IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 17 June 2024, accepted 2 July 2024, date of publication 8 July 2024, date of current version 29 August 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3424685

RESEARCH ARTICLE

Proof of Trust and Expertise (PoTE): A Novel Consensus Mechanism for Enhanced Security and Scalability in Electronic Health Record Management

MD. ZIA UR RAHMAN[1], (Senior Member, IEEE), SUMALATHA AKUNURI[2], D. NAGABHUSHANA BABU[3], M. V. S. RAMPRASAD[4], SK. MOHAMMED SHAREEF[5], AND MASRESHAW DEMELASH BAYLEYEGN[6]

[1]Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, K. L. Deemed to be University, Vaddeswaram, Andhra Pradesh 522502, India
[2]Department of Electronics and Instrumentation Engineering, Siddhartha Academy of Higher Education (SAHE)–Deemed to be University, Kanuru, Vijayawada, Andhra Pradesh 520007, India
[3]Department of Data Science and Information Technology, School of Engineering, Malla Reddy University, Hyderabad, Telangana 500100, India
[4]Department of EECE, GITAM School of Technology, GITAM (Deemed to be University), Visakhapatnam, Andhra Pradesh 530045, India
[5]Department of Electronics and Communication Engineering, Narasaraopeta Engineering College (A), Narasaraopeta, Andhra Pradesh 522601, India
[6]Center of Biomedical Engineering, Addis Ababa Institute of Technology, Addis Ababa University, Addis Ababa 1176, Ethiopia

Corresponding author: Masreshaw Demelash Bayleyegn (masreshaw.demelash@aau.edu.et)

ABSTRACT This paper proposes a paradigm that combines edge computing and blockchain technology in the healthcare field, providing a groundbreaking method to handle, analyze, and safeguard medical data. The method effectively decreases the time delay, addresses problems related to data transmission capacity, and improves the protection of sensitive patient data by processing it locally. The blockchain network is essential to the system since it offers a secure and unchangeable record for storing processed data. The integration of this novel system guarantees that patient data, once recorded, is unable to be modified in a way that affects previous entries, thereby preserving the integrity of the data. This approach prominently incorporates the innovative Proof of Trust and Expertise (PoTE) consensus process, which utilizes the reliability and specialized knowledge of users in the network. This approach not only guarantees the secure and efficient validation of transactions, but also conforms to the essential demands of managing healthcare data. The proposed model provides efficient environment that is scalable and reliable with average block processing time of 0.25 sec, transactional throughput of 140 transactions per second (tps) and a success rate of 97% while operating over larger number of nodes in the network. The incorporation of edge computing and blockchain in healthcare is positioned to establish a novel benchmark in the management, processing, and security of medical data, consequently augmenting the overall caliber of healthcare services.

INDEX TERMS Blockchain, edge computing, Internet of Things, privacy, security.

I. INTRODUCTION

The healthcare industry is undergoing a digital transformation, driven by the need to improve service delivery, patient outcomes, and operational efficiencies. Central to this transformation is the management and utilization of Electronic Health Records (EHRs), which contain sensitive patient information and are essential for modern healthcare services. However, the increasing volume of data, coupled with rising cyber threats and stringent regulatory requirements, presents significant challenges. There is always a need for scalable, secure, and efficient system for managing EHRs. EHRs are foundational to contemporary healthcare systems, facilitating the storage, retrieval, and sharing of patient information [1].

The associate editor coordinating the review of this manuscript and approving it for publication was Agostino Forestiero.

They are also prime targets for cyber-attacks due to the sensitive nature of the data they contain. Breaches can lead to significant privacy violations and substantial financial and reputational damage. Furthermore, as the healthcare industry continues to expand its digital footprint, the volume of data generated increases exponentially, necessitating scalable solutions that can accommodate this growth without compromising performance or security [2].

The traditional centralized models for data management are increasingly inadequate in this context. They often suffer from bottlenecks, single points of failure, and scalability issues. Moreover, they may not fully comply with emerging regulations that demand greater transparency, data integrity, and patient control over their information. Therefore, a new paradigm that can secure sensitive health data while ensuring it is readily available and manageable on a large scale is the need of the hour. The digitalization of patient records has made them accessible to a wide range of healthcare providers, improving the continuity and quality of care. However, it also exposes sensitive patient data to various cyber threats, including data breaches, unauthorized access, and ransomware. These threats not only compromise patient privacy but also undermine trust in healthcare systems. Additionally, the increasing volume of healthcare data necessitates scalable solutions that can manage this growth without degradation in performance or security [3].

Edge computing refers to the decentralized paradigm where computation is performed near the data source. In healthcare, this means processing patient data on-site at clinics, hospitals, or even on the patient's wearable devices [4]. This approach minimizes latency, reduces the bandwidth required for data transmission, and allows for real-time data processing, crucial for time-sensitive medical decisions. Scientifically, edge computing leverages principles from distributed computing and real-time systems to ensure data is processed efficiently and securely at the network's edge. Edge computing brings data processing closer to the source of data generation. In the context of healthcare, this means processing patient data directly at the point of care — in hospitals, clinics, or even through wearable devices. This approach reduces latency, alleviates bandwidth pressure on central servers, and enhances the ability to make real-time decisions based on the data [5]. However, while edge computing addresses aspects of scalability and performance, it introduces new challenges in managing and securing distributed nodes.

The integration of healthcare services facilitates the development of novel applications in the healthcare sector. The potential applications range from remote patient monitoring and telemedicine to ensuring secure pharmaceutical supply chains and facilitating research data sharing, offering huge and transformative possibilities [6]. Developing a new consensus mechanism designed specifically for the healthcare industry in blockchain technology. It utilizes the trust and experience present in the healthcare community. It guarantees that the verification of transactions and health data is managed by reliable and authoritative nodes, providing an additional level of dependability and precision.

Blockchain provides a decentralized and secure framework for data management. It ensures data integrity, transparency, and traceability through its immutable ledger system [7], [8]. Each transaction on the blockchain is encrypted and linked to the previous transaction, creating a secure chain of data that is resistant to tampering. Furthermore, smart contracts automate and enforce access controls and other rules without the need for intermediaries, enhancing the system's efficiency and security [9]. Fig 1 illustrates a block diagram to illustrate the structure and components of Blockchain technology, emphasizing its distributed ledger feature, cryptographic elements, and the underlying scientific principles. Blockchain is a distributed ledger technology known for its robust security and immutability. Each block in the chain contains a cryptographic hash of the previous block, a timestamp, and transaction data, creating a chronological chain of records that is resistant to modification. From a scientific standpoint, blockchain employs cryptographic algorithms and consensus mechanisms to ensure data integrity and security. Its decentralized nature eliminates single points of failure, significantly reducing the risk of data tampering and loss [10].

The combination of edge computing with blockchain in healthcare yields not only additive but multiplicative advantages. This integration addresses the essential requirements of contemporary healthcare systems. Integrating the real-time data processing capabilities of edge computing with the secure and unchangeable record-keeping features of blockchain technology forms a strong framework for effectively managing health data. This technology guarantees the efficient processing of patient data at the edge and its secure storage on the blockchain, providing an optimal combination of rapidity and safety [11]. Given the growing apprehensions around data privacy and the implementation of strict legislation, this integration provides a solution that adheres to the required standards. The local data processing capabilities of edge computing improve privacy, while the secure and transparent nature of blockchain guarantees compliance with data protection standards. Scalability and efficiency are of utmost importance as the amount of healthcare data increases significantly. Edge computing mitigates the data burden on central servers, while blockchain offers a scalable architecture for data governance. This synergy effectively manages increasing data requirements while maintaining optimal performance.

Although the combination of edge computing and blockchain in healthcare offers numerous benefits, it also presents certain difficulties [12]. Significant obstacles include technical intricacies, interoperability challenges, adherence to regulatory requirements, and the necessity for a strong infrastructure. Furthermore, due to the newness of these technologies, it is necessary to provide extensive instruction and training to healthcare professionals and

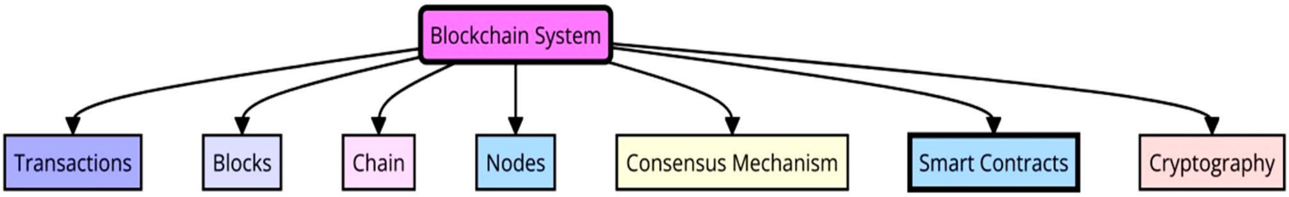


FIGURE 1. Block diagram illustrating the components and features of blockchain.

IT people. The use of edge computing and blockchain technology in the healthcare sector is a new and essential advancement in the era of digitalization. It fulfills the fundamental requirements of security, efficiency, confidentiality, and expandability in the handling of healthcare data. The integration of data management in the healthcare sector represents a significant advancement in healthcare technology, as it addresses the challenges posed by the large volume of data and the need for secure and effective data handling. The objectives of the proposed model include

•To provide a highly secure environment for storing and managing healthcare data, utilizing blockchain's immutability for ensuring the integrity of health records, making them tamper-proof and reliable.

•To process and encrypt data locally at edge nodes, reducing the risk of data breaches during transmission and enable immediate processing of critical healthcare data at the source, which is crucial in time-sensitive medical scenarios.

•To reduce latency in data access and processing, this is essential for emergency medical services and real-time health monitoring.

•To efficiently handle the increasing volume of healthcare data generated by electronic health records and IoT devices by implementing energy-efficient consensus mechanisms and system operations.

II. EXISTING SYSTEMS

In recent years, the healthcare industry has witnessed a surge in the adoption of innovative technologies to address the challenges associated with managing electronic health records (EHR). Two such technologies, namely, edge computing and blockchain have gained significant attention for their potential to enhance security and scalability in healthcare record management [13]. Existing models and approaches in the literature that leverage edge computing and blockchain for EHR management that emphasize the need for enhanced security and scalability in the healthcare sector are discussed here along with the conventional edge based and blockchain based approaches [14].

Traditional methods of healthcare record management typically rely on centralized systems, such as electronic health record (EHR) systems and health information exchanges (HIEs), to store and manage patient data. These systems provide a centralized repository for healthcare records, enabling healthcare providers to access and update patient information as needed. While centralized systems offer convenience and ease of access, they also pose significant challenges in terms of security, scalability, and interoperability [15]. Centralized storage makes healthcare data vulnerable to cyber attacks, data breaches, and unauthorized access, compromising patient privacy and confidentiality. Additionally, as the volume of healthcare data continues to grow, centralized systems struggle to scale effectively, leading to performance issues and delays in data retrieval. Interoperability remains a major challenge in healthcare record management, as different systems often use different data formats, standards, and protocols, making it difficult to exchange and integrate patient data across different healthcare organizations and systems. This lack of interoperability hinders care coordination, medical research, and public health initiatives, leading to inefficiencies and gaps in patient care. Data mapping and transformation techniques are often complex, time-consuming, and costly to implement, requiring significant coordination and investment from healthcare organizations and stakeholders [16].

By leveraging blockchain, healthcare organizations can enhance the security and privacy of patient information, streamline data exchange, and improve trust and transparency among stakeholders. Moreover, blockchain's smart contracts enable automated and trustless transactions, facilitating secure data sharing and access control in healthcare record management [17], [18]. The integration of edge computing and blockchain represents a novel approach to healthcare record management, combining the benefits of real-time data processing at the network edge with the security and transparency of blockchain technology. Decentralized EHR systems use blockchain technology to create a secure and immutable ledger of health records. This approach ensures that records are not stored in a central location, reducing the risk of data breaches [19]. Methods developed in [11] and [20] leverage integration of edge computing and blockchain to secure patient data and enable controlled access by authorized parties.

Existing models in edge computing for healthcare record management focus on leveraging edge devices such as wearable sensors, medical devices, and IoT devices to collect and process patient data. These models emphasize the importance of edge analytics and edge caching techniques to optimize data processing and storage at the network edge [21], [22], while blockchain technology is used to securely store and manage electronic health records. Smart contracts govern access control and data management, ensuring that only authorized users can access and update patient information [23]. Smart contracts automate the execution of agreements, ensuring that access to health records is granted only under predefined conditions. This method enhances data privacy by enforcing strict access controls and permissions, which are recorded and verifiable on the blockchain. The integration of edge computing and blockchain brings together the benefits of real-time data processing at the network edge with the security and transparency of blockchain technology [24].

