A Secure Data Storage Model for Wearable Medical IoT Devices Using Blockchain Technology

Zouhair Elhadari, Hicham Zougagh, Noureddine Idboufker, Mohamed Ech-chebaby, and Samir Elouaham.

Abstract— **In the healthcare domain, the Internet of Things (IoT) plays a crucial role in connecting medical devices to the internet, enabling the automatic collection and exchange of medical data. However, this increased connectivity also introduces cybersecurity risks, including malicious attacks and vulnerabilities in sensitive data storage. To address these challenges, we propose a blockchain-based model specifically designed for secure and scalable healthcare data storage. By leveraging a decentralized architecture, our approach enhances security, traceability, and operational efficiency, mitigating the risks associated with centralized storage systems. The model is designed to support high transaction volumes, with storage throughput scaling from less than 1 byte/second with a small network to over 100 bytes/second as the number of nodes increases, ensuring robust performance under high workloads. Unlike conventional storage solutions, which experience high packet loss rates due to congestion, our system maintains a packet loss rate of 0%, even when processing hundreds of thousands of transactions. Furthermore, our model achieves a 100% success rate in transaction validation, ensuring that all medical data is securely recorded and accessible without failures, unlike existing solutions that suffer from inconsistencies in transaction finalization. In addition to security, the proposed system ensures seamless compatibility with various communication protocols, making it adaptable to diverse healthcare environments. While an increase in network size results in higher latency, reaching a few seconds in large-scale deployments, this trade-off remains within acceptable limits for secure healthcare applications. Through extensive simulations, our study demonstrates that blockchain-based data storage not only enhances security and reliability but also ensures scalability and efficiency, making it a highly suitable solution for managing healthcare data in IoT-driven environments.**

Index Terms—**Blockchain, Internet of Things in healthcare, Secure data storage, Wearable medical devices, Blockchain for medical IoT applications.**

Manuscript received December 13, 2024; revised April 16, 2025.

Zouhair Elhadari is a Ph.D. student in the Department of Computer Science, Faculty of Sciences and Techniques, Moulay Slimane University, Beni Mellal, Morocco. (email: zouhair.hdr@gmail.com).

Hicham Zougagh is a full Professor in the Department of Computer Science, Faculty of Sciences and Techniques, Moulay Slimane University, Beni Mellal, Morocco. (email: h.zougagh@usms.ma).

Noureddine Idboufker is a full Professor in the Department of Telecommunications and Computer Sciences, National School of Applied Sciences, Cady Ayyad University, Marrakech, Morocco. (email: n_idboufker@yahoo.fr).

Mohamed Ech-chebaby is a Ph.D. student in the Department of Computer Science, Faculty of Sciences and Techniques, Moulay Slimane University, Beni Mellal, Morocco. (email: med.echchebaby@gmail.com).

Samir elouaham is a full Professor in the Department of Physics, Chouaib Doukkali University, Eljadida, Morocco. (email: elouahamsamir@gmail.com).

I. INTRODUCTION

The rapid adoption of Medical Internet of Things (MIoT) technologies is transforming healthcare by enabling real-time data collection, remote patient monitoring, and automated medical processes. MIoT devices offer significant advantages, including enhanced efficiency [1] and automation [2]. However, their deployment also introduces critical cybersecurity challenges, such as vulnerability to malicious attacks, weak authentication mechanisms, and unauthorized data access [3], [4], [5]. These security concerns threaten the integrity, confidentiality, and availability of sensitive medical data, making it imperative to develop robust protection mechanisms [6], [7].

Blockchain technology has emerged as a promising solution for securing MIoT ecosystems by leveraging decentralization, immutability, and cryptographic security. However, traditional blockchain implementations face challenges related to scalability, storage efficiency, and resource constraints of IoT devices. To address these limitations, we propose an optimized blockchain-based data storage model tailored for wearable medical IoT devices.

The main contributions of this work are as follows:

- A novel blockchain-based framework designed to ensure the secure storage of medical data collected from wearable MIoT devices.
- A dual blockchain architecture integrating a local blockchain for temporary data buffering and a public blockchain for permanent storage.
- An authentication mechanism using a voting-based Proof of Stake (PoS) consensus, enhancing security and access control for connected devices.
- A scalable and adaptable model capable of integrating a large number of MIoT devices without compromising performance.
- A hybrid deployment strategy, enabling seamless integration of blockchain technology with wearable medical IoT sensor networks.

