Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.065156

ARTICLE

Blockchain and Smart Contracts: An Effective Approach for the Transaction Security & Privacy in Electronic Medical Records

Amal Al-Rasheed[1], Hashim Ali[2,*], Rahim Khan[2,*] and Aamir Saeed[3]

[1]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh, 11671, Saudi Arabia

[2]Department of Computer Science, Abdul Wali Khan University, Mardan, 23200, Pakistan

[3]Department of Computer Science and IT, University of Engineering and Technology Peshawar, Jalozai Campus, Peshawar, 25120, Pakistan

*Corresponding Authors: Hashim Ali. Email: hashimali@awkum.edu.pk; Rahim Khan. Email: rahimkhan@awkum.edu.pk

Received: 05 March 2025; Accepted: 16 July 2025; Published: 23 September 2025

ABSTRACT: In the domain of Electronic Medical Records (EMRs), emerging technologies are crucial to addressing longstanding concerns surrounding transaction security and patient privacy. This paper explores the integration of smart contracts and blockchain technology as a robust framework for securing sensitive healthcare data. By leveraging the decentralized and immutable nature of blockchain, the proposed approach ensures transparency, integrity, and traceability of EMR transactions, effectively mitigating risks of unauthorized access and data tampering. Smart contracts further enhance this framework by enabling the automation and enforcement of secure transactions, eliminating reliance on intermediaries and reducing the potential for human error. This integration marks a paradigm shift in management and exchange of healthcare information, fostering a secure and privacy-preserving ecosystem for all stakeholders. The research also evaluates the practical implementation of blockchain and smart contracts within healthcare systems, examining their real-world effectiveness in enhancing transactional security, safeguarding patient privacy, and maintaining data integrity. Findings from the study contribute valuable insights to the growing body of work on digital healthcare innovation, underscoring the potential of these technologies to transform EMR systems with high accuracy and precision. As global healthcare systems continue to face the challenge of protecting sensitive patient data, the proposed framework offers a forward-looking, scalable, and effective solution aligned with the evolving digital healthcare landscape.

KEYWORDS: Smart-contracts; internet of things; privacy; security; blockchain; EMR

1 Introduction

Blockchain, Artificial Intelligence, and the Internet of Things make up Industry 4.0. In the era of digitization, the healthcare sector is undergoing a paradigm shift with the integration of advanced technologies. Among these, EMR plays a crucial role in transforming the way patient data is stored and managed [1,2]. However, the increasing reliance on digital platforms raises concerns about the security & privacy of sensitive healthcare transactions. This paper describes the potential of leveraging smart contracts and blockchain technology to address the challenges associated with transaction privacy & security in EMRS. Blockchain and Smart Contracts offer a unique synergy to improve integrity, privacy, and security of healthcare transactions. IoT devices are connected via a cyber-physical system [3]. For effective monitoring of the health data-intensive applications in real-time, predictive maintenance can be employed. Moreover, Smart intelligence

capabilities embedded into each program can help policymakers find data-driven solutions to pressing concerns, contributing to the advancement of Sustainable Development Goals (SDGs). Blockchains are triggered by the Smart contracts to perform the tasks through a predefined activity [4]. Smart contract-based approaches automate transportation processes, minimizes human related mistakes, and increasing efficiency. Privacy is also a key concern in transportation, particularly with the increasing use of connected vehicles. Through blockchain and IoT, sensitive data such as location and personal information can be securely encrypted and stored on a decentralized platform [5]. Smart contracts can be used to restrict access to this data, ensuring that only authorized parties have access to it [6]. Through smart contract-based approaches, transportation processes become automated and efficient while risks are reduced. Moreover, a mature model is used to interact with gateway, edge or cloud [7,8]. Hybrid blockchain, often referred to as consortium blockchain, presents a compelling fusion of both private and public blockchain features. Homomorphic encryption, a cornerstone feature introduced, encrypts user data at the source and subsequently outsources it to the cloud. This strategic approach empowers the system to perform a multitude of statistical and machine-learning operations on encrypted data, thereby unlocking new avenues for advanced analysis while upholding data confidentiality. Applications of the industrial IoT has been rapidly grown and led to significant rise in scalability of the active smart devices [9]. These devices are equipped with dedicated sensor units capable of capturing real-time industrial data. This transformation in system interactions with both physical and digital elements is driven by industrial progress and technological innovation. Currently, a center-oriented architecture is commonly employed to transmit data (real time) and manage key IoT components, i.e., management of the identity [10]. Adaptive self-configuration is a key mechanism to enhance the efficiency and resilience of the IoT ecosystem, mitigating the risks associated with a single failure point. Expanding beyond the current paradigm, there is a growing anticipation of the integration of IoT applications over the upcoming 6G network. The sixth generation of wireless technology is expected to bring about transformative changes, offering higher speeds, lower latency, and increased capacity [11]. The article discusses a federated learning scheme that is based on fuzzy and ensemble-oriented for the recognition of the EEG emotion on the IoMT, allowing privacy-preserving and accurate analysis. It also discusses IoMT data fusion techniques, points out major security issues, and suggests possible solutions such as standardization and integration with blockchain [12]. Leveraging the capabilities of the 6G network, IoT applications are confident to explore effectiveness in terms of performance, scalability, and commercial viability. Although blockchain-enabled frameworks are available to ensure privacy and security of the patients' data, however majority of these solutions haven't considered the overall impact of smart contacts. Secondly, existing schemes are domain-oriented and have a degraded performance in other environments.

This paper makes a significant contribution by thoroughly investigating the potential impact of smart contracts and blockchain technology on the levels of security & privacy within transportation. The utilization of blockchain and Internet of Things (IoT) technologies establishes a decentralized infrastructure for storing and sharing data, thereby offering a promising avenue to enhance the overall security of transportation systems. The integration of smart contract-based approaches further enhances operational efficiency by automating processes, thereby reducing the potential for human error and streamlining various aspects of transportation management. The paper goes beyond theoretical exploration and delves into practical applications of these technologies within the transportation sector. Specific use cases, such as cargo tracking and driver credential verification, are meticulously discussed. This not only sheds light on the versatility of blockchain and smart contracts but also underscores the potentially transformative benefits they can bring to core transportation processes. The emphasis on how smart contracts can specifically augment these processes adds depth to the understanding of their practical applications. In addition to highlighting the positive aspects, the paper engages with the challenges associated with the widespread adoption of these

technologies in the transportation domain. By addressing these challenges, the paper offers valuable insights that can serve as a foundation for guiding future research and development efforts. This forward-looking approach ensures that the exploration of blockchain and IoT in transportation is not only theoretically sound but also cognizant of the real-world hurdles that need to be overcome for successful implementation.

1. The design of a blockchain and trust-aware security approach for wearable devices in the Internet of Things.
2. Effective utilization of the smart contacts and elliptic curve in making a privacy-preserving networking infrastructure for the Internet of Things, especially in smart hospitals.
3. Every device in the proposed smart contact-based network is embedded with appropriate sensors and 6-G based wireless communication modules.
4. Finally, data values such as bio-metric, video, and speech are considered in the proposed setup.