Consensus mechanisms are essential in integrating blockchain with edge computing, ensuring the security, integrity, and consensus of transactions across distributed networks [25]. These mechanisms are protocols or algorithms that enable nodes in a decentralized network to agree on the validity of transactions and reach a consensus on the state of the ledger. When combined with edge computing, these mechanisms help maintain the integrity of data stored on the blockchain while enabling efficient and scalable data processing at the network edge [26]. Some common consensus mechanisms include Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), and Federated Consensus. PoW is known for its security and resistance to attacks, but it requires significant computational power and energy consumption, making it less suitable for edge devices with limited resources and energy constraints. PoS is an alternative consensus mechanism where validators are chosen to create new blocks based on the amount of cryptocurrency they hold and are willing to "stake" as collateral. DPoS is known for its scalability and speed, allowing for faster transaction processing compared to traditional PoW and PoS mechanisms. Practical Byzantine Fault Tolerance (PBFT) is a consensus mechanism designed for permissioned blockchain networks where all participating nodes are known and trusted. It allows nodes to reach consensus on the order of transactions through a series of voting and message exchange, known for its high throughput and low latency, making it suitable for applications requiring fast transaction processing, such as edge computing environments. Federated consensus is a consensus mechanism where a group of pre-selected nodes collectively validate transactions and produce new blocks, offering greater scalability and flexibility compared to traditional blockchain networks [27]. Consensus mechanisms play a critical role in integrating blockchain with edge computing by ensuring the security, scalability, efficiency, and flexibility of decentralized networks. By selecting appropriate consensus mechanisms that balance the requirements of security, scalability, and resource efficiency, blockchain networks can effectively support edge computing applications and enable secure and efficient transaction processing at the network edge.

Existing models in the literature propose various approaches to integrating edge computing and blockchain for healthcare record management. These models leverage edge devices for data collection and processing, while blockchain technology is used to securely store and manage electronic health records. By combining the low-latency data processing capabilities of edge computing with blockchain's decentralized and immutable ledger, these integrated solutions offer enhanced security, scalability, and privacy in healthcare record management [28], [29]. Integrating edge computing with blockchain addresses scalability issues by distributing data processing tasks across the network of edge nodes. This reduces the burden on the central server and ensures that the system can handle growing amounts of data without significant delays or increased costs [30].

By leveraging edge computing for real-time data processing and blockchain for secure data storage and management, these integrated solutions offer a robust framework for safeguarding electronic health records and ensuring the efficient delivery of healthcare services. However, further research is needed to explore the practical implementation and deployment of these models in real-world healthcare settings.

III. SYSTEM DESIGN

The proposed model illustrates a synergistic integration of edge computing and blockchain for providing remote patient monitoring by utilizing edge computing for real-time data analysis from wearable devices, ensuring timely medical interventions. It can also be used in telemedicine to securely transmits patient data between edge devices and healthcare providers using blockchain, ensuring data integrity and privacy. The proposed model also enhances data security and accessibility through immutable blockchain storage and real-time data processing at the edge. The overall system components and services are illustrated in Fig 2. These services are grouped together in different layers for flexibility in operations and each layer is explained as follows.

A. EDGE LAYER

This layer is responsible for localized data processing and security. At the edge, data preprocessing algorithms are employed to clean, standardize, and structure incoming patient data. This includes noise reduction, normalization, and feature extraction, which are crucial for ensuring the data's quality and utility. Leveraging machine learning and statistical models, the edge layer implements real-time anomaly detection to identify unusual patterns or potential security threats. Machine learning and statistical models are utilized for real-time anomaly detection in the edge layer, including Isolation Forest, One-Class SVM, and statistical methods like Z-Score. Isolation Forest efficiently isolates anomalies in high-dimensional data, while One-Class SVM uses kernel functions to classify data points into normal or outlier classes. Statistical methods like Z-Score provide a simple and effective technique for detecting anomalies in normally distributed data. These models are integrated into the edge layer to preprocess data, select appropriate models based on data characteristics, and perform real-time anomaly detection, ensuring quick response times. Detected anomalies are flagged, and relevant data is securely stored on the blockchain for audit and traceability, enhancing data integrity and security while maintaining high performance and efficiency. This proactive approach allows for immediate response to potential issues, enhancing the system's overall security. To address scalability and privacy concerns, data minimization techniques are applied. These techniques extract and encrypt only the necessary information, reducing the data volume transmitted and stored while preserving its essential characteristics.

Let, $E_{i,0}$ represents the initial energy level, ECR_i represents the energy consumption rate and EHR_i represents the energy harvesting rate of node i in the edge network. The energy level equation at any instant t, taking into account both energy consumption and energy harvesting, is given by

$$E_i\left(t\right) = E_{i,0} - \int_0^t \left(ECR_i - EHR_i\right) dt \tag{1}$$

The edge layer efficiently preprocesses and also minimizes the data at the edge before it is being sent to the blockchain with compromising the data quality and relevance. The data minimization function is defined as

$$D_p = Minimize\left(D_r; \lambda\right) \tag{2}$$

where D_p is the preprocessed data, D_r is the raw data from sensors and λ regularization parameter that controls trade-off between data minimization and information loss. The data quality assurance score is given by

$$Q\left(D_p\right) = q - \alpha.L(D_r, D_p) \tag{3}$$

where q, and α are the maximum quality score of the processed data and weight quotient for the loss. L is the loss function measuring the information loss de to data minimization. This model ensures that data is processed efficiently at the edge and provides the balance required for the trade-off between data minimization and integrity. The time taken by edge node to process data packet is given by

$$T_{edge} = T_{process} + T_{communication} \tag{4}$$

where $T_{process}$ is the time required for local data processing at the edge node and $T_{communication}$ is the time required for communication with the other nodes or blockchain nodes. The trust score for the edge nodes is given by

$$Trust\ Score = \frac{\sum Trust\ Score_i}{N} \tag{5}$$

where $Trust\ Score_i$ is the trust score assigned by the other nodes to the edge node i, and N is the total number of interactions of that particular node. This score quantifies the trustworthiness of the edge node based on the historical behavior and interaction within the network. The edge node's expertise level is a measure of the expertise level in a specific domain (healthcare in this case). Device such as Raspberry Pi can have more processing capability compared to Arduino. Based on this expertise score, the other nodes can understand the services they can expect from a specific node and this expertise level is given by

$$Expertise\ Level = \frac{\sum EL_i}{N} \tag{6}$$

where EL_i is the expertise level of a node in that specific domain. The edge node availability is given by

$$E_{availability} = \left(\frac{T_{available}}{T_{total}}\right) \times 100\% \tag{7}$$

where $T_{available}$ is the total time, the node is available and T_{total} is the observation period time.

B. BLOCKCHAIN LAYER: IMMUTABLE RECORD KEEPING AND ACCESS CONTROL

This layer house smart contract autonomously executes predefined rules for data access and modification. They provide a transparent, auditable, and enforceable means of managing access to EHRs, ensuring that only authorized individuals can interact with the data. A carefully selected consensus mechanism balances efficiency and security. For healthcare applications running on resource-limited networks, mechanisms like Proof of Authority or Federated Consensus might be preferred for their speed and reduced computational requirements compared to Proof of Work. Innovative algorithm called Proof of Trust and Expertise (PoTE) is employed in the proposed model. Let, $B_{j,0}$ represents the initial energy level, BCR_j represents the energy consumption rate and NP_j represents the energy harvesting rate of node j in the blockchain network. The energy level equation at any instant t, equation takes into account the energy consumed by a blockchain node j for its participation in the consensus process over time is given by

$$B_j\left(t\right) = B_{j,0} - \int_0^t \left(BCR_j.NP_j\right) dt \tag{8}$$

The network latency due to the transaction delay within the blockchain is given by

$$B_{latency} = \frac{\sum T_{delay_i}}{M} \tag{9}$$

where T_{delay_i} is the delay for transaction i, and M is the total number of transactions. The trust scores over time based on the node i action at any time t is denoted as $TrustScore_i(t)$ and the update function is given by

$$TrustScore_i\left(t+1\right) = TrustScore_i\left(t\right) + \xi.\left(A_i\left(t\right) - \rho.I_i(t)\right) \tag{10}$$

$A_i\left(t\right)$ indicates the successful validations of node i at time t, $I_i(t)$ is the invalid transactions down time and ξ, ρ are the weight coefficients for successful and unsuccessful validations. The validator selection is based on the trust and expertise scores determined by the validator weighting function given by

$$W_{i,a} = \omega_{TrustScore}.TrustScore_i^{\theta} + \omega_E.E_{i,a}^{\eta} \tag{11}$$

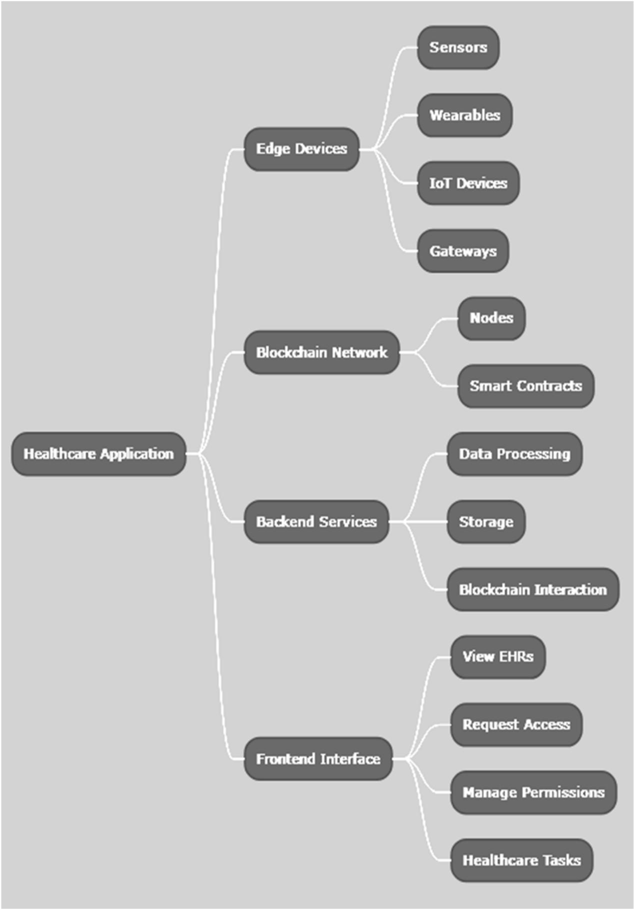


FIGURE 2. **Overall components in the proposed architecture.**

where $W_{i,a}$ weight of the node i for being a validator in area a. $TrustScore_i^{\theta}$ and $E_{i,a}$ are trust score and expertise level of the node i. $\omega_{TrustScore}$ and ω_E are the weight coefficients of trust and expertise and θ and η are the exponents controlling the impact of trust and expertise. The probability that a node i for being a validator in area a is given by

$$P_v(i,a) = \frac{W_{i,a}}{\sum_{j=1}^{N} W_{j,a}} \tag{12}$$

C. INTEGRATION LAYER

This layer provides seamless integration and ensures that data across the edge and blockchain layers remain consistent and up-to-date. It employs sophisticated synchronization algorithms that detect and resolve discrepancies, maintaining the system's integrity and reliability. Given the diverse nature of healthcare systems and data formats, interoperability is the key. The integration layer implements protocols that allow seamless communication and data exchange between different systems and standards, enhancing the model's applicability and effectiveness. The services offered by this synergy are illustrated in Fig 3. To optimize the energy usage across the network, the problem in the proposed design is modeled as minimizing the total energy consumption subject to constraints on the operational requirements and energy capacities of the nodes.

$$minimize : \sum ECR_{i/j} - EHR_i \tag{13}$$

subject to Energy levels must remain above a critical threshold to ensure uninterrupted service, Task scheduling must meet all operational and QoS requirement and energy harvesting and replenishment rates are maximized. Here, $ECR_{i/j}$ represents the energy consumption of the nodes i or j in the edge and blockchain networks, respectively.

The integration layer in the proposed system ensures interoperability with diverse healthcare systems by implementing a variety of industry-standard protocols and standards. These protocols and standards facilitate seamless data exchange, integration, and communication across different systems and platforms, enhancing the overall efficiency and effectiveness of healthcare operations. The integration layer in the proposed system implements a variety of industry-standard protocols and standards to ensure interoperability with diverse healthcare systems.HL7 is a set of international standards for the exchange, integration, sharing, and retrieval of electronic health information. It provides a framework for the exchange of clinical and administrative data between healthcare applications. The model uses HL7 Version 2 (v2) used for messaging standards that define the structure of messages exchanged between healthcare systems.

In emergency situations, immediate access to critical patient data is essential for timely medical intervention and decision-making. The proposed system is designed to handle such scenarios efficiently while ensuring robust security measures are in place to protect sensitive information. The system uses a priority-based access control mechanism to grant immediate access to critical data during emergencies. Medical personnel with higher priority levels (e.g., emergency doctors, paramedics) are granted expedited access to necessary information.

