for privacy-preserving learning from distributed IoT data. However, the coordination overhead between channels and the real-world value of PrivyCoin remain open concerns [15].

Keyword-based Re-Encryption (KRE) and Oblivious Transfer-based Re-Encryption (OTRE) are two schemes designed for privacy-preserving health data sharing over a hybrid blockchain architecture. However, Security analysis confirmed that both KRE and OTRE are indistinguishable under chosen-plaintext attacks using a random Oracle model [16].

The proposed BAISMDT is a Blockchain and AI-Enabled Secure Medical Data Transmission model explicitly designed for IoT-based healthcare networks. However, although blockchain enhances security, its application across many IoT devices might limit scalability due to potential latency or network congestion issues [17].

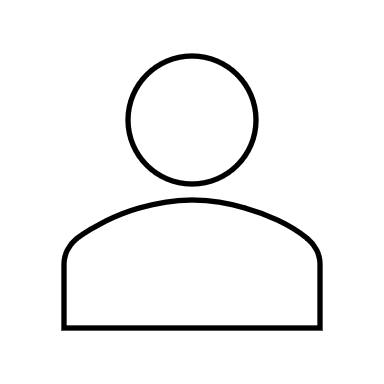
Key-Policy Attribute-(KP-ABE) is employed, while smart contracts enforce security and automate access procedures. However, while edge-based IoMT is efficient, executing KP-ABE, Bloom filters, and game-based incentive mechanisms on resource-constrained devices could be demanding [18].

The Proof of Authority (POA) adopts Ethereum evidence of the consensus mechanism to promote efficiency and reduce transaction delays. However, the system uses proxy re-encryption, but the flexibility of access control policies is not discussed, which can limit its practical appropriateness in diverse settings [19].

This paper addresses the security and privacy challenges of storing and sharing sensitive patient health data in cloud environments—however, there is Limited support for advanced or role-based access control [20].

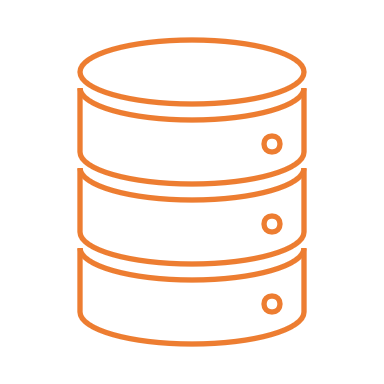
**3. Proposed Methodology**

The proposed privacy-preserving architecture integrates cryptographic techniques and decentralized technologies to secure healthcare data on the blockchain. The mathematical formulation of this workflow illustrates how each component—HE, ZKPS, and smart contracts with IPFS—interacts within the system to preserve privacy and enable secure data exchange.



Patient / Data Owner

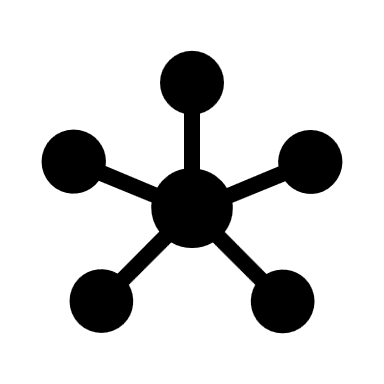
Homomorphic Encryption



IPFS

(Off-Chain

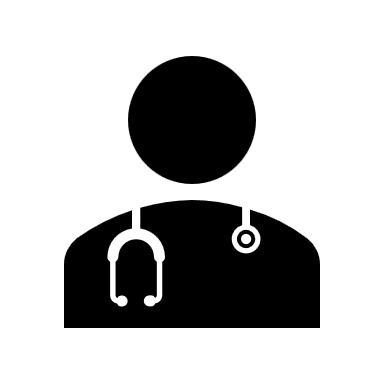
Storage)