The rest of the manuscript is organized as follows.

In Section 2, the proposed model is described in detail, along with the necessary algorithms and other parameters. A detailed discussion of the proposed module is available in Section 3. Simulation results are presented in Section 4 of the paper where various important metrics are considered. Finally, concluding remarks are given.

2 Proposed Model

The proposed methodology presents a comprehensive approach, encompassing a series of systematic steps meticulously designed to yield reliable and accurate system outputs. Initially, IoT fortifies security measures and ensures the utmost protection of sensitive data; the information undergoes a meticulous process of homomorphic encryption in the subsequent stage. Homomorphic encryption, renowned for its robust security protocols, adds a layer of protection, rendering the transmission of sensitive information in an encrypted form impervious to unauthorized access. This encrypted data is then securely outsourced to the cloud, where it is meticulously stored and accessed for further processing, maintaining data confidentiality and integrity during entire life cycle. The integration of homomorphic encryption in this process is not merely a precautionary measure but a strategic choice aimed at expanding the system's capabilities. By enabling various deep learning and statistical operations on encrypted data, homomorphic encryption empowers the system to conduct sophisticated analyses while safeguarding the privacy and confidentiality of sensitive information. This innovative approach ensures that even during data processing, the privacy of individuals and the confidentiality of their information remain paramount. Following the secure transmission and storage of data, the proposed framework seamlessly transitions to the pivotal step of feature extraction. Feature extraction plays a pivotal role in distilling essential insights from the amassed data, encompassing crucial attributes, i.e., height, sex, age, heart rate, and weight. This meticulous process transforms raw data into meaningful information, laying the groundwork for subsequent analysis and classification. In our proposed methodology, we have employed Support Vector Machines to separate data and users based on the extracted features. SVM, revered for its robustness and efficiency, augments the system's ability to discern intricate patterns and interpret data accurately. By harnessing the power of SVM, our methodology facilitates effective interaction with the system, enabling it to categorize and analyze data with precision and agility.

The incorporation of SVM adds a layer of intelligence to the system for ensuring informed decisions based on the extracted features. This enhances the overall efficacy of the methodology, empowering it to derive actionable insights and facilitate seamless decision-making processes. As a result, our approach not only ensures the security and confidentiality of data but also enhances the system's analytical capabilities, and leads to advancement of the transformation activity in data-driven applications. IoT data is systematically

gathered from sensors distributed across the network. These data are then transmitted to the cluster head, which acts as a central hub for data aggregation and management. This initial phase establishes the foundation for the subsequent processes, laying the groundwork for a cohesive and streamlined flow of information within the system. Building upon the data collection phase, Step 2 involves a crucial blockchain-based data transaction. During this step, the collected data undergoes a meticulous process of verification and authentication through numerous IoT edge devices. This blockchain-based transaction not only enhances the security of the data but also ensures a transparent and tamper-resistant record of the information flow. This step is instrumental in establishing trust and integrity within the system.

To fortify the security measures and ensure utmost protection of sensitive data, information undergoes a meticulous process of homomorphic encryption in the subsequent stage. Homomorphic encryption, renowned for its robust security protocols, adds a layer of protection, rendering the transmission of sensitive information in an encrypted form impervious to unauthorized access. This encrypted data is then securely outsourced to the cloud, where it is meticulously stored and accessed for further processing, maintaining the confidentiality and integrity of the data throughout its life cycle. The integration of homomorphic encryption is not merely a precautionary measure but a strategic choice to expand the capabilities of the systems.

In the proposed methodology, SVM classifies users and data based on the extracted features. SVM, revered for its robustness and efficiency, augments the system's ability to discern intricate patterns and interpret data accurately. By harnessing the power of SVM, our methodology facilitates effective interaction with the system, enabling it to categorize and analyze data with precision and agility. The incorporation of SVM adds a layer of intelligence to the system for ensuring informed decisions based on the extracted features. This enhances the overall efficacy of the methodology, empowering it to derive actionable insights and facilitate seamless decision-making processes. As a result, our approach not only ensures the security and confidentiality of data but also enhances the system's analytical capabilities, paving the way for transformative advancements in data-driven applications.

Finally, the output generated by the system undergoes a rigorous validation process in the concluding step. This validation process is executed through a dedicated validation model, ensuring the reliability and accuracy of the results derived from the proposed methodology. This final step is crucial in verifying the integrity of the entire process, providing assurance that the outcomes are consistent, trustworthy, and align with the intended objectives of the system. In summary, the proposed methodology represents a holistic and systematic approach to handling IoT data, incorporating elements of blockchain, homomorphic encryption, feature extraction, and machine learning for robust and secure processing. The sequential steps outlined in the schematic diagram guide the system through a well-defined process, ultimately leading to validated and dependable outcomes. As the realm of data processing and IoT applications continues to evolve, this methodology stands as a robust framework, offering a reliable solution to resolve problems with data security, integrity, and meaningful interpretation.

2.1 System Model

Incorporation of blockchain in healthcare holds significant promise for enhancing transaction security & privacy, particularly in the context of electronic medical records (EMRs). Smart contracts are very crucial for this transformation by facilitating transactions on a blockchain without third party, i.e., mediators. In the domain of EMRs, smart contracts act as a safeguard to make sure that patients data is accessed and shared exclusively by authorized parties. The system model for employing smart contracts and blockchain in EMR transactions comprises multiple integral components. Firstly, there is the EMR system itself, housing patient data that is accessed by healthcare providers. Secondly, the decentralized blockchain network serves as a secure ledger, meticulously recording all transactions. Lastly, smart contracts automate the execution of

transactions on the blockchain. The EMR system shoulders the responsibility of creating and storing patient data, encompassing crucial information such as medical history, test results, prescriptions, and other relevant details. It is imperative for the EMR system to be meticulously designed to guarantee the security, accuracy, and currency of patient data. Access to the EMR system should be restricted solely to authorized users, predominantly healthcare providers, and fortified by robust authentication and authorization mechanisms. On the other hand, the blockchain network is entrusted with maintaining a secure and tamper-proof ledger that chronicles all transactions related to EMRs. Decentralized blockchain ensures that the ledger is resistant to changes or updates carried out by intruders, thereby reinforcing the integrity and transparency of the healthcare transactions recorded within the system. In essence, the combination of blockchain and smart contracts introduces a layer of trust, security, and efficiency to EMR transactions, significantly useful for both healthcare owner and patients. The ledger in question is dispersed across numerous nodes, a design ensuring that no single entity wields control over the network. Transactions occurring on the blockchain undergo validation through a mechanism (preferably consensus), ensuring all member devices agreement related to the ledger's status. This arrangement renders it practically implausible for any individual or entity to monopolize data sharing, thereby securing patient data access exclusively for authorized parties. The focus of this section is to establish an industrial automation authentication system that is not only reliable but also straightforward. The testing of private keys for security, facilitated by a multisig-compatible contract, ensures stringent control to prevent unauthorized access. In the realm of industrial automation, a cash on leave intelligent approach is proposed to explore the computational processes of IoT devices. Comprising myriad tiny sensors, computers, cloud, edge devices, RFID, and WiFi. IoT generates vast amounts of data. Due to the sheer volume of this data, security breaches and mismanagement are potential threats. The multisig-compatible contract scrutinizes every facet of a transaction, encompassing quality control, mechanical techniques, and decision-making processes. To facilitate independent decision-making, the intelligent model leverages traffic patterns. A smart contract analyzes the fundamental operational operations of an IoT device, optimizing the overall system efficiency. Cloud computing, by providing on-demand resource allocation regardless of location and time, stands as a pivotal asset in modern organizational frameworks. The proposed model focuses on elucidating the functionality of three pivotal algorithms: Algorithm 1 for policy management, Algorithm 2 for attribute checking, and Algorithm 3 for cluster head selection. Algorithm 1 is used to create, update, and delete records of entities, i.e., patients, doctors, and paramedical staff. Secondly, Algorithm 2 initiates the record management process of the proposed smart contact and blockchain based system. This algorithm ensures that a device is trustworthy or not. Cluster head selection is a critical process in the resources constraint domain, therefore, Algorithm 3 is designed to perform this task in a professional way. Additionally, CH serves as a sub data collection point for the server module in the IoMT and every wearable device resides in the coverage area communicate via the dedicated CH.