Edge devices preprocess the data locally before transmitting it to the blockchain for secure storage. The preprocessing includes data cleaning, normalization, encryption, and anomaly detection. Once the data is preprocessed and encrypted at the edge, it is sent to the blockchain layer. The blockchain layer handles data validation, consensus, and storage. Listing 1 gives the algorithm of this integration process. Edge devices preprocess data locally to reduce latency and improve data quality. Anomaly detection mechanisms are employed to ensure data integrity before transmission. The blockchain layer ensures data immutability and security through the PoTE consensus mechanism. Validated data is stored in the blockchain, providing a tamper-proof record of transactions. Fig 4 shows the interaction between edge layer and blockchain network. This integration ensures efficient local data processing at the edge, secure transmission, and immutable storage in the blockchain, enhancing the overall system performance and security.

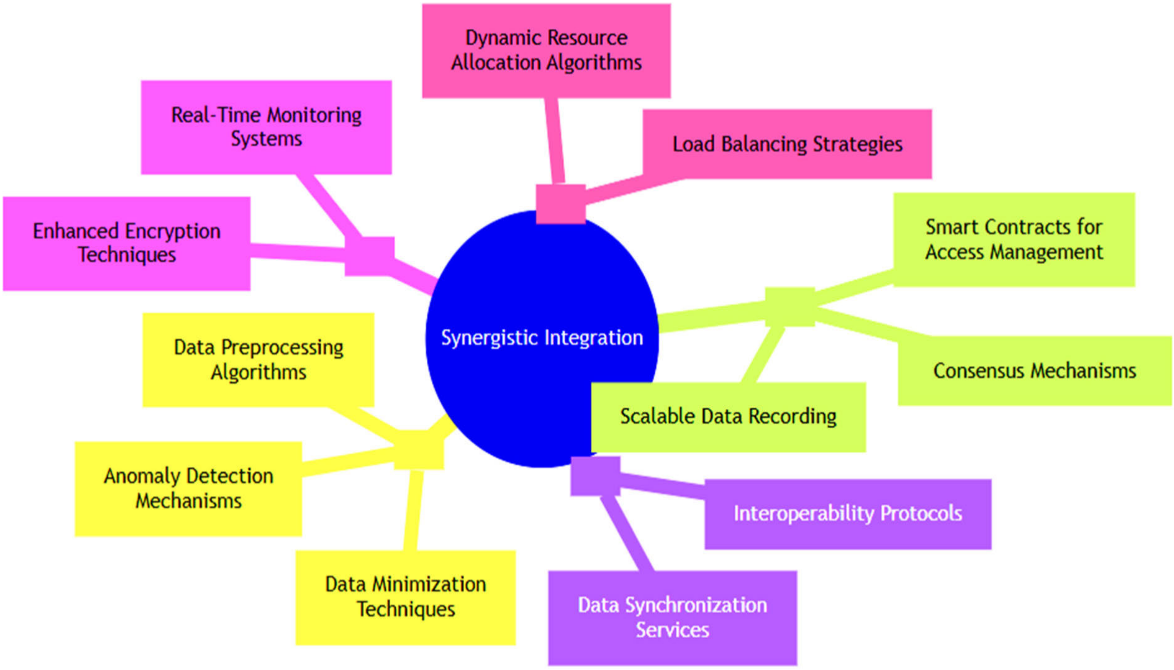

Dynamic Resource Allocation Algorithms
Real-Time Monitoring Systems
Load Balancing Strategies
Enhanced Encryption Techniques
Smart Contracts for Access Management
Synergistic Integration
Data Preprocessing Algorithms
Consensus Mechanisms
Scalable Data Recording
Anomaly Detection Mechanisms
Interoperability Protocols
Data Minimization Techniques
Data Synchronization Services

FIGURE 3. Services offered by the proposed integrated model.

LISTING 1. Algorithm for edge and blockchain interfacing.

```
def edge_data_processing(raw_data):
{
  # Step 1: Data cleaning and normalization
  cleaned_data = clean_data(raw_data)
  normalized_data = normalize_data(cleaned_data)

  # Step 2: Data encryption
  encrypted_data = encrypt_data(normalized_data)

  # Step 3: Anomaly detection
  anomalies = detect_anomalies(encrypted_data)
  if anomalies:
    handle_anomalies(anomalies)
  return encrypted_data
}
def blockchain_interaction(preprocessed_data):
{
  # Step 1: Create a new block with the
preprocessed data
  new_block = create_block(preprocessed_data)

  # Step 2: Validate the block using Proof of Trust
and Expertise (PoTE)
  is_valid = validate_block(new_block)
  if not is_valid:
    return "Block validation failed"
  # Step 3: Add the block to the blockchain
  add_block_to_blockchain(new_block)
  return "Block successfully added to the blockchain"
}
```

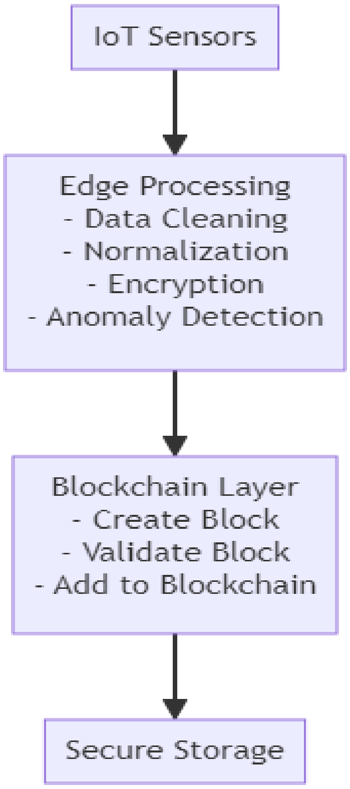


FIGURE 4. Interfacing of edge layer and blockchain network in the proposed model.

D. SECURITY ENHANCEMENTS

Beyond standard encryption methods, the model incorporates advanced techniques like homomorphic encryption, which allows certain computations to be performed on encrypted data, providing an additional layer of security and privacy. To further enhance security, real-time monitoring systems are integrated to continuously scan for unusual activities or potential threats, providing immediate alerts and triggering automated responses to mitigate risks.

E. PERFORMANCE OPTIMIZATION

Dynamic resource allocation algorithms assess the current demand and available resources across the network, dynamically allocating computational power and storage where needed. This not only ensures optimal performance but also enhances the system's ability to scale. The dynamic resource allocation algorithm in the proposed system involves continuous monitoring f resource usage, predictive analytics to forecast future demands, and real-time decision-making to adjust resource allocations. By implementing criteria based on utilization thresholds and predictive models, the system ensures optimal use of computational power and storage, maintaining high performance and efficiency in real-time. This approach helps prevent resource bottlenecks, optimize resource utilization, and ensure the system can adapt to changing demands effectively. Employing load balancing, the system efficiently distributes workload across multiple nodes, preventing any single node from becoming a bottleneck, thereby maintaining high performance and reliability even under high loads.

Smart Contract based EHR access manager is defined to securely and efficiently manage access to patient EHRs, ensuring that only authorized individuals can view or modify records according to predefined rules and permissions. The system maintains an access control list (ACL) that contains a list of users and their corresponding access rights. A structure that creates mapping of user identifiers (e.g., public keys) to their access rights (e.g., read, write, admin) is created. Functions to add, remove, or update user access rights, only executable by users with admin rights are provided. An authentication mechanism to authenticate users attempting to access EHRs utilizes cryptographic methods e.g., digital signatures) to ensure that access requests are rom legitimate users. Verification process is used to cross-reference the public key from the access request with the ACL to verify permissions.

The Entity-Relationship model for the smart contract in the proposed model is illustrated in Fig. 5, Access Logs are used to maintain an immutable record of all access attempts, successful or not. The structure stores records of access attempts, including user ID, timestamp, action attempted (e.g., read, write), and whether the attempt was successful.

Fig. 6 demonstrates the sequence of operations while accessing the EHRs through smart contracts. Dynamic Permissioning mechanism is used to adjust user permissions dynamically based on predefined rules. This implemented by using conditional logic to modify user permissions based on factors such as user role changes, emergencies, or consent revocation. Consent Management ensures patient consent is central to the EHR access process. This integration allows patients to directly manage their consent preferences, which in turn dynamically adjusts the ACL. In emergency cases, where immediate data access could be life-saving, a secure override function that grants temporary access in emergencies, with strict logging and post-emergency audit processes.

Since, conventional consensus mechanisms are resource-intensive, a novel consensus mechanism called Proof of Trust and Expertise (PoTE) is used in the proposed method. PoTE relies on trustworthiness and reputation, assigning trust scores based on past behavior, contribution to the network, and adherence to consensus rules. When a new transaction is proposed, participants evaluate its validity based on consensus rules and trust scores. If valid, it is included in a candidate block. Votes are cast based on trust scores and expertise levels, with higher scores having more influence. The candidate block is then proposed to the network for validation, verifying its integrity and validity. If successful, it is finalized and added to the blockchain as the latest block. Incentives may be included to encourage active participation and cooperation. PoTE allows for dynamic adjustment of trust scores and expertise rankings based on participants' behavior, contributions, and interactions within the network. The overall process is summarized in the form of a flowchart in Fig. 7. Listing 2 provides the algorithm for the PoTE consensus mechanism. When discrepancies are detected, several measures are in place to handle and mitigate these issues effectively. These measures include automated reconciliation processes, anomaly detection mechanisms, manual reviews, and consensus revalidation.

LISTING 2. Algorithm for proof-of-trust-and-expertise (PoTE).

```
Input:  List of transactions T to be validated, List of
blockchain nodes N, each with a trust score and expertise
level
Output:  List of validated transactions
Begin
   // Step 1: Initialize
   Initialize validated_transactions as an empty list

   // Step 2: Transaction Validation Loop
for each transaction tx in T do
      // Step 2.1: Select Validators
      validators = select_validators(N, tx)
      // Step 2.2: Initialize Approval Count
approval_count = 0
      // Step 2.3: Validators Validate Transactions
      for each validator in validators do
ifvalidator_approves(validator, tx)then
approval_count = approval_count + 1
endIf
endFor
      // Step 2.4: Check for Majority Approval
if approval_count> (number of validators / 2)then
         Add tx to validated_transactions
endIf
endFor
   // Step 3: Return Validated Transactions
   Return validated_transactions
End
```

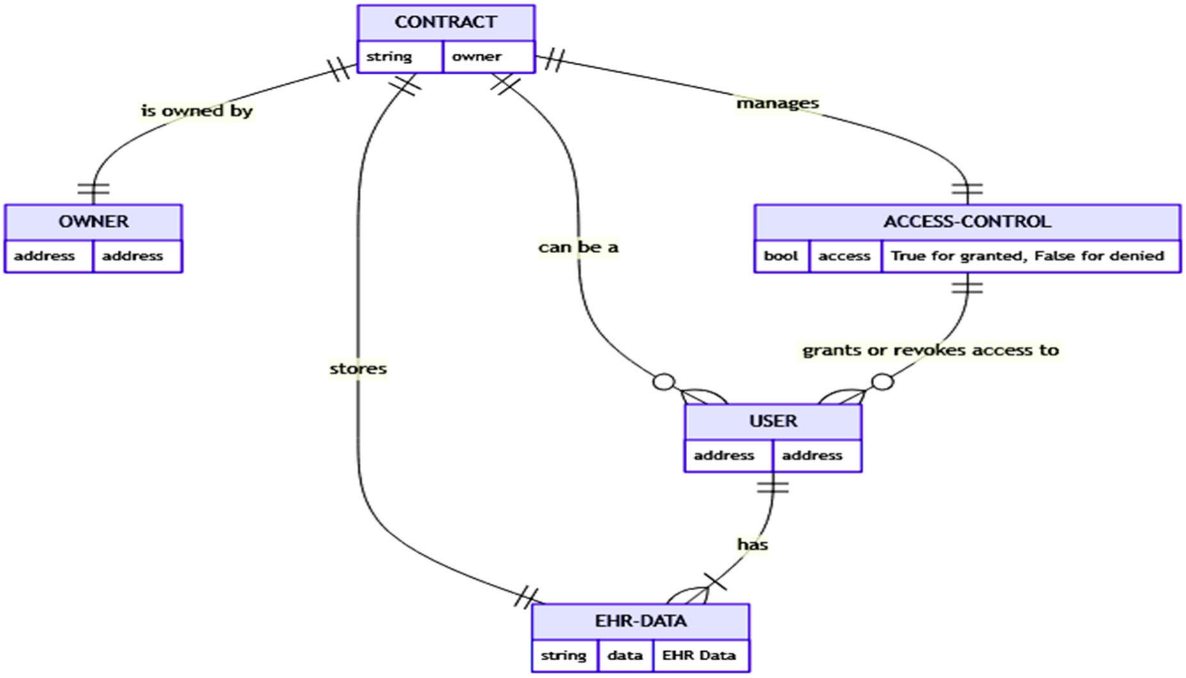


FIGURE 5. E-R model for the smart contract in the proposed method.