To validate the effectiveness of our approach, we perform extensive performance evaluations, focusing on key metrics such as latency, storage throughput, packet loss rate, and success rate. Our findings demonstrate that the proposed model offers enhanced security, scalability, and efficiency compared to existing blockchain-based solutions.

The remainder of this article is structured as follows: Section 2 reviews related work in MIoT security and blockchain integration. Section 3 presents the security mechanisms of blockchain technology in the context of MIoT. Section 4 details the proposed data storage model and its authentication mechanism. Section 5 discusses the simulation scenarios, results, and performance evaluation. Finally, Section 6 concludes the paper and outlines future research directions.

II. Related works

This section provides a comprehensive and detailed review of the related works on the application of blockchain technology in healthcare data storage.

Blockchain technology has gained increasing attention in the healthcare industry, particularly in securing and managing medical data. Several studies have explored its potential applications, ranging from electronic health records (EHRs) to supply chain management and drug traceability.

A report from Allied Market Research [45] states that the global blockchain in healthcare market was valued at $531.19 million in 2021 and is projected to reach $16.30 billion by 2031, with a compound annual growth rate (CAGR) of 40.8% from 2022 to 2031. This rapid growth is driven by the rising demand for secure, interoperable, and transparent healthcare data management solutions.

One of the key applications of blockchain in healthcare is the enhancement of security, privacy, and accessibility of EHRs. Traditional centralized EHR systems are prone to security breaches, unauthorized access, and data tampering. Several studies have proposed blockchain-based EHR models to mitigate these risks. Study [8] developed a blockchain-based method for assessing the sufficiency of medical data, ensuring tamper-proof storage and allowing patients to retain control over their health records. Similarly, Study [9] introduced a patient-centric blockchain architecture utilizing BigchainDB, IPFS, and AES encryption to enhance access control in EHR management. Study [10] further explored blockchain's role in healthcare, detailing its architecture, security challenges, and interoperability constraints under regulatory frameworks like HIPAA. While these studies highlight blockchain's potential in securing EHRs, they mainly focus on permissioned blockchain models and do not extensively address challenges related to cross-institutional data sharing and real-time access.

Beyond EHRs, blockchain has been widely investigated for secure medical data exchange and interoperability between healthcare providers. Study [11] analyzed security risks across blockchain layers and discussed its applicability in healthcare data sharing. Research [12] proposed a blockchain-based deep reinforcement learning framework to optimize medical data scheduling while ensuring secure data transmission. Additionally, Study [13] introduced LightMED, a blockchain-enabled access control mechanism integrated with fog computing and CP-ABE to secure electronic medical records in cloud environments. These studies demonstrate blockchain's ability to enhance data sharing security; however, most solutions introduce computational overhead due to cryptographic operations, limiting their feasibility for resource-constrained IoT-based healthcare systems.

Ensuring drug authenticity and preventing counterfeit pharmaceuticals is another critical application of blockchain in healthcare. Study [14] presented a blockchain-based decentralized patient-centric healthcare data management (PCHDM) framework to enhance drug authenticity and traceability. Similarly, Study [15] developed a smart contract-based verification system for drug authentication, while Study [16] explored various smart contract-based tracking mechanisms to improve transparency in pharmaceutical supply chains. Despite these advancements, current solutions often overlook scalability concerns, as storing and verifying large volumes of pharmaceutical transaction data on the blockchain remains computationally expensive.

Blockchain has also been leveraged to enhance the integrity and transparency of clinical trial data and laboratory test management. Study [17] proposed a blockchain framework for immutable and verifiable clinical trial records, preventing data manipulation and fraud. Additionally, Study [18] demonstrated the use of smart contracts to automate patient consent processes, ensuring ethical compliance and secure record management. While these studies offer promising solutions, challenges remain in integrating blockchain with existing clinical trial management systems and ensuring regulatory compliance across different jurisdictions.

Although blockchain presents significant opportunities in healthcare, existing research has several limitations. Many studies focus on specific applications such as EHR security, data exchange, or drug traceability, but few provide a comprehensive, integrated solution that addresses multiple aspects of secure medical data storage and access control. Moreover, issues such as blockchain scalability, high energy consumption, and regulatory compliance remain underexplored. In this work, we propose a secure and scalable blockchain-based data storage model for wearable medical IoT devices, addressing these limitations by integrating lightweight cryptographic techniques and an optimized smart contract mechanism to enhance security, privacy, and efficiency.