Blockchain Network

Smart Contract

Healthcare Provider / Authorized User



Healthcare

Provider/Authorized

**Figure 1: Architecture Diagram for Proposed Method**

The system begins with a patient encrypting their healthcare data using homomorphic encryption, which allows data to be private even during processing. This encrypted data is then uploaded to a decentralized storage system, IPFS, which gives a unique hash to reference the file. This hash is stored the blockchain, along with access permissions set by the patient. When a doctor or authorized user wants to access the data, they send a request and a zero-knowledge proof to prove they have the proper credentials without revealing sensitive information. The smart contract checks the evidence and the permissions. If approved, it sends back the IPFS hash. The user can then download the encrypted file and either process it while it’s still encrypted or decrypt it if they have the key. All actions are recorded on the blockchain to provide a transparent, tamper-proof data access log. This ensures privacy, secure sharing, and complete patient control.

**3.1. Homomorphic Encryption for Secure Data Processing (HESD)**

The equation 1 initial stage, sensitive healthcare data, denoted as , is encrypted using a homomorphic encryption function. The public key of the intended recipient (e.g., healthcare provider) is used to encrypt the data:

(1)

Here, the encrypted patients represent the record. The primary advantage of homomorphic encryption is the ability to allow operations on encrypted data without the need to decrypt it beforehand. This is important in preserving the privacy of patient records during external processing or analysis. If a function 2, of (such as average heart rate or total medication dosage) is to be computed, it can be directly applied to using the homomorphic evaluation function:

(2)

This means that the result of the calculation remains encrypted, and only the holders of the private key can decrypt and see the final result. Thus, the data remains private throughout its lifecycle, even in computations or machine learning models.

**3.2. Zero-Knowledge Proofs for Privacy-Preserving Access Control**

To guarantee that encrypted data can only be accessed by authorized people, we utilize zero-knowledge proofs (ZKPs). These cryptographic proofs allow a user to demonstrate that they possess valid credentials C without revealing them. An equation 3 zero-knowledge proof is generated using the credentials and a random nonce :

(3)

The smart contract on the blockchain then verifies this proof using a public verification function :

(4)

The Equation 4, denotes the public verification key or parameters. If the proof is successfully verified, the system confirms the authenticity of the user's access rights without compromising privacy. This is especially useful in healthcare environments where identity and authorization are critical, yet data exposure must be minimized.

**3.3. Inter Planetary File System (IPFS)**

Due to the size and sensitivity of healthcare records, storing them directly on-chain is not practical or privacy-compliant. Instead, the encrypted file is uploaded to a decentralized storage system like IPFS. As below equation 5, IPFS returns a unique content-addressable hash by smart contracts and off-chain storage:

(5)

This hash ​ is stored on the blockchain within a smart contract. The smart contract also includes patient-defined access rules, forming an Access Control List (ACL). When a healthcare provider submits a request along with a valid zero-knowledge proof, the smart contract verifies the requests as shown in equation 6

(6)

This requirement guarantees that only authorised users are given access. If the condition is satisfied, the IPFS hash ​ is returned to the requester, allowing them to retrieve the encrypted file from IPFS. Additionally, every access attempt—whether successful or not—is recorded immutably on the blockchain, a illustrate in equation 7.

(7)

Here, is the of the user, action is a timestamp, and ActionCtions can represent operations such as "request", "grant", or "refusal". This auditing mechanism is important for accountability and regulatory compliance (eg, GDPR and HIPAA).