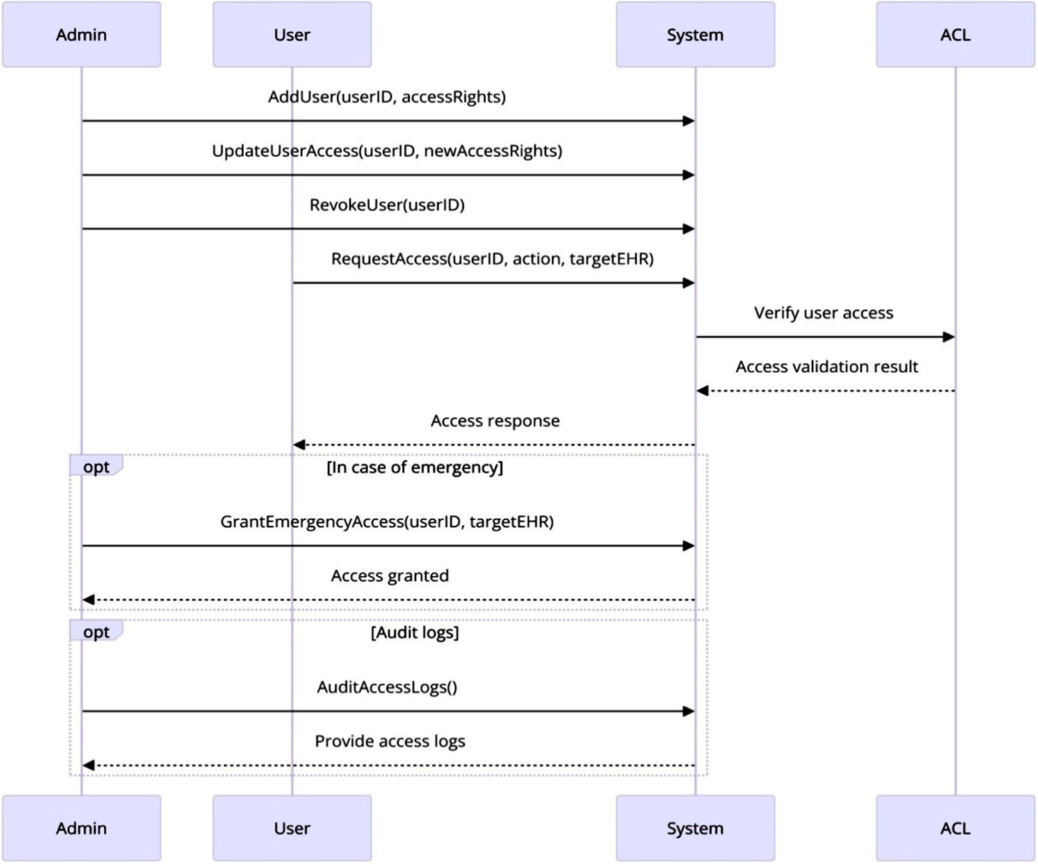


FIGURE 6. Sequence of operation happening during the smart contract call in the proposed model.

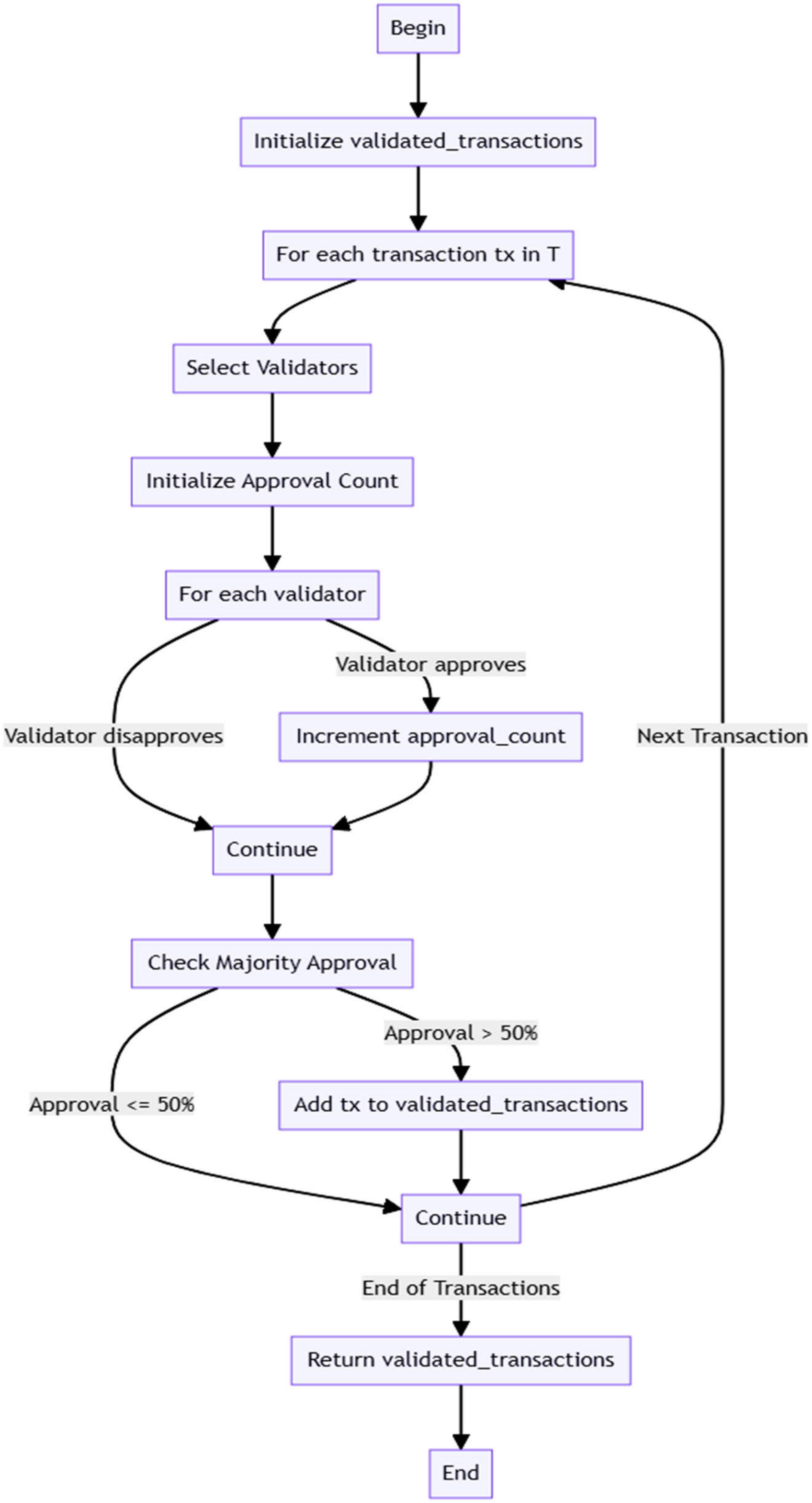


FIGURE 7. **Flowchart illustrating the mechanisms involved while validating the transactions using Proof-of-Trust-and-Expertise.**

IV. RESULTS

The simulation environment for the proposed model includes a 1000 square meters network area, 50 edge nodes, an Ethereum-based blockchain network, a Proof of Authority consensus mechanism, 1 MB block size, 24-hour simulation duration, MQTT, TCP/IP communication protocols, energy harvesting from solar panels and kinetic energy converters, and a Poisson distribution network traffic model. A high-performance laptop with a processor of Intel Core i7-10750H 6-Core Processor, 16 GB DDR4 RAM, 512 GB PCIe NVMe SSD storage, and a dedicated graphics card for visualization and analysis of simulation results was used. The laptop's operating system is Windows 10 Home 64-bit, and it supports Gigabit Ethernet, Wi-Fi 6 (802.11ax), and Bluetooth 5.0. Table 1 lists the simulation parameters used while evaluating the proposed system.

Fig 8 illustrates the performance of the proposed model for healthcare with lower average block processing time and average edge processing time compared to standard methods. Fig 9 shows the block time comparison and energy consumption of various blockchain networks. This combines average block time, the time taken to create and validate a new block .and consistency of block time, variance in block time, indicating the stability of the blockchain network. For PoW based blockchains, the average block time is typically around 10 minutes (e.g., Bitcoin) and has high variance due to the probabilistic nature of mining. Block times can fluctuate significantly depending on the mining difficulty and network conditions. In PoW based blockchains, the average time is lower than PoW, around 15 seconds to a few minutes. This network is more consistent than PoW as block creation depends on validators' stakes rather than computational effort. PoS relies on validators who are chosen based on their stake, leading to more predictable and shorter block times. The proposed PoTE has a very low, typically in the range of a few seconds. This network is highly consistent due to the deterministic nature of trust and expertise scores. PoTE leverages trust and expertise scores to quickly and efficiently validate transactions, leading to significantly lower and more consistent block times compared to PoW and PoS. Pow consumptions extremely high energy s it deals with computationally intensive puzzles. ss consumes a significant amount of electricity. PoTE has no redundant computations, and the process is streamlined for quick and energy-efficient validations.

Computational efficiency is a crucial metric for evaluating and selecting blockchain consensus mechanisms. It measures how effectively a system uses computational resources to achieve its objectives Fig 10 compares the computational efficiencies of various blockchain models. The PoTE has the highest computational efficiency, relying on trust and expertise scores for validation, which requires minimal computational effort and energy. Hence, PoTE provides extremely cost-effective and sustainable, making it ideal for applications with limited resources, such as IoT networks, and for large-scale deployments where scalability and low operational costs are essential. Fig 11 shows the performance of the proposed model in terms of latency, throughput, success rate, and network utilization, which are crucial metrics for evaluating the performance of networked systems like blockchain and distributed computing environments. Latency (Fig 11(a)) refers to the time it takes for data to travel from its source to its destination across a network, which is crucial for real-time applications like financial transactions and online gaming. High latency can lead to delays and poor user experience. Throughput (Fig 11(b)) is the amount of data successfully processed or transmitted within a given period, indicating the system's capacity to handle traffic. Higher throughput indicates a system can handle more transactions or data in less time, ensuring scalability and efficiency.

TABLE 1. Simulation parameters used while evaluating the proposed system.

Parameter	Value
Network Area	1000 square meters
Number of Edge Nodes	50
Blockchain Network	Ethereum-based
Consensus Mechanism	Proof of Authority (PoA)
Block Size	1 MB
Simulation Duration	24 hours
Communication Protocol	MQTT, TCP/IP
Energy Harvesting	Solar panels, Kinetic energy converters
Network Traffic Model	Poisson distribution, Realistic healthcare data traffic patterns

A high success rate (Fig 11(c)) indicates a stable and reliable system, impacting user trust and overall service quality, especially in financial services. Network utilization (Fig 11(d)) measures the extent to which network resources are being used, ensuring efficient use without overloading the network or leaving too much idle capacity. Optimal utilization balances between overuse, which can cause congestion and slowdowns, and underuse, which may indicate overcapacity and unnecessary costs. These performance metrics are shown in the Table 3.

Fig 12 illustrates the load balancing efficiency of the proposed model, which measures the distribution of the network's workload evenly across nodes. This is crucial to prevent bottlenecks and reduced system performance. Initially, with 50 nodes, the model achieves a load balancing efficiency of 1, indicating an optimal workload distribution. As the node count increases to 100 and beyond, slight variations in load balancing efficiency are observed, indicating a high level of efficiency in workload distribution across an increasing number of nodes. These changes reflect the system's adaptive mechanisms to maintain operational efficiency. Staying high load balancing efficiency with increasing nodes is significant for several reasons, including scalability, resource utilization, and system reliability and performance. Expanding the number of nodes can significantly enhance data processing capabilities, reliability, and system resilience, especially in healthcare applications. The model's advanced design in handling increased network size is crucial for achieving these benefits.