III. Overview of Blockchain Technology for Medical IoT data storage Concept

In the realm of medical IoT, blockchain technology offers a groundbreaking approach to secure data storage [19], [20], [21]. By using a distributed ledger system, each data block is cryptographically linked, ensuring the system's security [22], [23], immutability, and tamper resistance [24]. This ledger functions like a database, organizing data chronologically and regulating access through permissions. The primary objective of this paper is to introduce a blockchain-based data storage architecture for medical IoT applications, providing a robust and secure solution for managing sensitive healthcare data storage.

Using blockchain technology for data storage offers a secure solution, particularly for medical IoT sensor networks. Blockchain introduces several key features that are highly beneficial for data storage, such as:

Immutability: Blockchain ensures the immutability of stored data [25], meaning that once data is stored in a block, it cannot be altered. This feature enhances traceability and

auditability, which are critical aspects of healthcare data management.

Decentralization and Distribution: These features are fundamental to blockchain technology [26], [27], [28]. Decentralization eliminates the need for centralized data storage systems that are vulnerable to cyber-attacks. By employing a peer-to-peer (P2P) architecture, data transfers occur directly between nodes, reducing the risk of system-wide failures [26]. In addition, data redundancy across multiple nodes enhances resilience against cyber-attacks, ensuring both data integrity and availability.

Consensus Mechanism: Consensus mechanisms are crucial for ensuring the integrity and security of data in a decentralized blockchain network [29], [30]. They establish rules that all nodes in the medical network must follow, preventing unauthorized modifications or tampering. Without a consensus mechanism, the network is vulnerable to exploitation by malicious entities, which could undermine the validity and integrity of the data.

Despite these advantages, conventional blockchain models often introduce high computational overhead, making them impractical for resource-constrained MIoT devices. Our approach enhances blockchain-based MIoT data storage by addressing key challenges related to security, scalability, and efficiency. To mitigate network congestion, our adaptive blockchain architecture dynamically adjusts block sizes based on demand, ensuring efficient data processing with low latency. Additionally, we integrate a lightweight consensus mechanism designed for resource-constrained MIoT devices, reducing computational overhead while preserving transaction integrity. By supporting high-throughput data handling and maintaining reliability under varying workloads, our model provides a robust, scalable, and efficient solution for secure medical record storage in IoT-driven healthcare environments.

IV. Data Storage Model for Wearable Medical IoT Devices Using Blockchain Technology

In this section, we present the architecture of our proposed data storage model for wearable MIoT devices utilizing blockchain technology. We describe the key components of the system and outline their roles and interactions in managing data storage.

A. The proposed model

Blockchain technology revolutionizes MIoT networks by reducing the reliance on centralized servers for critical functions such as data storage and authentication. It enhances data integrity, privacy, and accessibility through smart contracts, thereby reducing administrative burdens and improving patient outcomes.

Blockchain introduces a decentralized and distributed approach to managing both data and nodes within a P2P network. In our system, wearable medical device (WMD) nodes retain full control over the network, with any new WMD requiring approval from existing nodes via the consensus mechanism. The architecture of the WMD network utilizing blockchain technology is illustrated in Figure 1.

The proposed model integrates an innovative modular approach by utilizing both a public blockchain and a lightweight blockchain for the storage of the data collected by WMDs.

A description of the main entities in proposed architecture is developed as follows:

Local Blockchain: This complementary ledger in the proposed architecture manages node identities and stores hash addresses referencing data packets on the public blockchain. It records key information, such as the total number of data packets, the ID of the validator node, and the address of new blocks added to the public blockchain.