Algorithm 1: Insert, modify, and delete records

1 Function createRecord id, name, status **Data:** ID, Name, Status
Result: New Record
2 NewRecord ← new Record()
3 NewRecord.ID ← id
4 NewRecord.Name ← name
5 NewRecord.Status ← status
6 return NewRecord
7 Function updateRecordexistingRecord, newName, newStatus **Data:** Existing Record, New Name, New Status

(Continued)

Algorithm 1 (continued)

```
8 if existingRecord is not null then
9       existingRecord.Name ← newName
10      existingRecord.Status ← newStatus
11 else
12      Record not found
13
14 Function revokeRecord(records, id) Data: List of Records, ID
15 recordToDelete ← findRecordById (records, id)
16 if recordToDelete is not null then
17      records.remove(recordToDelete)
18 else
19      Record not found
20 Functionfind RecordById (records, id) Data: List of Records, ID
21 foreach record in records do
22      if record.ID = id then
23          return record
24 return null
25 Example Usage:
26 records ← []
27 newRecord ← createRecord(1, "John Doe", "Active")
28 records.append(newRecord)
29 recordToUpdate ← findRecordById (records, 1)
30 updateRecord (recordToUpdate, "Jane Doe", "Inactive")
31 revokeRecord (records, 1)
```

Algorithm 2: Initialization and record management algorithm

```
1 Function: Initialization
2     PHL ← PHL Trustworthy wearable device
3     σ ← H(h, σ, r)
4     w ← H(h, d, N)
5     if σ is True then
6         w ← u.t ∈ G
7         u ← e(S, P) ∈ G
8         if PHL is a valid device then
9             CreateRecords (Patient_ID, Patient_REC, BN)
10        else
11            UpdateRecords (Patient_ID, Patient_REC, BN)
12        ReadRecords (Patient_ID, Patient_REC, C_ID, L_ID, BN)
13    else
14        NotExist (Patient_ID)
15    if Visit (Patient_ID, C_ID, L_ID, BN) then
16        MPatient_ID ← MedRecord (Patient_ID)
```

(Continued)

Algorithm 2 (continued)

```
17        if MPatient_lD, PHL, BN then
18            GrantRecords (MPatient_ID, C_ID, L_ID, BN)
19        else
20            (C_ID, L_ID) ← Notify (Not Found)
21    if h2 = H2(W0 ... Wn, N) Success then
22        else Failure
```

Algorithm 3: Cluster head selection algorithm

```
1 Function: Clinician (Cid):
2     while True do
3         if CIDBN then
4             if Granted MPatient_ID C_ID then
5                 ReadRecords(C_ID, PREC_ID, MPatient_ID, BN)
6                 UpdateRecords(C_ID, PREC_ID, MPatient_ID, BN)
7             else
8                 WriteRecords(C_ID, MPatient_ID, B_N)
9                 ReadRecords(C_ID, L_ID, BN)
10        else
11            NotExist(C_ID)
```

2.2 Alternate Key: Elliptic Curve Cryptography (ECC)-Based Methodology

The proposed methodology leverages ECC ensure distribution of the secret key and digital signature exchange, thereby strengthening overall system security and user trust. Additionally, the integration of ring signatures further enhances user anonymity and confidence in the system [13,14]. A systematic mathematical methodology of the proposed approach, which integrates ring signatures and Elliptic Curve Cryptography (ECC), is presented below: In ECC, let a, b, x, and y be rational numbers ($\mathbb{Q}$). $P(x, y)$ lies on an elliptic curve if it satisfies the corresponding elliptic curve Eq. (1). $Q(x, y)$ represents the inverse of $P(x, y)$, denoted as $Q = -P$. Now, consider two distinct points on the elliptic curve defined by parameters a and b: P(x_1, y_1) and Q(x_2, y_2), where $P \neq Q$. Let a line l pass through both P and Q, intersecting the curve at a third point $R_0 = (x_3, y)$. Reflecting R_0 across the x-axis yields the point R = (x_3, y_3), which is defined as the sum $R = P + Q$. The set of all such points on the elliptic curve defined by a and b, together with the point at infinity $\mathcal{O}$, generate an extra group (preferably cyclic) of the prime order q.

$$E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q | y^2 = x^3 + ax + b \mod q\} \cup \{\mathcal{O}\}$$

where $\mathbb{F}_q$ denotes the finite field of prime order q, and $E(\mathbb{F}_q)$ represents the set of points that satisfy the elliptic curve equation modulo q. The ring signature mechanism plays a crucial role in ensuring trust and anonymity within the system. It allows an individual within a group to authenticate a message for the entire group while keeping their identity hidden, ensuring both confidentiality and privacy are maintained. In a ring signature scheme, any group member can generate a signature using their private key, that is verified through the public keys of all group members. However, it is computationally infeasible to identify the specific member who generated the signature, ensuring the anonymity of the signer. Mathematically, a ring signature can be expressed as follows:

Let $PK_1, PK_2, \ldots, PK_n$ be the public keys of n users in the group, and let SK_i denote the private key of user i. To generate a ring signature for a message m, user i computes: $s = \text{RingSign}(m, SK_i, PK_1, PK_2, \ldots, PK_n)$. Where RingSign is the ring signature generation algorithm, that is verified using the public keys of all users in the group.