The graph in Fig 13 shows the throughput of transactions against the node count for three different consensus mechanisms: Proof of Work (PoW), Proof of Stake (PoS), and the proposed Proof of Trust and Expertise (PoTE). PoW starts at a high point, suggesting a low node count can process

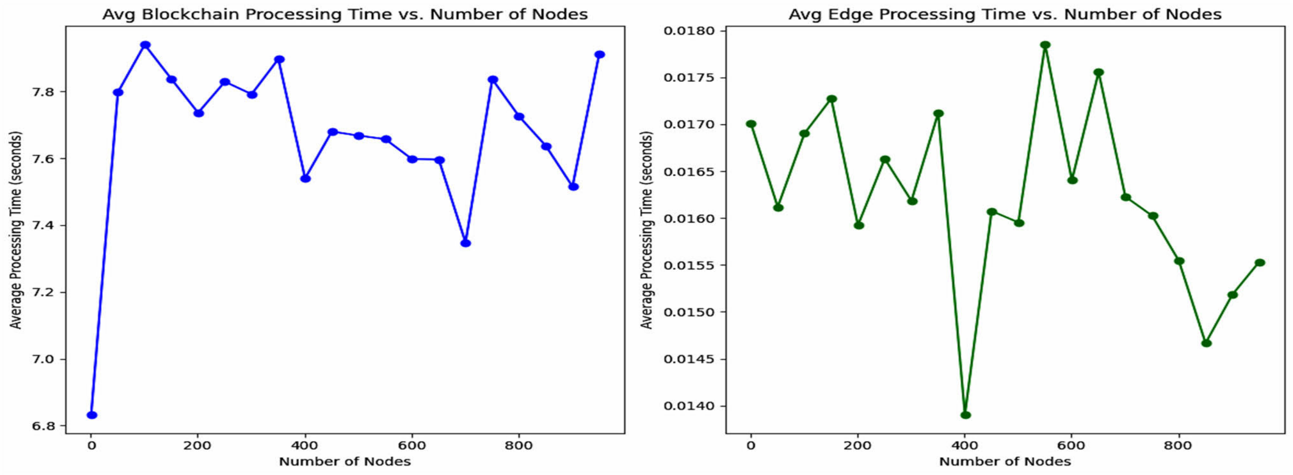


FIGURE 8. Processing times in blockchain and edge nodes as a function of increasing nodes.

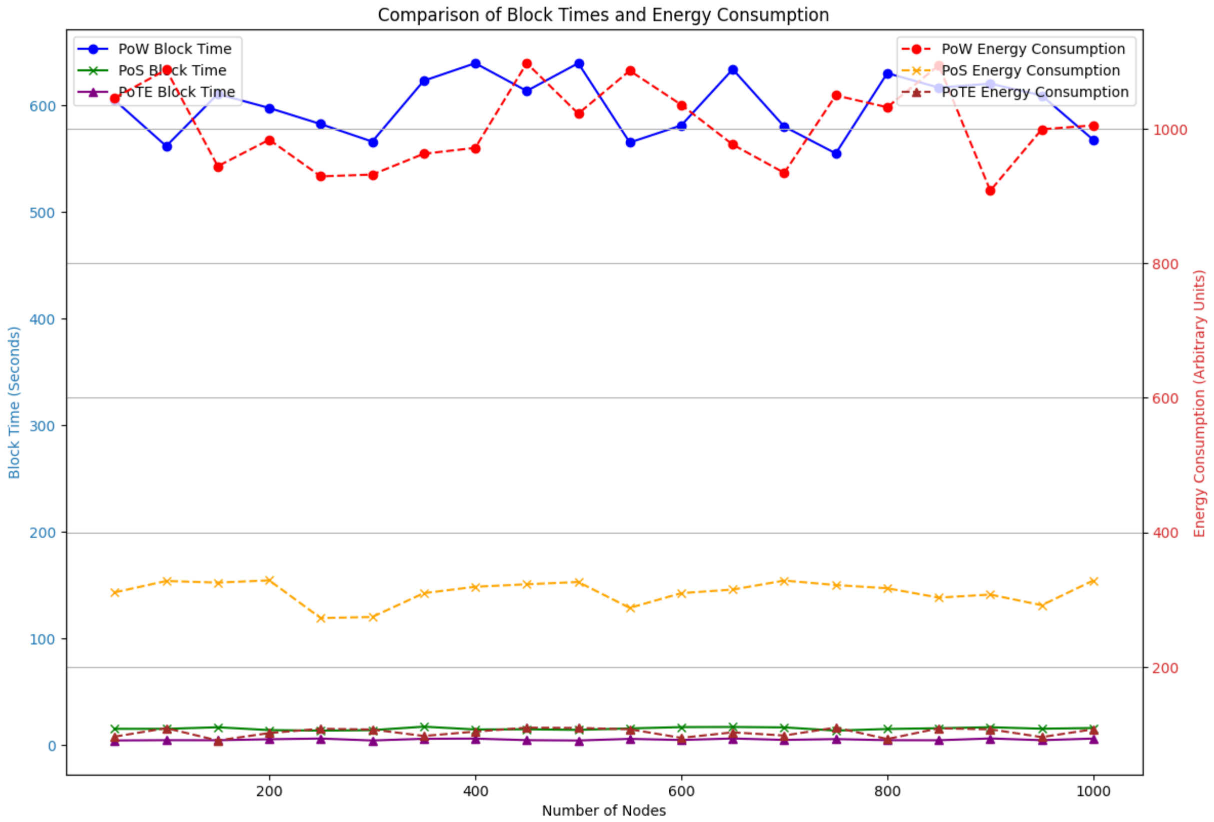


FIGURE 9. Comparison of block times and energy consumption in various blockchain networks.

large transactions quickly. As the node count increases, the throughput for PoW dramatically decreases, likely due to the high computational effort required to validate transactions. PoS starts high, indicating good performance with fewer nodes. However, the throughput decreases as more nodes are added but not as sharply as PoW. Proof of Trust and Expertise (PoTE) shows a flatter curve compared to PoW and PoS, maintaining its throughput better as the node count increases. This shows a significant advantage in scalability, allowing the proposed model to handle a large number of nodes without a substantial decrease in performance.

From the graph it is evident that PoTE is more scalable than PoW and PoS in terms of throughput as the network grows, which is critical for blockchain networks that need to

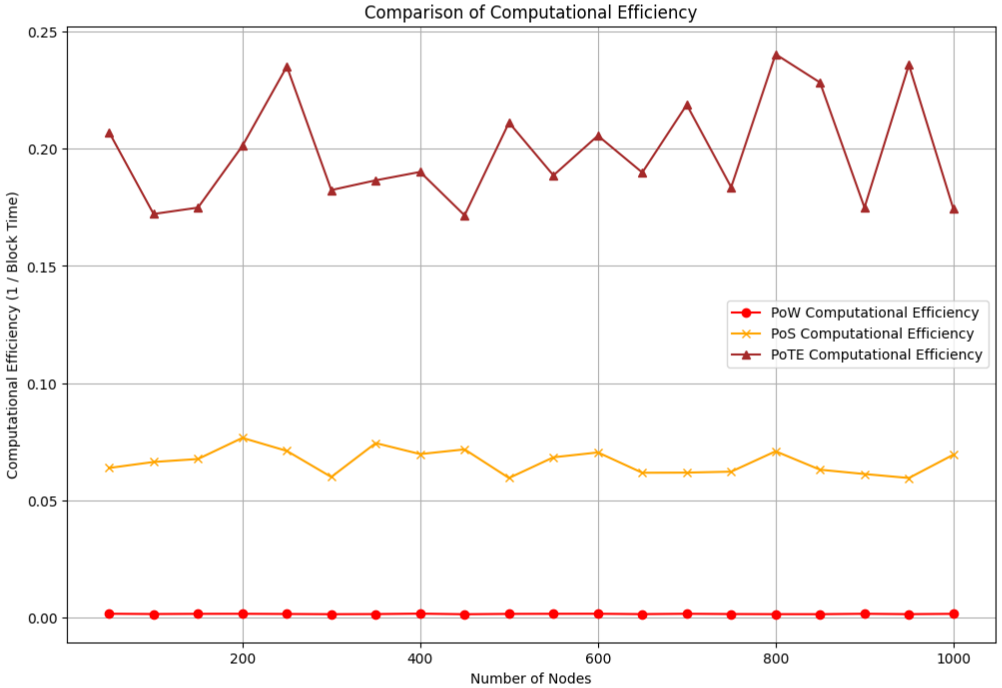
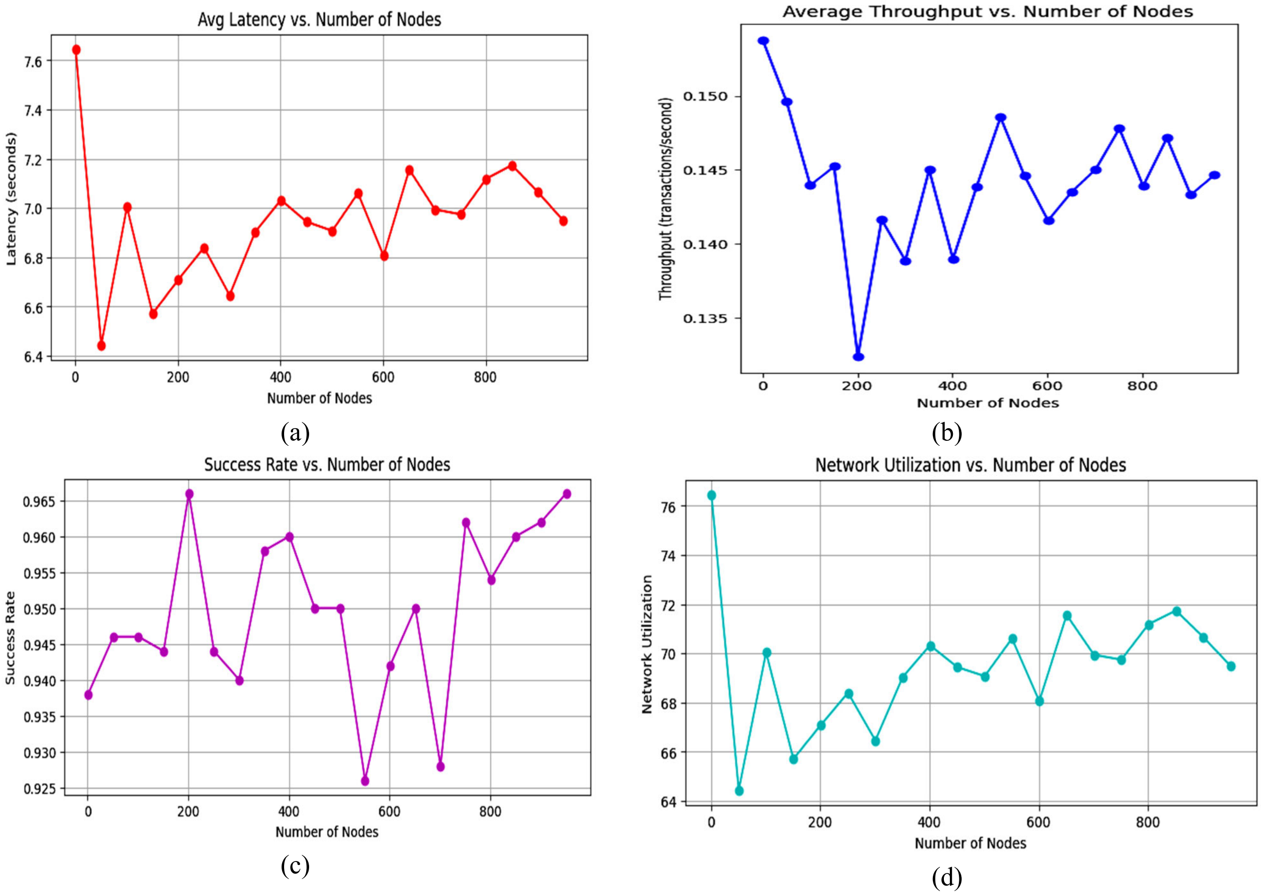


FIGURE 10. Comparison of various blockchain models in terms of computational efficiency.



(a)

(b)

(c)

(d)

FIGURE 11. Performance of the proposed model in terms of (a) Latency (b) Throughput (c) Success rate (d) Network Utilization.

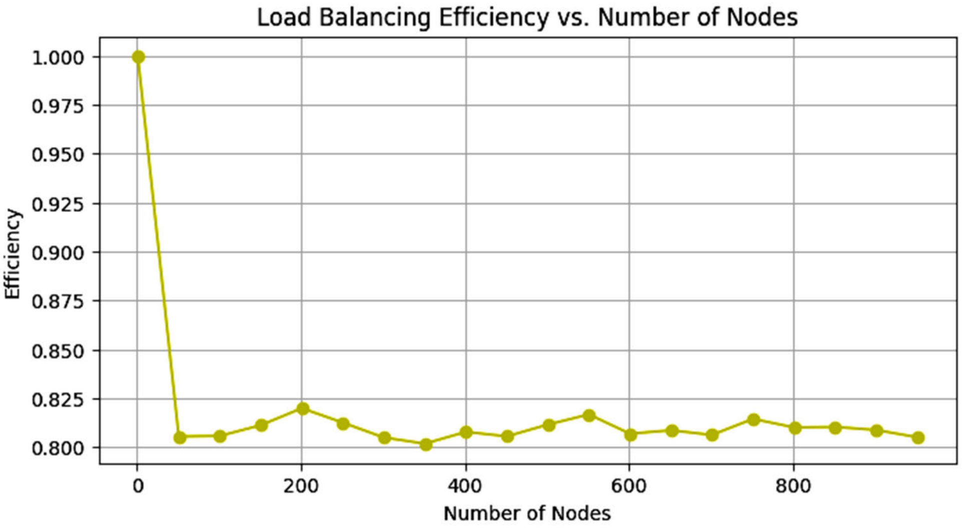


FIGURE 12. Load balancing in the proposed model as function of increasing nodes.