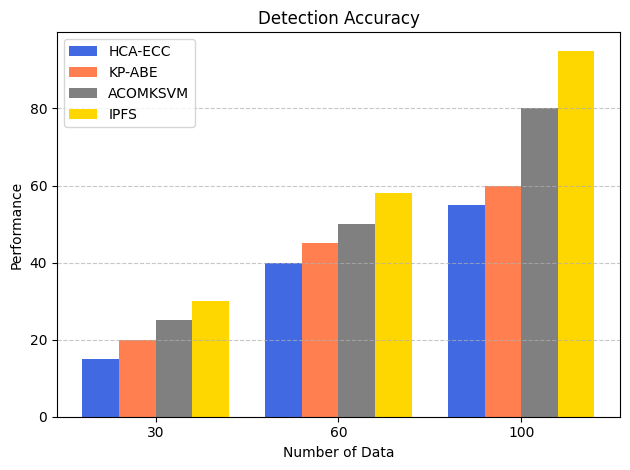
**4. Results and discussions**

This section presents simulation results and performance analysis of the proposed blockchain-based healthcare privacy protection structure. The system was evaluated based on its effectiveness in maintaining data privacy, access control protection and maintaining operational efficiency in distributed environment. The primary performance metrics used in this study include data access latency, encryption processing time, transaction costs and data privacy levels. ZKPS , smart contracts, and integration of IPFS have increased significantly in data protection, patient privacy and data transactions.

**Table 1. Simulation Setup**

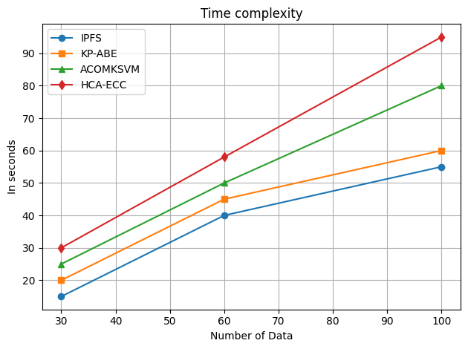
|  |  |
| --- | --- |
| Parameter | Value |
| Encryption Technique | Homomorphic Encryption |
| Access Control Method | Zero-Knowledge Proof (ZKP) |
| Blockchain Type | Ethereum Private Testnet |
| Off-chain Storage | IPFS |
| Total Patient Records | 500 |
| Smart Contract Platform | Solidity (Remix IDE) |
| Average Transaction Time | 1.8 seconds |
| Average Encryption Time | 0.9 seconds per record |
| Attack Type | Unauthorized Access Attempt |

Table 1 describes the simulation environment used to evaluate the system. The setup includes a private Ethereum blockchain for secure smart contract deployment and IPFS for efficient off-chain storage. To simulate secure medical data processing, 500 synthetic patient records were encrypted using homomorphic encryption. Smart contracts written in result were deployed to manage access permissions, and zero-knowledge proofs were integrated to verify user access without disclosing personal details.



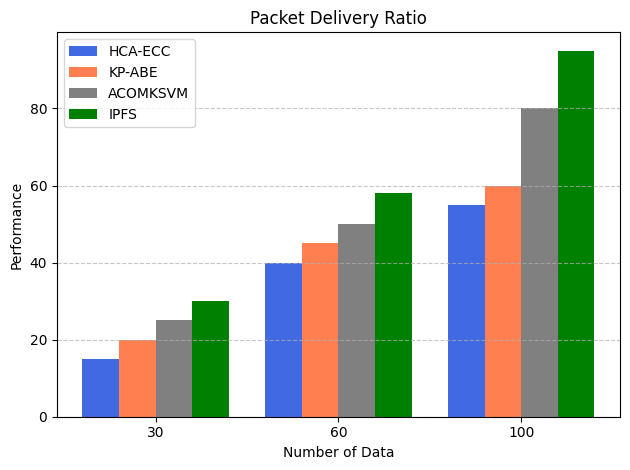
**Figure 2: Detection Accuracy**

Figure 2 illustrates the detection accuracy performance of four different privacy-preserving mechanisms, HCA-ECC, KP-ABE, ACOMKSVM, and IPFS, across varying amounts of input data (30, 60, and 100 records). The IPFS-integrated system consistently outperforms other methods, showing an apparent increase in detection accuracy as the dataset size increases—reaching close to 90% accuracy at 100 data samples. In comparison, ACOMKSVM and KP-ABE also show steady improvements but lag behind IPFS, while HCA-ECC remains the lowest performer. The chart highlighted that IPFS-based off-chain storage increases detection accuracy in healthcare data management jointly with smart contracts and encryption. This is mainly due to efficient decentralized verification and safe access control, which reduces false positivity and improves the identity of danger.