Fig. 1 is a graphical representation of the blockchain and smart contract based access control. This illustration serves as a visual guide to understanding the intricate processes involved in securing and managing data access within the system. The top portion illustrates various details about the various access control measures. Various user attributes, i.e., private key, gender, age, height, weight, and location, are considered during the access control process. The access control mechanism ensures that only users with the appropriate and authorized attributes are granted access to EMR. In the middle section, there may be a depiction of the homomorphic encryption (HE) process applied to Internet of Things (IoT) data. This aligns with the framework's strategy of encrypting data before outsourcing it to the cloud. HE enables the performance of various statistical operations on encrypted data. The lower part illustrates the integration of Blockchain technology. Blockchain acts as a decentralized and secure ledger that records all transactions, including those related to access control and data outsourcing. The proposed hybrid mechanism automate and enforce policies related to the access control, ensuring that only users with the appropriate attributes gain access. The arrows or flow lines in the figure likely show the end-to-end process, demonstrating how data moves through the various stages from the initiation of access control checks, to HE of IoT data, and finally to the secure outsourcing of data through Blockchain. Equations encapsulate the homomorphic encryption employed in the proposed approach. The function H1 is the homomorphic encryption function responsible for converting plain text into ciphertext, denoted as Cs. Homomorphic encryption is a cryptographic technique that enables the encryption of data, allowing it to be outsourced to the cloud while still facilitating the performance of various statistical operations on the encrypted data. This contributes significantly to enhanced privacy and security measures. In Fig. 2, a comprehensive depiction of the end-to-end process of access control and encryption throughout the network is presented. The proposed framework strategically employs homomorphic encryption to secure IoT data for outsourcing to the cloud. By utilizing homomorphic encryption, the framework gains the ability to perform a wide range of operations on encrypted data, ensuring strong security & privacy protections. Additionally, the access control mechanism evaluates user attributes such as username, ID, age, gender, location, and height. This assessment is critical for determining access to Electronic Health Records (EHR) or Electronic Medical Records (EMR). If a user's attributes match the required criteria, access is granted through the use of smart contracts; otherwise, access is denied. This process is visually represented to enhance understanding, illustrating how data flows through various stages of the network while highlighting the effectiveness of both homomorphic encryption and access control measures in maintaining secure and regulated data access.

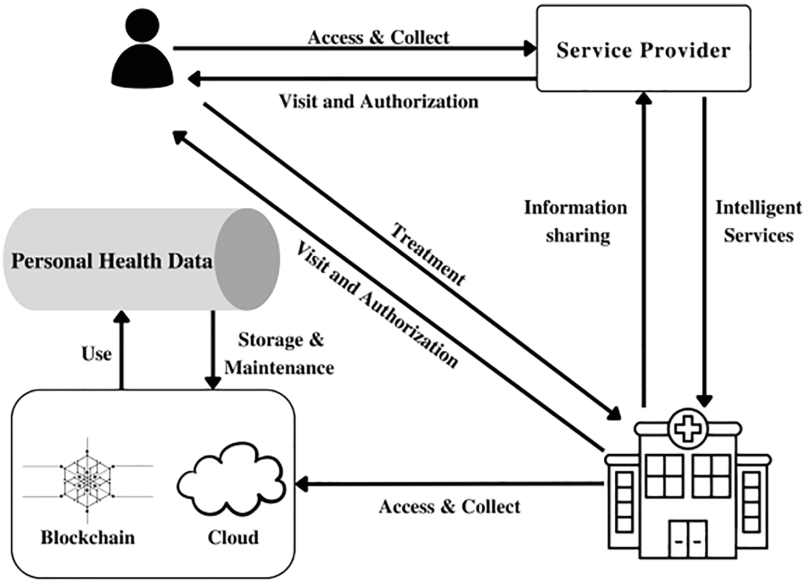

Figure 1: Proposed outsourcing and access control

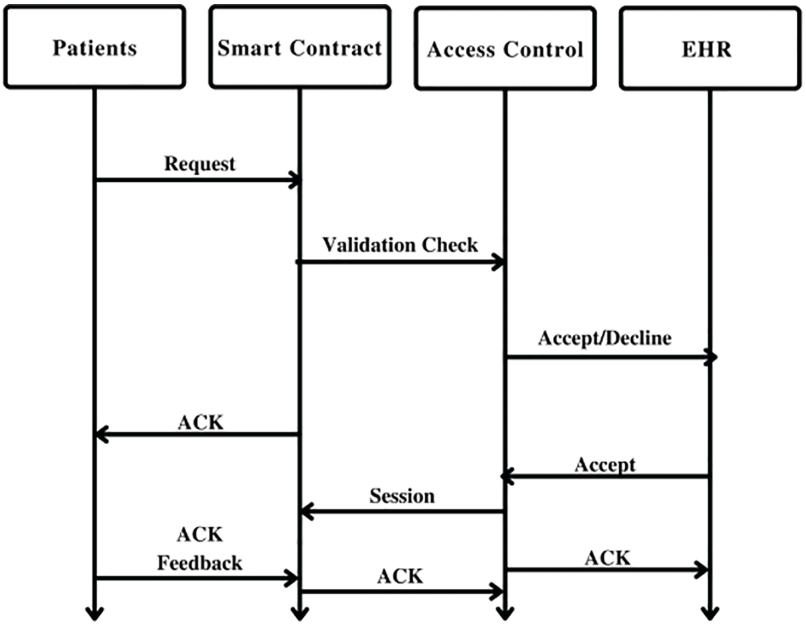

Figure 2: Data flow through proposed network

Modeling and Design of the Security Protocol

The process of mathematical modeling and designing security protocols for IoT systems is a multifaceted endeavor that unfolds across several distinct phases. Each of these phases plays a crucial role in enabling users to securely access and interact with the IoT system, whether it's for reading data from sensors or transmitting information to the network. This initial phase involves a comprehensive analysis of the system's requirements and objectives. It entails identifying the specific functionalities that users need to perform within the IoT environment, such as reading sensor data or sending commands to actuators. Additionally, potential security

threats and vulnerabilities are identified during this stage to inform subsequent security protocol design. In this phase, the architectural framework of the IoT system is designed. This includes defining the structure of the network, specifying the roles and responsibilities of different system components, and outlining the communication protocols that will be utilized. Security considerations are integrated into the architectural design to ensure that the system is resilient to potential cyber threats. Mathematical modeling plays a pivotal role in ensuring the integrity and security of data transmission within the IoT system. This phase involves the development of mathematical algorithms and models that govern various aspects of data encryption, authentication, and access control. Mathematical techniques such as cryptography are employed to safeguard sensitive information from unauthorized access or tampering. Building upon the mathematical models developed in the previous phase, the security protocols for the IoT system are meticulously designed in this phase. These protocols define the mechanisms for authenticating users, encrypting data, and enforcing access control policies. Additionally, measures for detecting and mitigating security breaches, such as intrusion detection systems, may be incorporated into the protocol design. Once the security protocols have been designed, they are implemented within the IoT system's infrastructure. This involves integrating the protocols into the system's software and hardware components, ensuring compatibility with existing technologies and standards. Rigorous testing is conducted to verify the efficacy and reliability of the security measures, including penetration testing and vulnerability assessments. The final phase involves deploying the IoT system into operational environments and ensuring its ongoing maintenance and support. Regular updates and patches are applied to address newly discovered security vulnerabilities and adapt to evolving threats. Continuous monitoring and auditing of the system's security posture are essential to detect and respond to potential security incidents promptly.