TABLE 2. Average processing times in blockchain and edge networks in the proposed system.

Nodes	Avg Blockchain Processing Time (S)	Avg Edge Processing Time (S)
50	6.832896	0.017006
100	7.797276	0.016118
150	7.939972	0.016902
200	7.837104	0.017274
250	7.73596	0.015923
300	7.829088	0.016632
350	7.79169	0.016184
400	7.896883	0.017119
450	7.53995	0.013904
500	7.679927	0.016075
550	7.667702	0.015954
600	7.657203	0.01785
650	7.597469	0.016403
700	7.596275	0.017556
750	7.347746	0.016228
800	7.836325	0.016025
850	7.725422	0.015544
900	7.6373	0.014666
950	7.515387	0.015183
1000	7.912344	0.015531

maintain performance despite increasing node numbers. PoTE effectively balances the load across the network, preventing any single node from becoming a bottleneck. Additionally, PoTE and PoS are likely to be more energy-efficient, with PoTE showing the best performance, potentially leading to lower operational costs.

Fig 14 shows the comparison of latency as a function of increasing node count for three consensus mechanisms namely, PoW, PoS, and the proposed Proof of Trust and Expertise (PoTE). PoW and PoS starts with low latency, indicating quick transactions with a small number of nodes. As the number of nodes increases, the latency increases significantly due to computational difficulty. The PoTE mechanism maintains low latency even as the number of nodes grows. This indicates its efficiency and scalability, making it suitable for large-scale applications requiring fast transaction processing times without compromising growth and addition of new nodes. The PoTE mechanism's ability to maintain low latency with increasing nodes highlights its scalability, responsiveness, resource management, and user experience. In conclusion, the proposed PoTE mechanism outperforms both PoW and PoS in maintaining low latency across various network sizes, making it better suited for large-scale applications requiring fast transaction processing times without compromising growth and addition of new nodes.

The graph shown in Fig. 15 demonstrates the success rate of three different consensus mechanisms PoW consensus shows a significant decline in success rate as node count increases, suggesting challenges in maintaining a high success rate as the network scales. PoS consensus shows a less severe decline but stabilizes at a higher success rate as node count increases. This may be due to PoS's reliance on stake rather than computational power, reducing conflicts and errors during consensusPoTE mechanism shows a small initial dip but maintains a stable success rate across different network sizes, indicating its resilience to network scaling and effective transaction integrity. The PoTE mechanism's high success rate is crucial for applications requiring consistent and reliable transaction processing, such as healthcare data management. Its efficiency suggests that the system can

TABLE 3. Performance metrics in the proposed system.

Nodes	Avg Throughput (TPS)	Avg Latency (S)	Total Energy Consumption (mJ)	Success Rate	Network Utilization (%)	Load Balancing Efficiency
50	0.130783	7.646235	0.05	0.938	76.46235	1
100	0.155179	6.444169	2.55	0.946	64.44169	0.805527
150	0.142765	7.004506	5.05	0.946	70.04506	0.805812
200	0.152188	6.570813	7.55	0.944	65.70813	0.811288
250	0.149059	6.708758	10.05	0.966	67.08758	0.819966
300	0.146202	6.839865	12.55	0.944	68.39865	0.812596
350	0.150463	6.64617	15.05	0.94	66.4617	0.804988
400	0.14485	6.903702	17.55	0.958	69.03702	0.801859
450	0.142187	7.033013	20.05	0.96	70.33013	0.807876
500	0.144004	6.944237	22.55	0.95	69.44237	0.805598
550	0.144768	6.907589	25.05	0.95	69.07589	0.811601
600	0.141631	7.060608	27.55	0.926	70.60608	0.8168
650	0.146934	6.805778	30.05	0.942	68.05778	0.806952
700	0.139736	7.156371	32.55	0.95	71.56371	0.808679
750	0.14297	6.994482	35.05	0.928	69.94482	0.80631
800	0.143379	6.974509	37.55	0.962	69.74509	0.814516
850	0.140468	7.119049	40.05	0.954	71.19049	0.810173
900	0.139385	7.174385	42.55	0.96	71.74385	0.81041
950	0.141515	7.066388	45.05	0.962	70.66388	0.808837
1000	0.143904	6.949075	47.55	0.966	69.49075	0.805169

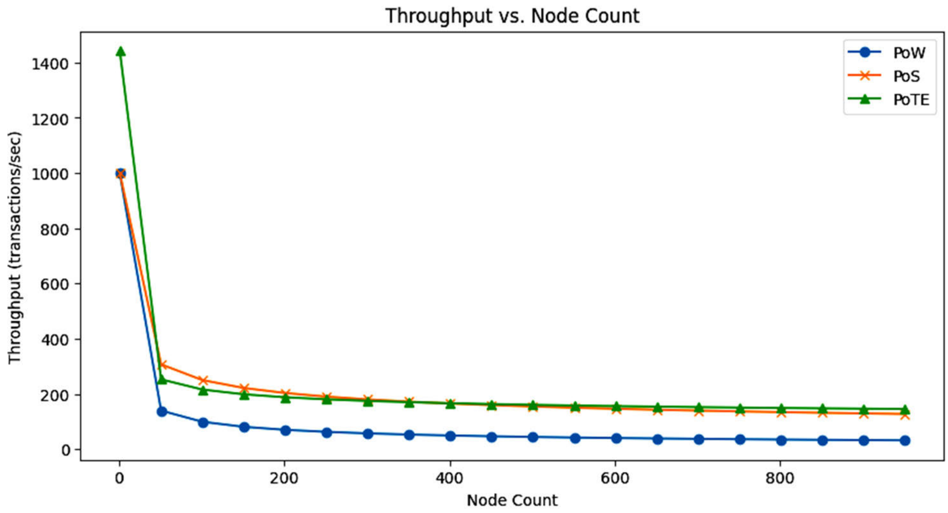


FIGURE 13. Comparative analysis of throughput between the proposed and standard models as function of increasing nodes.

resolve inconsistencies or errors with a small increase in nodes, ensuring high-quality service without extensive reprocessing or error correction.

Fig.16 shows the network utilization as a function of increasing node count. This figure compares the network utilization percentages of three different blockchain consensus algorithms, PoW (Proof of Work), PoS (Proof of Stake), and PoTE (Proof of Elapsed Time). The graph shows that PoW's network utilization increases significantly with the number of nodes, suggesting that its efficiency decreases as the network grows. PoS shows a more linear growth in network utilization, suggesting better scalability. PoTE appears to have the best

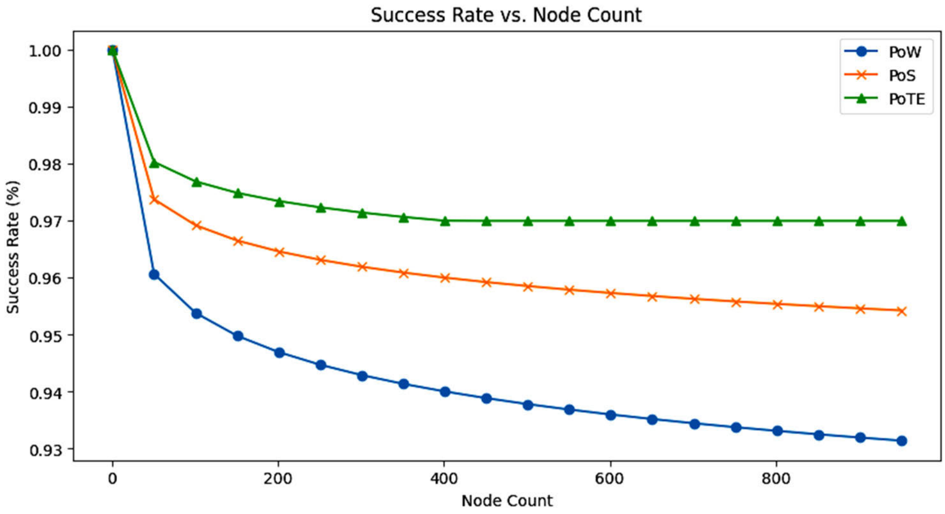


FIGURE 14. Comparative analysis of latency between the proposed and standard models as function of increasing nodes.

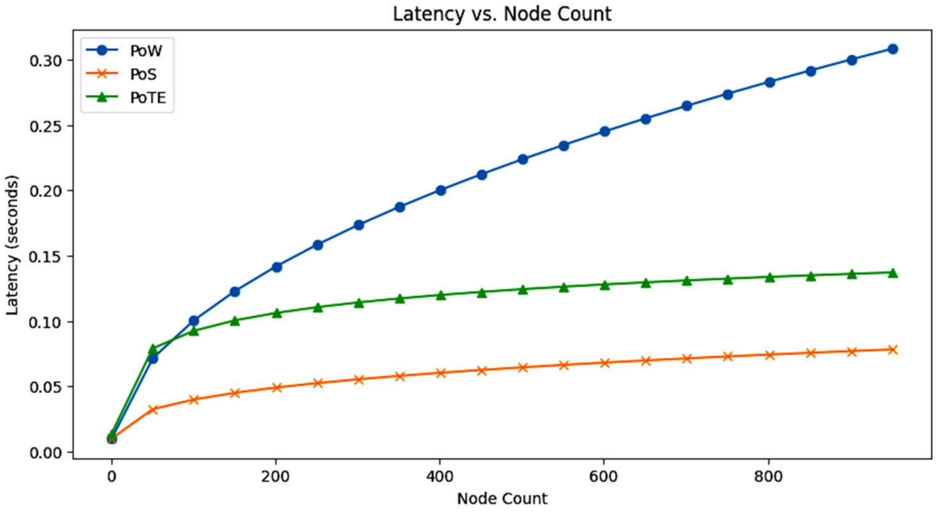


FIGURE 15. Comparative analysis of successful validations between the proposed and standard models as function of increasing nodes.

scalability, as its network utilization remains constant despite the increasing number of nodes. PoS increases in utilization more gradually, suggesting it might be more efficient than PoW at scale but less efficient than PoTE. It is also evident that the network load each algorithm puts on the system as it grows. PoW starts low but increases significantly, implying a higher computational load as more nodes participate. PoS increases steadily, suggesting a predictable growth in load. PoTE maintains a consistent load, which could be advantageous for planning and resource allocation.

Fig 17 shows the average consensus time in seconds for three different consensus mechanisms PoTE mechanism shows relatively low and stable consensus times across varying node counts, suggesting it can handle increased loads without significantly impacting the time it takes to reach consensus. PoW mechanism shows the highest consensus times, with considerable variability, suggesting a decrease in efficiency. The Proof of Stake (PoS) mechanism presents an intermediate range of consensus times between PoTE and PoW, with some fluctuations but maintaining a trend lower than PoW but higher than PoTE. The proposed PoTE model's low and stable consensus times suggest it is highly scalable, capable of maintaining efficiency despite an increase in the number of nodes. Its lower average consensus time compared to PoW and PoS indicates it is more efficient, which is critical for applications requiring quick transaction validation, such as healthcare data management. The stability of the consensus time in PoTE also points to its reliability, which is essential for maintaining trust in distributed ledger technologies, especially in healthcare.

Block finality time, shown in Fig 18, is crucial for determining the security and efficiency of a blockchain. Shorter

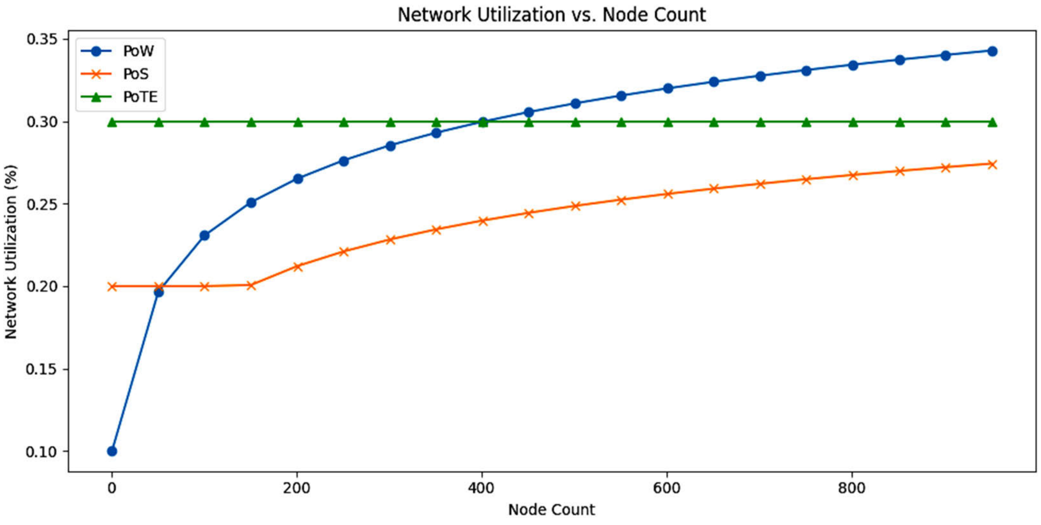


FIGURE 16. Comparative analysis of network utilization between the proposed and standard models as a function of increasing nodes.