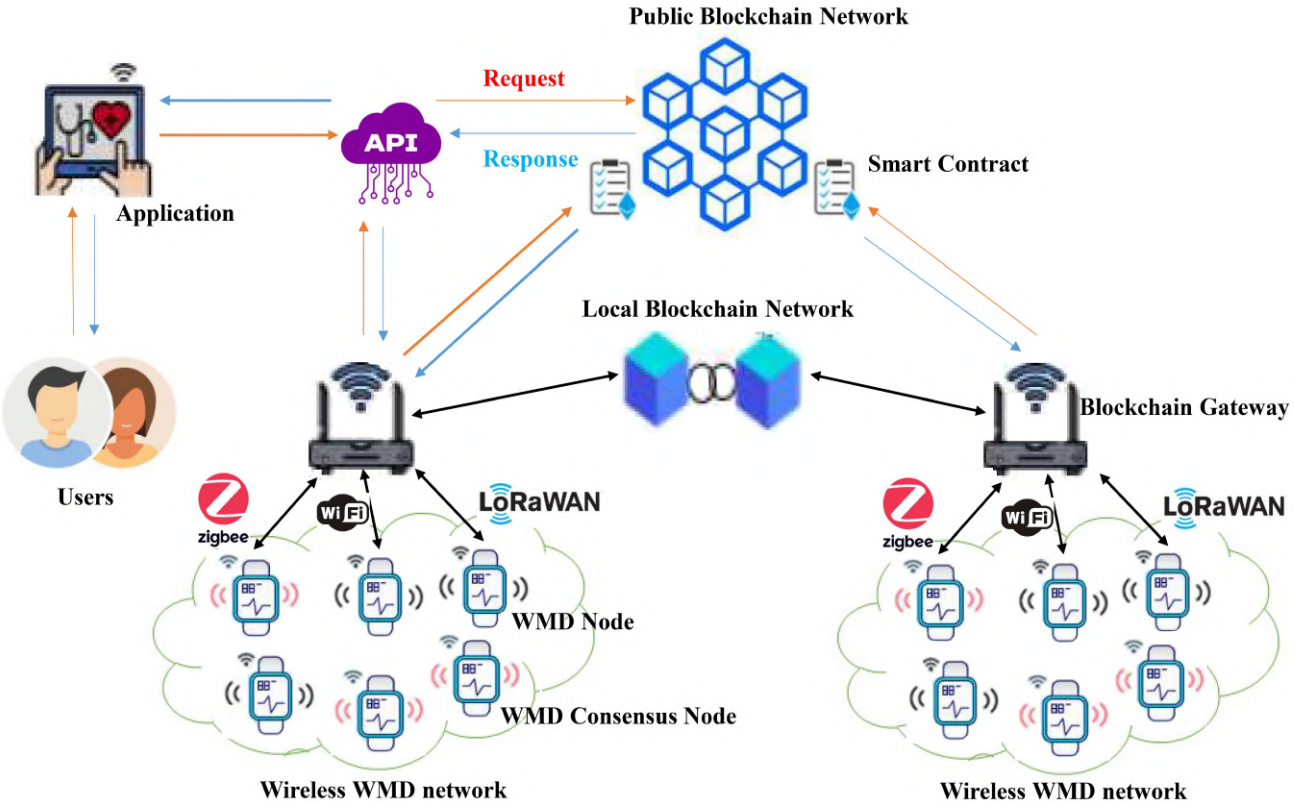

Fig 1: Proposed blockchain WMD architecture

Public blockchain: Serving as a comprehensive database, the public blockchain stores all data received from WMD nodes, including node authentication and registration details. It operates as a P2P system, where each blockchain storage entity maintains a complete copy of the blockchain for redundancy. These entities generally possess robust storage and computational capabilities, enabling the reconstruction of the entire system from a single node in case of data loss due to node inaccessibility [31].

WMD Nodes: Within the WMD network [32], [33], there are two distinct types of nodes: sensor nodes and consensus nodes, each serving specific functions.

- Sensor Nodes: These nodes collect environmental data, operate with limited resources, and transmit information to the blockchain gateway at specified intervals. They receive instructions from WMD consensus nodes and are designed to minimize power consumption[34].
- Consensus Nodes: These nodes collect data and execute consensus mechanisms. They are typically powered by mains and designed to avoid excessive power consumption.

Both sensor and consensus nodes communicate bidirectionally with the blockchain gateway.

Blockchain gateway: The blockchain gateway plays a pivotal role in communicating with WMDs to collect and transmit data for storage on the public blockchain[35]. It facilitates interactions with consensus WMD nodes during node registration and validator selection processes. Equipped with higher computational power, the gateway supports validator WMD nodes in their network validation tasks. Additionally, the blockchain gateway maintains a lightweight copy of the public blockchain and oversees the implementation of the network consensus mechanism, selecting validators through mechanisms such as Proof of Stake (PoS) to add new blocks [36],[46].