Throughout these phases, a systematic approach is employed to address the complex challenges associated with securing IoT systems while enabling users to access and utilize the system's capabilities effectively.

1) System Setup

During it, the system initializes the necessary input parameters required for generating digital signatures and authenticating users. The step-by-step procedure of this phase is outlined below:

Setup(α): Begin by selecting a security parameter α. Let G_1 and G_2 be two multiplicative groups (1), and assume that g_1 and g_2 are generators of the group G_1 (2).

2) Encryption

In the proposed setup, the decision to choose ring signatures over group signatures or AES is rooted in the distinct advantages offered by this cryptographic technique. Group signatures may introduce potential vulnerabilities associated with a single group authority. On the other hand, the AES, while widely employed, may have limitations when it comes to ensuring the robustness required for certain security scenarios. By leveraging ring signatures, we not only bolster the security of our key exchange process but also pave the way for a more resilient and adaptive security architecture. The decentralized nature of ring signatures aligns seamlessly with the distributed and dynamic nature of modern transaction systems, minimizing collusion related risks and unauthorized access. In essence, our approach to transaction security is characterized by a strategic combination of attribute-based encryption and ring signatures, ensuring a multi-faceted defense against potential threats. This not only enhances the confidentiality and integrity of transactions but also contributes to the overall resilience of our security framework in the face of evolving cybersecurity challenges.

$$[(2+n)K+1]C_{ex} + (2K+1)C_m + (2K+1)C_m \tag{1}$$

$$Y_n = \sum_{x=0}^{n} \frac{x - x_j}{x_i - x_j} \tag{2}$$

2.3 Decryption

The complexity equation for the decryption is given below:

$$T = O(K \cdot n \cdot C)$$

where: -T represents the decryption time complexity. -K denotes the number of Certificate Authorities involved in key exchange. -n signifies the size of the message being decrypted. -C represents the ciphertext, the encrypted form of the message.

This equation highlights the linear relationship between decryption time complexity and key parameters such as the number of Certificate Authorities and message size. As the number of Certificate Authorities increases or the size of the message grows, the decryption time complexity proportionally scales, necessitating additional computational resources for timely decryption.

$$[(n+1)K+1]C_p + nKC_e + [3+(2+n)K]C_m \tag{3}$$

$$X = Q_k \in IC_e(C_2, D_k, u), \quad Y = e(C_3, D_{1k}, u) \tag{4}$$

$$S_k = Q_{ak,j} \in A_k \cap meC_{k,j},\ D_{jk}, u\delta_{ak,j},\ \tilde{A}_{jm}(0) \tag{5}$$

$$m = C_1 \frac{X}{Y} Q_k \in IC_s. \tag{6}$$

2.4 Hyperledger Fabric Configuration

The test setup used the Hyperledger Fabric official test network, which is intended for development and testing. Some important configurations are: The test network consists of two Wards (ward-I and II) and one server for ordering. One-node Raft ordering service defined to control the ordering and consensus of the transactions. Cryptogen tool is utilized to create cryptographic material, bypassing the use of TLS Certificate. mychannel is established to enable communication between the peer organizations. The network.sh script is utilized to deploy chaincode (smart contracts) on the channel. The goleveldb state database is used by default. The whole network is containerized by using Docker Compose, which guarantees isolated and reproducible environments for each part. This arrangement facilitates the emulation of a permissioned blockchain network, allowing the verification of smart contracts and transactions flows in a testing environment.

2.5 Ethereum Test Network Configuration

For the Ethereum part, the test environment, we have implemented smart contracts on an Ethereum test network to test interoperability and security functionalities. The main points are: Rinkeby is used to copy actual blockchain interactions without payment. Smart contracts were created with Solidity and tested with frameworks such as Truffle or Hardhat. Ganache is used to build a personal Ethereum blockchain for quick testing and development of the underlying system. MetaMask is set up for communication with deployed smart contracts, enabling transaction signing and handling. Security features, including access control and data integrity, are tested by emulating various attack vectors. Furthermore, it is validated that smart contracts respond correctly under different conditions.

2.6 Security Analysis

Data security within smart healthcare systems is a critical priority due to their heavy reliance on interconnected Internet of Things (IoT) devices. These devices continuously generate vast amounts of data, which is saved in the cloud and shared among the distributed networks. The repercussions of a potential cyber-attack targeting a healthcare domain, i.e., preferably a smart system, are severe, potentially disrupting its core functionalities, including the generation and distribution of electricity. Apart from substantial financial losses, such attacks can trigger operational failures, result in power outages, lead to the theft of crucial data, and even culminate in complete security breaches. Despite the integration of machine learning into cybersecurity practices, addressing the distinct demands of this field, particularly in managing the immense volume of data traversing numerous networks within a smart grid, necessitates unique approaches and theoretical perspectives. A diverse array of conceivable threats, including evasion identification, leakage of information, tampering, denial of service, repudiation, and extended privilege, are meticulously examined. The STRIDE framework serves as a foundational tool for identifying and categorizing attack vectors, enabling cybersecurity experts to develop robust defenses against potential threats. Furthermore, leveraging the renowned industrial framework known as MITRE ATTACK, researchers meticulously scrutinize threats, i.e., techniques, tactics, and procedures. Through these comprehensive approaches, our framework endeavors to bolster the security of smart healthcare systems and effectively mitigate the risks posed by potential cyberattacks.

In conclusion, the security of data within smart healthcare systems remains an ongoing concern, necessitating proactive measures and sophisticated strategies to safeguard against evolving cyber threats. By adopting a multi-faceted approach that integrates advanced technologies, threat modeling techniques, and industry frameworks, we aim to fortify the resilience of the healthcare domain and expand its ability to withstand potential cyberattacks, thereby ensuring the integrity and confidentiality of sensitive medical data.

Let's break down the equation step by step:

1. Initial Expression:

$$\hat{e}\left(T_{Q_1}, \sum_{i=1}^{t} C_i\right) = \hat{e}\left(mP, \sum_{i=1}^{t}(vh_i + uf_i)\right)$$

In this initial expression, T_{Q_1} is paired with the summation of C_i, where C_i is a collection of terms involving v, h_i, u, and f_i. This essentially represents a pairing between the target element T_{Q_1} and a set of elements derived from mP, v, h_i, u, and f_i.

2. Rearrangement of Terms:

$$= \hat{e}\left(mP, v\sum_{i=1}^{t} h_i + u\sum_{i=1}^{t} f_i\right) \qquad = \hat{e}\left(mP, v\sum_{i=1}^{t} h_i\right) \cdot \hat{e}\left(mP, u\sum_{i=1}^{t} f_i\right)$$

The expression is rearranged by factoring out v and u from the summation terms. This simplification is done to facilitate further manipulation.

3. Further Simplification:

$$= \hat{e}\left(vP, m\sum_{i=1}^{t} h_i\right) \cdot \hat{e}\left(ux_kP, \frac{m}{x_k}\sum_{i=1}^{t} f_i\right)$$

The expression is further simplified by rearranging terms and introducing new variables, such as $A = vP$ and $B = ux_kP$, to represent certain components of the pairing functions.