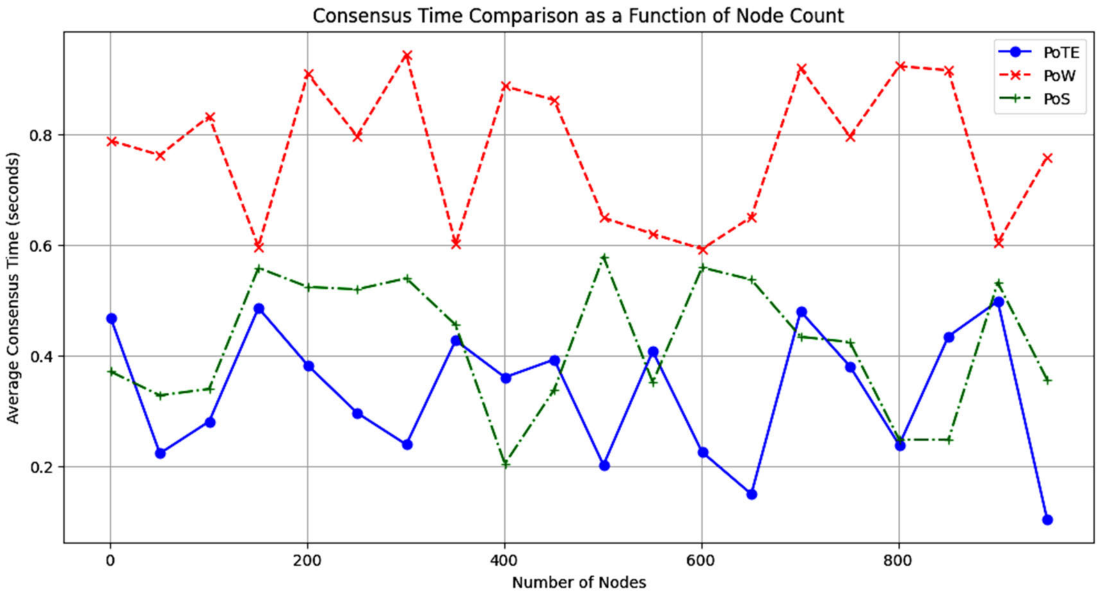


FIGURE 17. Comparison between various consensus mechanisms in terms of average consensus time.

finality times lead to quicker transactions, making them secure and immutable, especially in applications like Electronic Health Records (EHR) management. The proposed Proof of Trust and Expertise (PoTE) consensus mechanism is compared to other mechanisms. A shorter finality time indicates a more responsive and scalable system. In healthcare applications, rapid block finality can enhance patient experience by ensuring records are updated and secured quickly. Block finality time measures a blockchain network's responsiveness to new transactions and its ability to reach immutability, a core requirement for secure and reliable operations.

Fig 19 illustrates the Scalability Comparison of various models based on response time and resource utilization. Scalability testing involves assessing how well the system performs as the number of nodes increases. The key metrics analyzed are response time, resource utilization, and network latency. Response Time is the time taken to process a transaction. Resource Utilization indicates the percentage of resources (CPU, memory, etc.) utilized by the system. PoW require high resource consumption leading to increased response time and network latency as the number of nodes increases. PoS provide better scalability than PoW but still shows a gradual increase in response time and

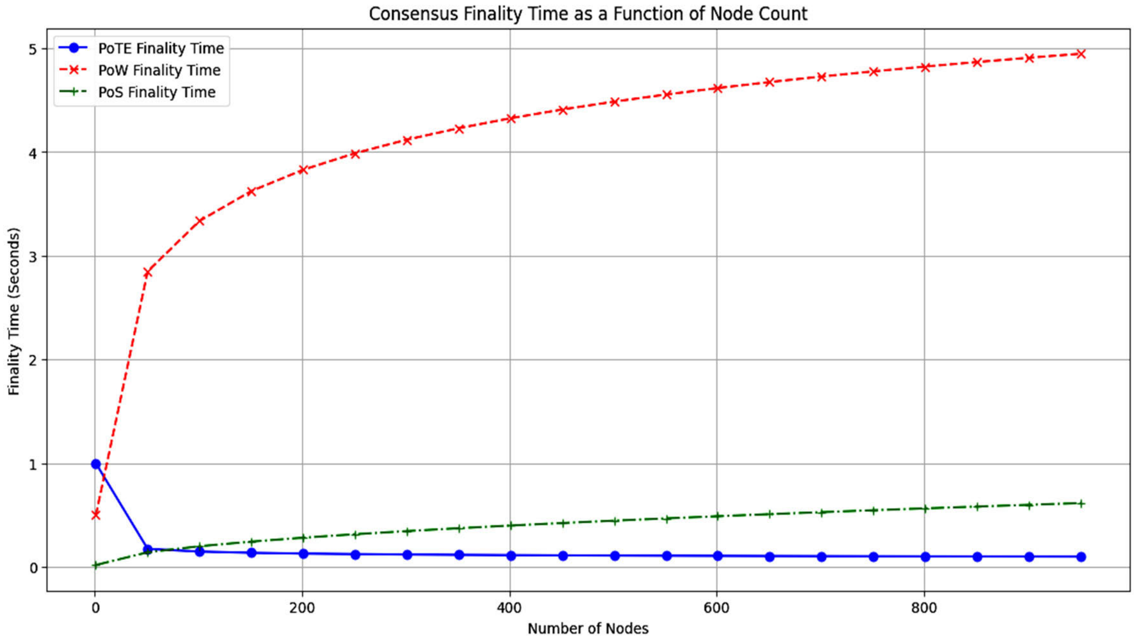


FIGURE 18. Comparison between various consensus mechanisms' finality time.

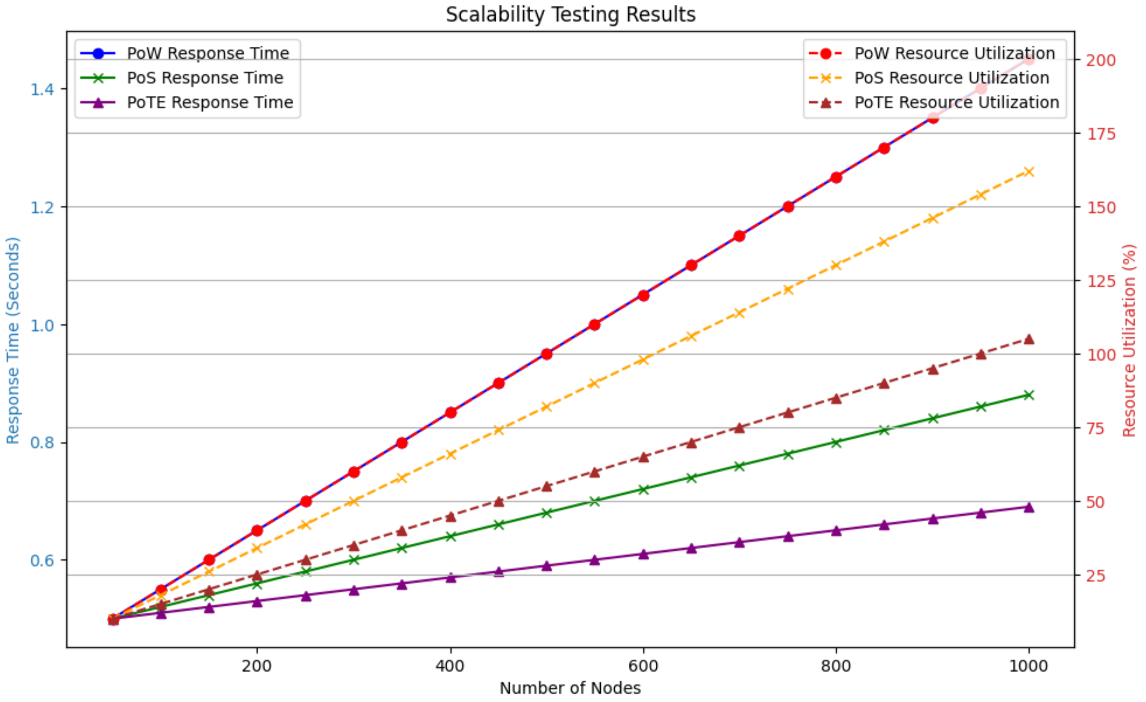


FIGURE 19. Scalability comparison of various models based on response time and resource utilization.

network latency with increasing nodes. The proposed PoTE Demonstrates stable and efficient performance with minimal increase in response time and network latency, indicating superior scalability.

Fig 20 illustrates the security breaches detected in the proposed model and the comparison with other models. Security breaches are evaluated based on the rate at which unauthorized access or tampering is detected. Security breach rate is the frequency of unauthorized access or data tampering incidents. PoW provides a higher breach rates due to vulnerabilities in computational challenges. The PoS offer lower breach rates than PoW but higher than PoTE due to the

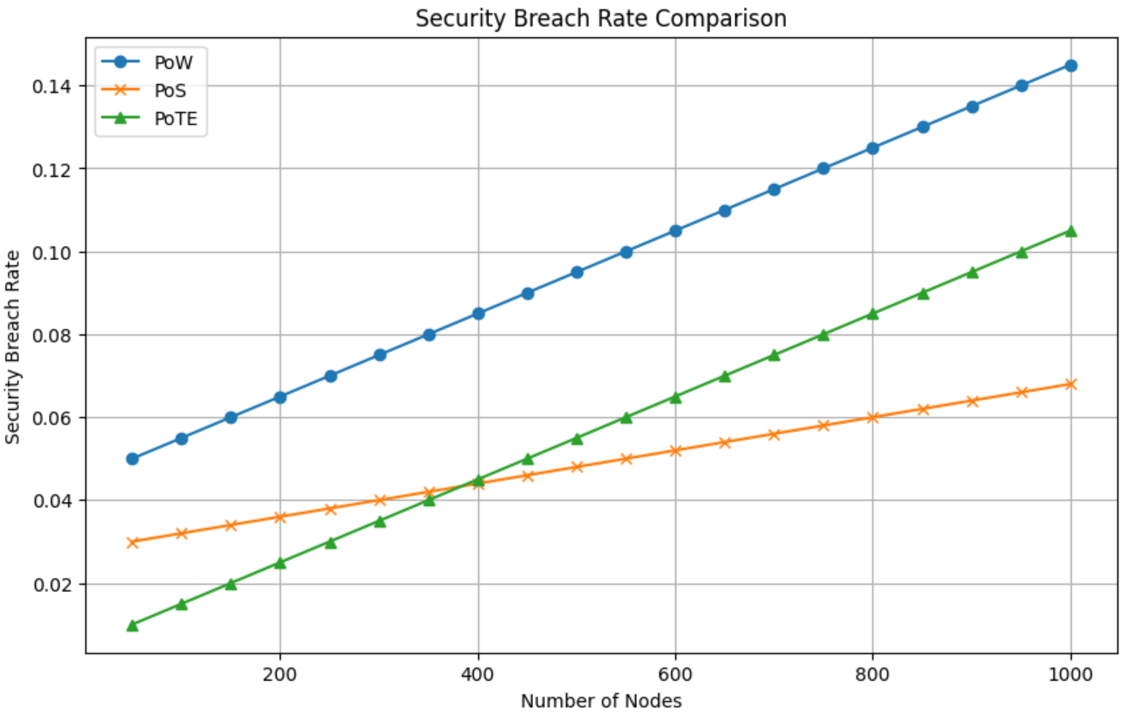


FIGURE 20. Security comparison among various blockchain consensus mechanisms.

potential for attacks on the staking mechanism. The proposed PoTE demonstrated the lowest breach rates, highlighting its robustness and enhanced security measures.

The system integrates multiple compliance measures to adhere to key regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union.

A. DATA ENCRYPTION

- **At Rest:** Data stored on the blockchain and edge devices is encrypted using advanced encryption standards (AES-256).
- **In Transit:** Data transmitted between edge devices and the blockchain is encrypted using Transport Layer Security (TLS) to prevent interception and tampering.

B. LEGAL IMPLICATIONS

- **HIPAA Compliance:** Ensures that all protected health information (PHI) is encrypted, meeting HIPAA's requirements for data security.
- **GDPR Compliance:** Satisfies GDPR requirements for data protection by ensuring data is secure both at rest and in transit.