Smart contracts (SCs): SCs automate predefined functions within the blockchain [37]. In our architecture, SCs operate at the public blockchain level managing tasks within the WSN ecosystem such as sensor node registration and facilitating communication between the public blockchain and the blockchain gateway. These contracts ensure automated and secure interactions, delivering predetermined results with minimal risk of error. Once deployed on the blockchain, SCs are immutable, meaning they cannot be updated or have additional features added to their source code.

Application Programming Interface (API): In our proposed architecture, blockchain queries are handled through an API [38], [39]. The API's sole function is to retrieve data from the blockchain, allowing only GET requests and prohibiting data addition via POST requests. To effectively respond to user queries, the API requires two parameters: the blockchain gateway ID and the WMD ID, ensuring prompt and accurate data retrieval from the blockchain.

B. WMD authentication process

As previously mentioned, WMD consensus nodes will implement a network consensus mechanism such as PoS, when a new WMD node requests to join the network. Figure 2 illustrates the authentication process and the steps involved in integrating a new node into the network.

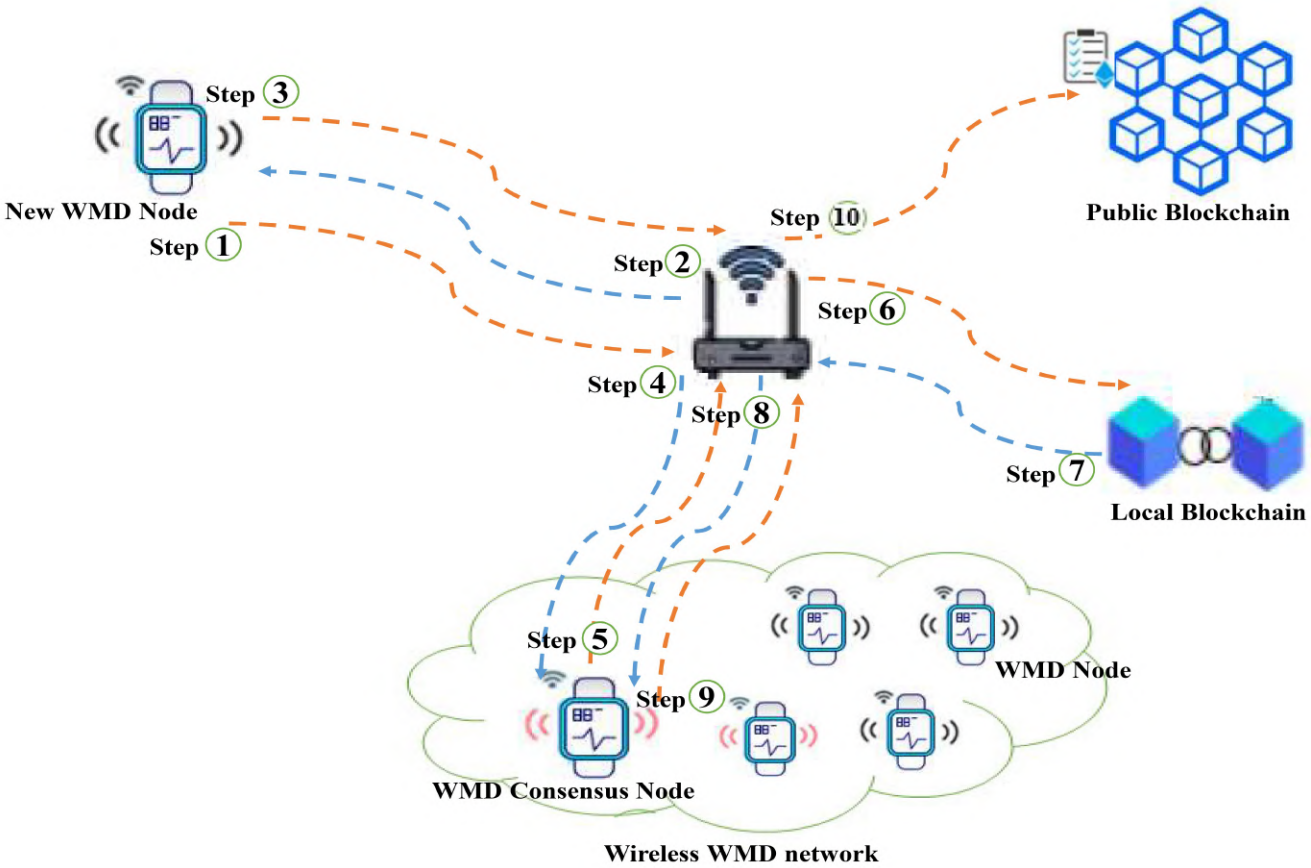

Fig 2: Node Addition Procedure in a Blockchain-Enabled WMD Network

Step 1 (Request Initiation): To join the WMD network, the new node WMD sends a request to the blockchain gateway to establish a communication channel.

Step 2 (Information Query): Once the communication channel is established, the blockchain gateway queries the new node for specific information, including its unique identifier (ID), MAC address, and other details.

Step 3 (Response Submission): The new node will respond to the blockchain gateway by providing the entire list of requested characteristics.

Step 4 (Data Forwarding): The blockchain gateway forwards the details of the new node to a WMD consensus node for validation through the consensus mechanism (such as PoS).

Step 5 (Data Verification Request): The WMD consensus node validator requests the blockchain gateway to verify whether the new node's data not exists in the local blockchain database.

Step 6 (Local Blockchain Query): Upon request from the WMD consensus node, the blockchain gateway queries the local (lightweight) blockchain to check if the new node's data is already present.

Step 7 (Data Retrieval): If the node data is found in the lightweight blockchain, it is sent to the blockchain gateway; otherwise, no data is returned.

Step 8 (Data Transmission): After retrieving the data, the blockchain gateway transmits it to the WMD consensus node.

Step 9 (Data Evaluation): The WMD consensus node evaluates the new node's data against existing records in the local blockchain to decide whether the new node should be allowed to join the WMD network.