4. Final Expression:

$$\hat{e}(A, T_{Q_2}) \cdot \hat{e}(B, T_{Q_3})$$

The final expression introduces two new target elements, T_{Q_2} and T_{Q_3}, with corresponding pairing functions involving the variables A, B, and the summation terms.

The proposed equation below represent the security & privacy of the proposed model. Let's break down the equation:

$$\begin{cases} x_1, x_2, \ldots, x_l & \text{if} \quad \dfrac{l}{s} < \dfrac{1}{3} \\ y_1, y_2, \ldots, y_m & \text{if} \quad \dfrac{m}{s} < \dfrac{1}{3} \\ z_1, z_2, \ldots, z_n & \text{if} \quad \dfrac{n}{s} > \dfrac{1}{3} \end{cases} \tag{7}$$

In this specific case, there are three cases, each defined with the `\begin{cases}` and `\end{cases}` tags.

Case 1:

$$x_1, x_2, \ldots, x_l \quad \text{if} \quad \frac{l}{s} < \frac{1}{3}$$

In this case, $x_1, x_2, \ldots, x_l$ are defined (presumably as variables) when the condition $\frac{l}{s} < \frac{1}{3}$ is satisfied.

Case 2:

$$y_1, y_2, \ldots, y_m \quad \text{if} \quad \frac{m}{s} < \frac{1}{3}$$

Similarly, $y_1, y_2, \ldots, y_m$ are defined when the condition $\frac{m}{s} < \frac{1}{3}$ holds.

Case 3:

$$z_1, z_2, \ldots, z_n \quad \text{if} \quad \frac{n}{s} > \frac{1}{3}$$

In this case, $z_1, z_2, \ldots, z_n$ are defined, but only if the condition $\frac{n}{s} > \frac{1}{3}$ is met.

So, the entire system represents a set of cases where different sets of variables are defined based on specific conditions involving the ratios $\frac{l}{s}$, $\frac{m}{s}$, and $\frac{n}{s}$. The conditions imply that the sizes of the sets x, y, and z in relation to some parameter s determine whether the respective sets are defined or not.

$$\begin{cases} x_1, x_2, \ldots, x_l & \dfrac{l}{s} \quad \dfrac{1}{3} \\ y_1, y_2, \ldots, y_m & \dfrac{m}{s} \quad \dfrac{1}{3} \\ z_1, z_2, \ldots, z_n & \dfrac{n}{s} \quad \dfrac{1}{3} \end{cases} \tag{8}$$

$$\hat{e}\left(T_{Q_1}, \sum_{i=1}^{t} C_i\right) = \hat{e}\left(mP, \sum_{i=1}^{t}(vh_i + uf_i)\right) = \hat{e}\left(mP, v\sum_{i=1}^{t} h_i + u\sum_{i=1}^{t} f_i\right) = \hat{e}\left(mP, v\sum_{i=1}^{t} h_i\right) \cdot \hat{e}\left(mP, u\sum_{i=1}^{t} f_i\right)$$

$$= \hat{e}\left(vP, m\sum_{i=1}^{t} h_i\right) \cdot \hat{e}\left(ux_kP, \frac{m}{x_k}\sum_{i=1}^{t} f_i\right) = \hat{e}(A, T_{Q_2}) \cdot \hat{e}(B, T_{Q_3})$$

$$\tilde{m} = \frac{c_2'}{(c_3')^{1/sk_j}} = \frac{m\hat{h}^{\frac{r}{x_k}}}{\hat{h}^{\frac{rx_jH_3(F_i)}{x_k} \cdot \frac{1}{x_jH_3(F_i)}}} = m\hat{e}(c_4', P) = \hat{e}(r(H_3(m)P_1 + P_2), P)$$

$$= \hat{e}(rP, H_3(m)P_1 + P_2) = \hat{e}(c_6', H_3(m)P_1 + P_2)\hat{e}(c_1', P)$$

$$= \hat{e}\left(r\sum_{i=1}^{t} H_3(w_i)P, P\right) = \hat{e}\left(rP, \sum_{i=1}^{t} H_3(w_i)P\right) = \left(c_6', \sum_{i=1}^{t} H_3(w_i)P\right)$$

3 Experimental Setup

In order to execute the experiment, we opted for the utilization of the Hyperledger Fabric tool, encompassing both blockchain and IoT nodes. Throughout the duration of the experiments, we meticulously documented and employed a multitude of parameters. These encompassed variables such as the quantity of nodes involved, the number of rounds conducted, metrics pertaining to block creation, specifics regarding block digest, encryption duration, and access control timing. The simulations themselves were carried out on a robust system configuration, boasting a core i7 GPU and running the Linux operating system. Moreover, to fortify the security integrity of our proposed model, we capitalized on the AVISPA [15] and METRE frameworks. These frameworks played a pivotal role in verifying the resilience of our model against potential threats such as collusion attacks and phishing endeavors. The experimental setup devised for the assessment of the efficacy of smart contracts and blockchain within healthcare transactions was structured around the following procedural steps: Identify the research question and objectives: Clearly define the research question and objectives that will guide the experiment. For example, the research question could be "Can smart contracts and blockchain improve data security and privacy in EMR transactions?" Define the variables: Identify the variables that will be tested, such as the use of smart contracts and blockchain in EMR transactions, and how they will be measured. Select the study population: Identify the study population, such as healthcare providers or patients, and obtain their consent to participate in the study. Develop the smart contracts and blockchain network: Develop the smart contracts that will be used to automate transactions and enforce rules around data access and sharing. Develop the blockchain network that will be used to maintain a reliable log record of every transaction carried out. Implement the technology: Implement the smart contracts and blockchain network in the healthcare setting, such as in a hospital or clinic. Collect data: Collect data on the use of blockchan & smart contracts in healthcare transactions, such as the number of transactions executed, the time taken to execute transactions. Analyze the data: Analyze the data using statistical methods to evaluate the effectiveness of blockchain & smart contracts in improving data security & privacy in healthcare transactions.

4 Performance Evaluation of the Proposed Hybrid Secure Communication

In this part, a detailed examination of the simulations conducted is presented along with the corresponding results. Each outcome is thoroughly analyzed to understand the framework's performance. The proposed

model is systematically evaluated against a benchmark model to assess its effectiveness. By employing the B+-Tree indexing data structure, the framework efficiently handles data retrieval operations.