C. ACCESS CONTROL

- Access to data is restricted based on user roles and permissions.
- **Smart Contracts:** Implemented to enforce access control policies on the blockchain.

The future prospects of this integration in the healthcare sector are highly promising. As these technologies progress and overcome initial challenges, they are poised to revolutionize the field of healthcare data management. The integration's full potential can be realized through research and development, as well as collaborative endeavors among technologists, healthcare experts, and policymakers.

V. CONCLUSION

The proposed method of integrating edge computing and blockchain in healthcare applications offers a promising solution to address the technical challenges and limitations of existing systems. The method enhances security and privacy by leveraging blockchain's cryptographic techniques and decentralized consensus mechanisms, along with the local data processing and encryption capabilities of the edge computing. This ensures data integrity and immutability, while edge devices enable secure local storage and processing, reducing the risk of unauthorized access and data breaches. Improved scalability and performance are achieved by distributing data storage and processing tasks across a network of edge devices and blockchain nodes. This ensures high performance and responsiveness, even as the volume of healthcare data grows. The method promotes interoperability and seamless data exchange between different healthcare entities through the use of blockchain's decentralized ledger and smart contracts. Blockchain's transparency and auditability mechanisms enhance trust among stakeholders by enabling them to verify the integrity and provenance of healthcare data at any time. The combined power of edge computing and blockchain opens up new opportunities for innovative healthcare applications, such as remote patient monitoring, personalized medicine, clinical trials, and population health management. The proposed model provides a reliable and scalable blockchain platform for healthcare applications by exhibiting an average consensus and finality times as low as 0.0089 seconds and 0.02 seconds, respectively.

REFERENCES

[1] S. Kraus, F. Schiavone, A. Pluzhnikova, and A. C. Invernizzi, "Digital transformation in healthcare: Analyzing the current state-of-research," *J. Bus. Res.*, vol. 123, pp. 557–567, Feb. 2021.

[2] G. Sarkar and S. K. Shukla, "Behavioral analysis of cybercrime: Paving the way for effective policing strategies," *J. Econ. Criminol.*, vol. 2, Dec. 2023, Art. no. 100034.

[3] M. Paul, L. Maglaras, M. A. Ferrag, and I. Almomani, "Digitization of healthcare sector: A study on privacy and security concerns," *ICT Exp.*, vol. 9, no. 4, pp. 571–588, Aug. 2023.

[4] L. U. Khan, I. Yaqoob, N. H. Tran, S. M. A. Kazmi, T. N. Dang, and C. S. Hong, "Edge-computing-enabled smart cities: A comprehensive survey," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10200–10232, Oct. 2020.

[5] Z. Yang, B. Liang, and W. Ji, "An intelligent end–edge–cloud architecture for visual IoT-assisted healthcare systems," *IEEE Internet Things J.*, vol. 8, no. 23, pp. 16779–16786, Dec. 2021.

[6] F. Wu, C. Qiu, T. Wu, and M. R. Yuce, "Edge-based hybrid system implementation for long-range safety and healthcare IoT applications," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 9970–9980, Jun. 2021.

[7] M. S. Arbabi, C. Lal, N. R. Veeraragavan, D. Marijan, J. F. Nygård, and R. Vitenberg, "A survey on blockchain for healthcare: Challenges, benefits, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 386–424, 1st Quart., 2023.

[8] W. A. N. A. Al-Nbhany, A. T. Zahary, and A. A. Al-Shargabi, "Blockchain-IoT healthcare applications and trends: A review," *IEEE Access*, vol. 12, pp. 4178–4212, 2024.

[9] A. Saini, Q. Zhu, N. Singh, Y. Xiang, L. Gao, and Y. Zhang, "A smart-contract-based access control framework for cloud smart healthcare system," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5914–5925, Apr. 2021.

[10] M. Zarour, M. T. J. Ansari, M. Alenezi, A. K. Sarkar, M. Faizan, A. Agrawal, R. Kumar, and R. A. Khan, "Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records," *IEEE Access*, vol. 8, pp. 157959–157973, 2020, doi: 10.1109/ACCESS.2020.3019829.

[11] A. A. Abdellatif, L. Samara, A. Mohamed, A. Erbad, C. F. Chiasserini, M. Guizani, M. D. O'Connor, and J. Laughton, "MEdge-chain: Leveraging edge computing and blockchain for efficient medical data exchange," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15762–15775, Nov. 2021.

[12] T. R. Gadekallu, Q.-V. Pham, D. C. Nguyen, P. K. R. Maddikunta, N. Deepa, B. Prabadevi, P. N. Pathirana, J. Zhao, and W.-J. Hwang, "Blockchain for edge of things: Applications, opportunities, and challenges," *IEEE Internet Things J.*, vol. 9, no. 2, pp. 964–988, Jan. 2022.

[13] L. D. Costa, B. Pinheiro, W. Cordeiro, R. Araújo, and A. Abelém, "Sec-health: A blockchain-based protocol for securing health records," *IEEE Access*, vol. 11, pp. 16605–16620, 2023.

[14] A. G. Alzahrani, A. Alhomoud, and G. Wills, "A framework of the critical factors for healthcare providers to share data securely using blockchain," *IEEE Access*, vol. 10, pp. 41064–41077, 2022.

[15] G. Wu, S. Wang, Z. Ning, and B. Zhu, "Privacy-preserved electronic medical record exchanging and sharing: A blockchain-based smart healthcare system," *IEEE J. Biomed. Health Informat.*, vol. 26, no. 5, pp. 1917–1927, May 2022.

[16] J. S. Marwaha, A. B. Landman, G. A. Brat, T. Dunn, and W. J. Gordon, "Deploying digital health tools within large, complex health systems: Key considerations for adoption and implementation," *NPJ Digit. Med.*, vol. 5, no. 1, pp. 1–7, Jan. 2022, doi: 10.1038/s41746-022-00557-1.

[17] K. P. Satamraju and B. Malarkodi, "A decentralized framework for device authentication and data security in the next generation internet of Medical Things," *Comput. Commun.*, vol. 180, pp. 146–160, Dec. 2021.

[18] M. Z. U. Rahman, S. Surekha, K. P. Satamraju, S. S. Mirza, and A. Lay-Ekuakille, "A collateral sensor data sharing framework for decentralized healthcare systems," *IEEE Sensors J.*, vol. 21, no. 24, pp. 27848–27857, Dec. 2021.

[19] A. Alzu'bi, A. Alomar, S. Alkhaza'leh, A. Abuarqoub, and M. Hammoudeh, "A review of privacy and security of edge computing in smart healthcare systems: Issues, challenges, and research directions," *Tsinghua Sci. Technol.*, vol. 29, no. 4, pp. 1152–1180, Aug. 2024.

[20] Y. Tang, J. Yan, C. Chakraborty, and Y. Sun, "Hedera: A permissionless and scalable hybrid blockchain consensus algorithm in multiaccess edge computing for IoT," *IEEE Internet Things J.*, vol. 10, no. 24, pp. 21187–21202, Dec. 2023.

[21] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "BEdge-Health: A decentralized architecture for edge-based IoMT networks using blockchain," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11743–11757, Jul. 2021.

[22] X. Wang, X. Ren, C. Qiu, Z. Xiong, H. Yao, and V. C. M. Leung, "Integrating edge intelligence and blockchain: What, why, and how," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 4, pp. 2193–2229, 4th Quart., 2022.

[23] J. Li, D. Li, and X. Zhang, "A secure blockchain-assisted access control scheme for smart healthcare system in fog computing," *IEEE Internet Things J.*, vol. 10, no. 18, pp. 15980–15989.2023, Nov. 2023.

[24] M. T. De Oliveira, L. H. A. Reis, Y. Verginadis, D. M. F. Mattos, and S. D. Olabarriaga, "SmartAccess: Attribute-based access control system for medical records based on smart contracts," *IEEE Access*, vol. 10, pp. 117836–117854, 2022, doi: 10.1109/ACCESS.2022.3217201.

[25] M. T. De Oliveira, L. H. A. Reis, Y. Verginadis, D. M. F. Mattos, and S. D. Olabarriaga, "SmartAccess: Attribute-based access control system for medical records based on smart contracts," *IEEE Access*, vol. 10, pp. 117836–117854, 2022, doi: 10.1109/ACCESS.2022.3217201.

[26] S. Islam, M. J. Islam, M. Hossain, S. Noor, K.-S. Kwak, and S. M. R. Islam, "A survey on consensus algorithms in blockchain-based applications: Architecture, taxonomy, and operational issues," *IEEE Access*, vol. 11, pp. 39066–39082, 2023.

[27] Y. Zhang and F. Zhao, "Consensus algorithm for medical data storage and sharing based on master–slave multi-chain of alliance chain," *High-Confidence Comput.*, vol. 3, no. 3, Sep. 2023, Art. no. 100122.

[28] N. Anita, M. Vijayalakshmi, and S. Mercy Shalinie, "Proof-of-improved-participation: A new consensus protocol for blockchain technology," *Comput. Syst. Sci. Eng.*, vol. 44, no. 3, pp. 2007–2018, 2023.

[29] B. N. Gangothri, K. P. Satamraju, and B. Malarkodi, "Sensor-based ambient healthcare architecture using blockchain and Internet of Things," in *Proc. 10th Int. Conf. Signal Process. Integr. Netw. (SPIN)*, Noida, India, Mar. 2023, pp. 543–546.

[30] O. Samuel, A. B. Omojo, S. M. Mohsin, P. Tiwari, D. Gupta, and S. S. Band, "An anonymous IoT-based E-health monitoring system using blockchain technology," *IEEE Syst. J.*, vol. 17, no. 2, pp. 2422–2433, Feb. 2022.

[31] H. Guo, W. Li, M. Nejad, and C.-C. Shen, "A hybrid blockchain-edge architecture for electronic health record management with attribute-based cryptographic mechanisms," *IEEE Trans. Netw. Service Manage.*, vol. 20, no. 2, pp. 1759–1774, Jun. 2023.

MD. ZIA UR RAHMAN (Senior Member, IEEE) received the M.Tech. and Ph.D. degrees from Andhra University, India.

Since 2013, he has been with the Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, K. L. University, Guntur, India, as a Professor. He has authored or co-authored more than 150 articles on indexed international conferences and journals, and five international books. His main areas of research interests include artificial intelligence, blockchain technology, sensors and sensing methods, signal processing applications, medical telemetry, machine learning, and the Internet of Things. He is a fellow of the Institute of Engineers, India; and the Institute of Biomedical Engineers, India. He is a Scientific Consultant for several national and international institutions. He serves as an Associate Editor for IEEE Access (USA); *Measurement* (Elsevier, NL); *Measurement: Sensors* (Elsevier, NL); and *Measurement: Food* (Elsevier, NL).

SUMALATHA AKUNURI received the M.Tech. and Ph.D. degrees from Andhra University, Visakhapatnam, India. Since 2008, she has been with the Department of Electronics and Instrumentation Engineering, Siddhartha Academy of Higher Education (SAHE)–Deemed to be University, Vijayawada, India, as an Assistant Professor. She has authored or co-authored more than 15 articles in indexed international conferences and journals. Her main areas of research interests include system identification, dynamic modeling of physical systems, sensing and control methods, signal processing applications, and the Internet of Things. She is a member of the International Society of Automation (ISA) and the International Association of Engineers (IAENG). She is a Scientific Consultant of several national institutions.

D. NAGABHUSHANA BABU received the B.Tech. degree in electronics and communications from the Nimra College of Engineering and Technology, JNTUH, the M.Tech. degree in communication systems from the College of Engineering, Andhra university, and the Ph.D. degree in electronics and communication engineering from K. L. University. He is with the Department of Data Science and Information Technology, School of Engineering, Malla Reddy University, Hyderabad. His research interests include communication systems, wireless sensor networks, health care informatics, AI, and ML applications.

M. V. S. RAMPRASAD is a Research Scholar with the Koneru Lakshmaiah Education Foundation, K. L. University. He is also with GITAM (Deemed to be University), Visakhapatnam, Andhra Pradesh, India. His areas of interests include biomedical image processing and VLSI.

SK. MOHAMMED SHAREEF is with the Department of Electronics and Communication Engineering, Narasaraopeta Engineering College. His current research interests include signal processing, medical telemetry applications, healthcare devices, and the IoT.

MASRESHAW DEMELASH BAYLEYEGN received the B.Sc. degree in electrical engineering from Mekelle University, Mekelle, Ethiopia, in 2005, the M.Sc. degree in optics from European Universities, in 2009, under a highly competitive and full scholarship Erasmus Mundus Mobility Program, and the Ph.D. degree in design and development of spectral-domain optical coherence tomography from Paris Sud 11, Paris, France, in 2012. Currently, he is an Assistant Professor with the Center of Biomedical Engineering and also the Dean of the School of Multidisciplinary Engineering, Addis Ababa Institute of Technology, Addis Ababa University, Ethiopia.