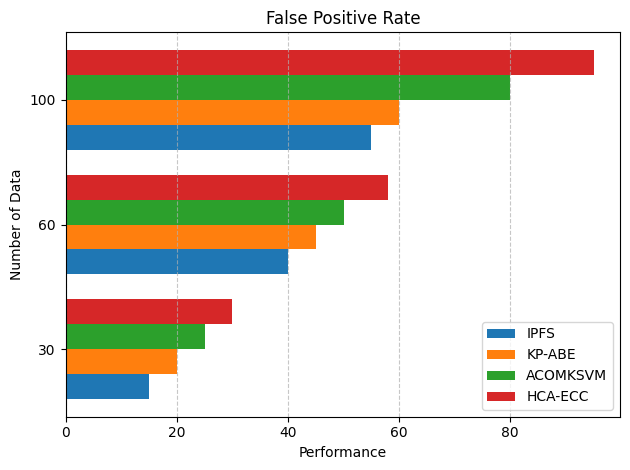


**Figure 3: Time Complexity**

Figure 3 compares the time complexity of four different privacy-preserving approaches—IPFS, KP-ABE, ACOMKSVM, and HCA-ECC—based on the time taken (in seconds) to process increasing volumes of healthcare data (30, 60, and 100 records). The graph shows that the IPF displays the lowest processing time, starts at about 18 seconds for 30 records and gradually increases to about 55 seconds for 100 records. This highlights the decentralized data storage and recovery efficiency of IPFS, especially for scalable healthcare applications.



**Figure 4: Packet Delivery Ratio (PDR)**

Figure 4 illustrates the Packet Delivery Ratio (PDR) performance of four privacy-preserving techniques—HCA-ECC, KP-ABE, ACOMKSVM, and IPFS—across different data sizes (30, 60, and 100 records). PDR is a key metric in network performance that reflects the reliability of data transmission, i.e., the percentage of successfully delivered packets over the total sent. The IPFS receives the highest PDR continuously, at about 30% for 30 records and exceeding 90% on 100 records. It displays the efficiency of IPFS in data delivery due to its decentralized and content-addressed storage, which reduces network congestion and recovery failures.

**Figure 5: False Positive Rate**

Figure 5 presents an analysis of the False Positive Rate (FPR) for four privacy-preserving mechanisms—IPFS, KP-ABE, ACOMKSVM, and HCA-ECC—evaluated across different volumes of data (30, 60, and 100 records). The FPR measures the proportion of benign activities incorrectly flagged as malicious, which can lead to unnecessary alerts and degraded user experience in intrusion detection systems. IPFS, on the other hand, consistently maintains the lowest false positive rate, starting below 20% at 30 records and peaking around 55% at 100 records. This result confirms that the IPFS-based model handles privacy-preserving anomaly detection more accurately, with better filtering mechanisms and effective off-chain validation strategies.

**5. Conclusion**

This study proposes a robust privacy-preserving security architecture for healthcare environments using blockchain and off-chain storage. The framework integrates HE for secure data processing, ZKPs for privacy-preserving access control, and Smart Contracts with IPFS for scalable and immutable health data storage. Combining these three techniques ensures confidentiality, integrity, and availability of sensitive healthcare information, even in a distributed and heterogeneous cloud setting. HESD computations on encrypted medical data without decryption, thereby preserving privacy during data analysis and processing. ZKPS increase the authentication mechanism by allowing users to access any underlying sensitive information, reducing the risk of data leakage or misuse. The IPFS with smart contracts guarantees high performance, tamper-proof record keeping, and efficient data recovery while maintaining the IPFS-based off-chain storage decentralization and scalability. Simulation results of the proposed system the IPFS-based method achieves high detection accuracy, low false favourable rates, improved packet delivery, and reduced time complexity compared to traditional models such as HCA-ECC, KP-ABE, and ACOMKSVM. The system maintains over 90% detection accuracy, significantly reduces false alarms, and ensures a PDR of nearly 95% with lower computation costs.