A comparative analysis is illustrated in Fig. 3, highlighting the relationship between the relative encryption time and nodes related to benchmark models. The proposed framework demonstrates marked improvements over traditional approaches, as further emphasized in this figure. Moreover, when compared with existing solutions such as MedRec, SHealth, and ECC-Smart, the proposed framework exhibits significantly lower communication overhead, primarily due to its lightweight authentication mechanism, as shown in Fig. 4. This section extends the discussion through an in-depth comparative analysis of simulation outcomes. The simulations were carried out using Hyperledger Fabric, a blockchain framework, and validated on the Ethereum test-net. A publicly available dataset from UNSW was utilized for the experiments. Key metrics of comparison include the number of transactions and network nodes, with results indicating that the proposed framework outperforms both permission-less and private blockchain models in terms of transaction throughput. Further, the analysis includes user classification based on behavior patterns using the Support Vector Machine (SVM) technique, as depicted in Fig. 5. Users are classified by examining their activity logs within the system. To enhance behavioral analysis, a Long Short-Term Memory (LSTM) deep learning model is employed, enabling the system to learn from users' historical interactions. This facilitates dynamic access control and authorization based on behavior-driven profiling. Lastly, Fig. 6 presents simulation results related to the movement and displacement of IoT-connected sensors. It specifically explores the correlation between the number of rounds and latency, offering valuable insights into the performance of the framework in dynamic IoT environments. Overall, the results affirm the robustness, scalability, and intelligence of the proposed model, especially in terms of secure access control, efficient communication, and adaptive user classification.

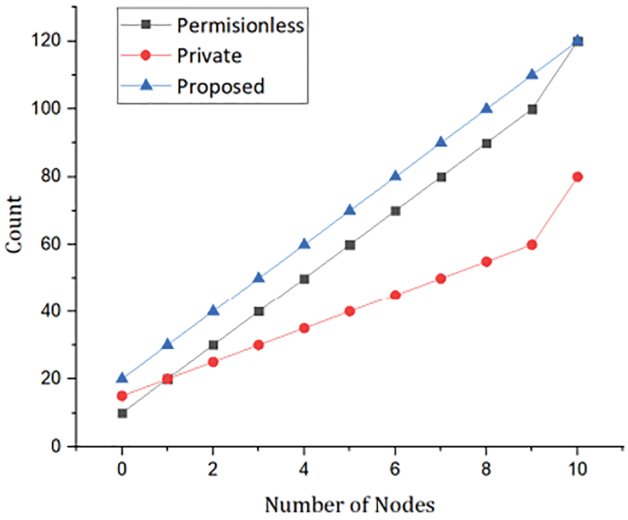

Figure 3: Proposed hybrid framework via blockchain

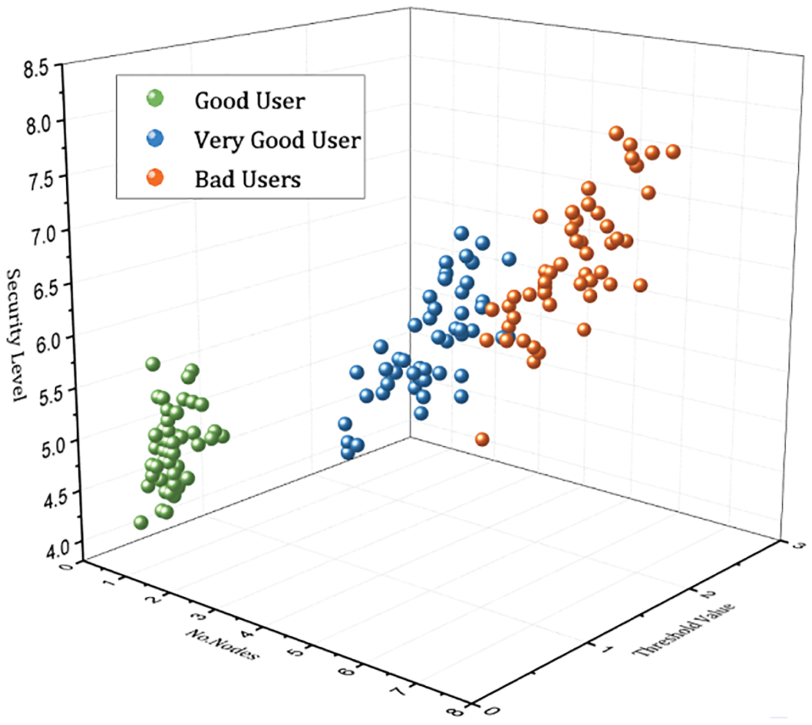

Figure 4: Proposed hybrid framework via blockchain

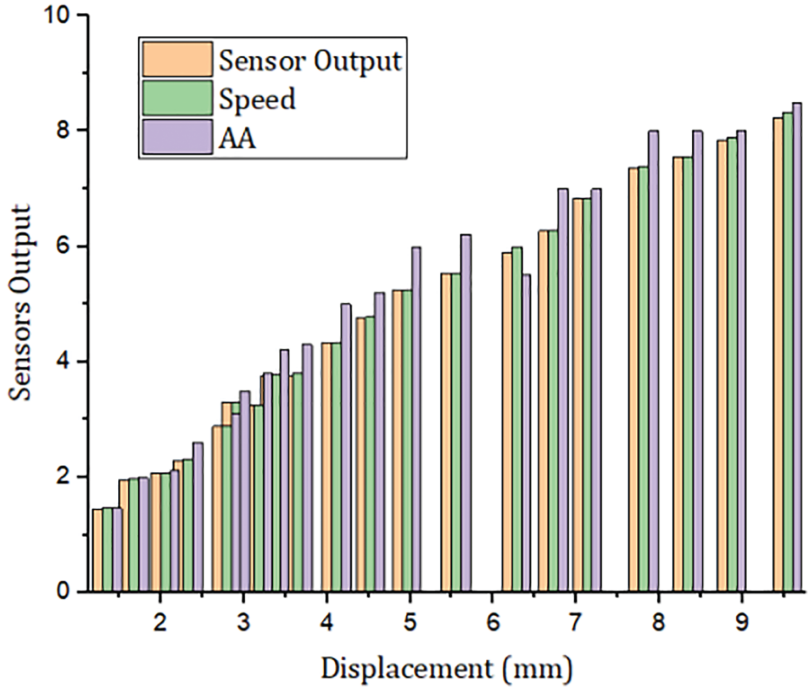

Figure 5: Proposed hybrid framework via blockchain

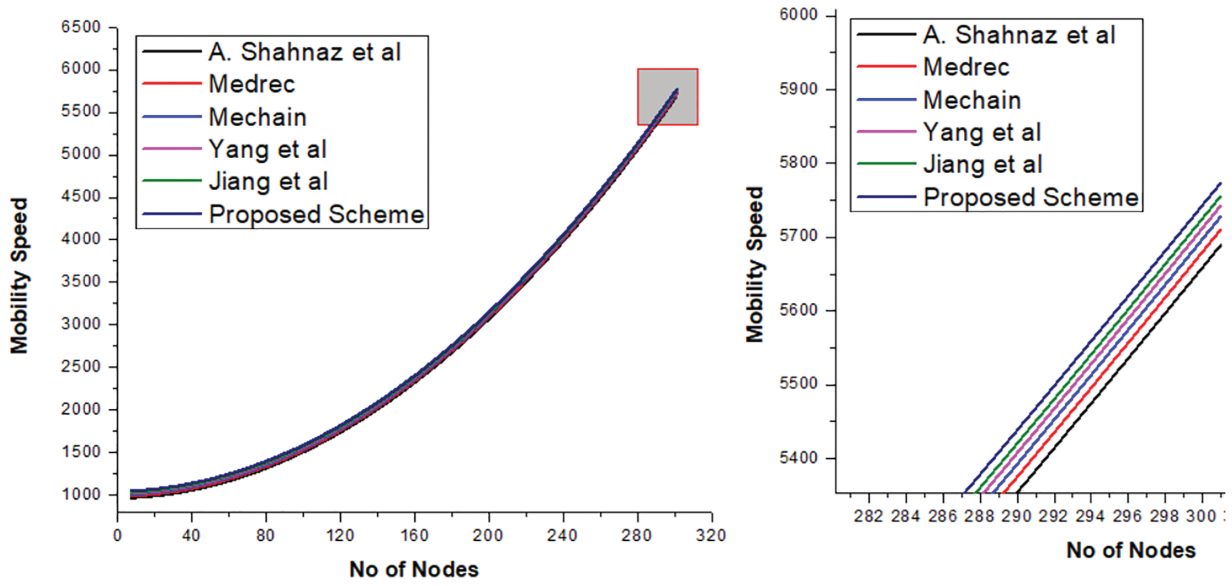

Figure 6: Proposed hybrid framework via blockchain [9,10,12]

5 Conclusion

This paper explores the powerful synergy between blockchain, IoT technologies, and smart contracts, with a particular focus on enhancing transaction security & privacy in EMR systems. The integration of these technologies enables a decentralized, tamper-resistant platform for secure data storage and sharing, improving both the efficiency and integrity of EMR operations. Smart contracts play a critical role by automating processes, reducing the risk of human error, and enforcing predefined conditions for secure data exchange. The findings highlight substantial benefits in strengthening healthcare data security & privacy. However, broader adoption in healthcare requires careful navigation of regulatory, legal, and technical challenges, including issues of data ownership, liability, interoperability, and scalability. Overcoming these hurdles is crucial for successful and widespread implementation. A decentralized ledger ensures data accuracy and real-time updates, while smart contracts enhance security by automating transaction execution. Together, they provide a robust solution to the growing concerns over data privacy and integrity in digital healthcare environments. Looking ahead, the potential applications of blockchain and smart contracts in healthcare are extensive. Future research should focus on evaluating their effectiveness in real-world settings through pilot projects and case studies. Seamless integration with existing EMR systems will require the development of standardized protocols to ensure interoperability and regulatory compliance. Beyond transaction security, blockchain's utility can extend to areas such as medical research, supply chain management, and patient consent handling. In summary, smart contracts and blockchain offer transformative potential for securing healthcare data, and while challenges remain, their benefits make them a compelling avenue for future innovation in EMR systems.

Acknowledgement: This research work is supported by the Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia, through Project number (PNURSP2025R235).

Funding Statement: This research is funded by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2025R235), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Author Contributions: The authors confirm contribution to the paper as follows: Study conception and design: Amal Al-Rasheed and Rahim Khan; data collection: Amal Al-Rasheed, Rahim Khan and Hashim Ali; analysis and

interpretation of results: Amal Al-Rasheed, Rahim Khan, Aamir Saeed; draft manuscript preparation: Amal Al-Rasheed, Rahim Khan, Aamir Saeed and Hashim Ali. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: This article does not involve data availability.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Alzahrani S, Daim T, Choo K-KR. Assessment of the blockchain technology adoption for the management of the electronic health record systems. IEEE Trans Eng Manag. 2022;70(8):2846–63. doi:10.1109/TEM.2022.3158185.
2. Sonkamble RG, Bongale AM, Phansalkar S, Sharma A, Rajput S. Secure data transmission of electronic health records using blockchain technology. Electronics. 2023;12(4):1015. doi:10.3390/electronics12041015.
3. Qu Z, Zhang Z, Zheng M. A quantum blockchain-enabled framework for secure private electronic medical records in Internet of Medical Things. Inf Sci. 2022;612(3):942–58. doi:10.1016/j.ins.2022.09.028.
4. Wu G, Wang S, Ning Z, Zhu B. Privacy-preserved electronic medical record exchanging and sharing: a blockchain-based smart healthcare system. IEEE J Biomed Health Inform. 2021;26(5):1917–27. doi:10.1109/JBHI.2021.3123643.
5. Datta S, Namasudra S. Blockchain-based smart contract model for securing healthcare transactions by using consumer electronics and mobile-edge computing. IEEE Trans Consum Electron. 2024;70(1):4026–36. doi:10.1109/TCE.2024.3357115.
6. Chamola V, Goyal A, Sharma P, Hassija V, Binh HTT, Saxena V. Artificial intelligence-assisted blockchain-based framework for smart and secure EMR management. Neural Comput Appl. 2023;35(31):22959–69. doi:10.1007/s00521-022-07087-7.
7. Kumar KP, Prathap BR, Thiruthuvanathan MM, Murthy H, Pillai VJ. Secure approach to sharing digitized medical data in a cloud environment. Data Sci Manag. 2024;7(2):108–18. doi:10.1016/j.dsm.2023.12.001.
8. Benil T, Jasper J. Blockchain based secure medical data outsourcing with data deduplication in cloud environment. Comput Commun. 2023;209(5):1–13. doi:10.1016/j.comcom.2023.06.013.
9. Hu F, Qiu S, Yang X, Wu C, Nunes MB, Chen H. Privacy-preserving healthcare and medical data collaboration service system based on blockchain and federated learning. Comput Mater Contin. 2024;80(2):2897–915. doi:10.32604/cmc.2024.052570.
10. Shahnaz A, Qamar U, Khalid A. Using blockchain for electronic health records. IEEE Access. 2019;7:147782–95. doi:10.1109/ACCESS.2019.2946373.
11. Ray PP, Chowhan B, Kumar N, Almogren A. BIoTHR: electronic health record servicing scheme in IoT-blockchain ecosystem. IEEE Internet Things J. 2021;8(13):10857–72. doi:10.1109/JIOT.2021.3050703.
12. Jiang W, Zhang Y, Han H, Liu X, Gwak J, Gu W, et al. Fuzzy ensemble-based federated learning for EEG-based emotion recognition in Internet of Medical Things. J Ind Inf Integr. 2025;44:100789. doi:10.1016/j.jii.2025.100789.
13. Maarouf A, Sakr R, Elmougy S. An offline direct authentication scheme for the internet of medical things based on elliptic curve cryptography. IEEE Access. 2024;12(18):134902–25. doi:10.1109/ACCESS.2024.3458424.
14. George N, Manuel M. A secure data hiding system in biomedical images using grain 128a algorithm, logistic mapping and elliptical curve cryptography. Multimed Tools Appl. 2025;84(4):2005–28. doi:10.1007/s11042-024-19147-2.
15. Mahore V, Aggarwal P, Andola N, Venkatesan S. Secure and privacy focused electronic health record management system using permissioned blockchain. In: 2019 IEEE Conference on Information and Communication Technology; 2019 Dec 6–8; Allahabad, India. p. 1–6. doi:10.1109/CICT48419.2019.9066204.