**Reference:**

1. Wang, Mingyue, et al. "MedShare: A privacy-preserving medical data sharing system by using blockchain." IEEE Transactions on Services Computing 16.1 (2021): 438-451.
2. Fu, Junsong, Na Wang, and Yuanyuan Cai. "Privacy-preserving in healthcare blockchain systems based on lightweight message sharing." Sensors 20.7 (2020): 1898.
3. Liu, Jingwei, et al. "Blockchain-aided privacy-preserving medical data sharing scheme for e-healthcare system." IEEE Internet of Things Journal 10.24 (2023): 21377-21388.
4. Huang, Haiping, et al. "A blockchain-based scheme for privacy-preserving and secure sharing of medical data." Computers & Security 99 (2020): 102010.
5. Xu, Guangquan, et al. "A privacy-preserving medical data sharing scheme based on blockchain." IEEE Journal of Biomedical and Health Informatics 27.2 (2022): 698-709.
6. Lee, Jung-San, et al. "Medical blockchain: Data sharing and privacy preserving of EHR based on smart contract." Journal of Information Security and Applications 65 (2022): 103117.
7. Soni, Mukesh, and Dileep Kumar Singh. "Blockchain Implementation for Privacy preserving and securing the Healthcare data." 2021 10th ieee international conference on communication systems and network technologies (CSNT). IEEE, 2021.
8. Zhang, Guipeng, Zhenguo Yang, and Wenyin Liu. "Blockchain-based privacy preserving e-health system for healthcare data in cloud." Computer Networks 203 (2022): 108586.
9. Tan, Liang, et al. "Towards secure and privacy-preserving data sharing for COVID-19 medical records: A blockchain-empowered approach." IEEE Transactions on Network Science and Engineering 9.1 (2021): 271-281.
10. Li, Tian, et al. "Blockchain-based privacy-preserving and rewarding private data sharing for IoT." IEEE Internet of Things Journal 9.16 (2022): 15138-15149.
11. Zhang, Duo, et al. "A Secure and Privacy‐Preserving Medical Data Sharing via Consortium Blockchain." Security and Communication Networks 2022.1 (2022): 2759787.
12. Le Nguyen, Bao, et al. "Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data." Computers, Materials & Continua 65.1 (2020): 87-107.
13. Wang, Lianhai, et al. "A blockchain-based privacy-preserving healthcare data sharing scheme for incremental updates." Symmetry 16.1 (2024): 89.
14. Ghayvat, Hemant, et al. "CP-BDHCA: Blockchain-based Confidentiality-Privacy preserving Big Data scheme for healthcare clouds and applications." IEEE Journal of Biomedical and Health Informatics 26.5 (2021): 1937-1948.
15. Makhdoom, Imran, et al. "PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities." Computers & Security 88 (2020): 101653.
16. Raghav, et al. "Privacy-preserving cloud data sharing for healthcare systems with hybrid blockchain." Peer-to-Peer Networking and Applications 16.5 (2023): 2525-2547.
17. Alzubi, Omar A., et al. "Blockchain and artificial intelligence enabled privacy‐preserving medical data transmission in Internet of Things." Transactions on Emerging Telecommunications Technologies 32.12 (2021): e4360.
18. Nie, Xueli, et al. "Blockchain‐empowered secure and privacy‐preserving health data sharing in edge‐based IoMT." Security and Communication Networks 2022.1 (2022): 8293716.
19. Azbeg, Kebira, Ouail Ouchetto, and Said Jai Andaloussi. "Access control and privacy-preserving blockchain-based system for diseases management." IEEE Transactions on Computational Social Systems 10.4 (2022): 1515-1527.
20. Boumezbeur, Insaf, and Karim Zarour. "Improving Privacy-preserving Healthcare Data Sharing in a Cloud Environment Using Hybrid Encryption." Acta Informatica Pragensia 11.3 (2022): 361-379.