Step 10 (Final Decision): At the end of the process, the result of the join request is sent by the blockchain gateway and recorded on the public blockchain.

We can conclude that the WMD authentication process ensures new nodes can securely join the WMD network through a series of validation steps using a consensus mechanism, such as PoS. This approach enhances the network's security and integrity, providing a robust and reliable environment for WMDs.

C. Performance evaluation methodology

Performance metrics

In our proposed solution, the system's performance is evaluated using key metrics to assess the efficiency and reliability of blockchain integration within wearable MIoT environments. The selected metrics include:

- **Average Latency**: This measures the time taken for a transaction to be confirmed after being sent. It is calculated as the difference between the transaction's start and end times. It reflects the system's responsiveness [40], [41].

$$\text{Latency} = (\text{end}_{\text{time}} - \text{start}_{\text{time}})$$

Where $\textbf{start}_{\textbf{time}}$ presents the time when the transaction is sent, and $\textbf{end}_{\textbf{time}}$ is the time when the transaction is confirmed.

- **Storage Throughput**: represents the volume of data stored per second during the simulation. It provides an indication of the system's capacity to manage large-scale data generated by wearable MIoT devices [40].

$$\text{Storage\_Throughput} = (\text{Total\_data\_stored} / \text{Sim\_duration})$$

Where **Total_data_stored** is total volume of stored data (in bytes), and **Sim_duration** is the total duration of the simulation (in seconds).

- **Packet Loss Rate (PLR)**: Represents the ratio of the number of packets that were not successfully received to the total number of packets sent. This metric shows the percentage of transactions lost during transmission. A high PLR could indicate network reliability issues or system overload [42].

$$\text{PLR} = (\text{total\_lost} / \text{total\_sent}) * 100$$

Where **total_lost** is the number of lost transactions, and **total_sent** is the total number of transactions sent during the simulation.

- **Success Rate**: This measures the percentage of successfully stored transactions compared to the total number of sent transactions in the blockchain network. It is calculated as the ratio of stored transactions to sent transactions, expressed as a percentage.

$$\text{Success\_Rate} = (\text{stored\_transactions} / \text{sent\_transactions}) * 100$$

Where **sent_transactions** represents the total number of transactions initiated by the blockchain nodes, and **stored_transactions** refers to the number of transactions successfully stored and validated within the blockchain.

By prioritizing the minimizing of latency and packet loss while maximizing storage throughput, our proposed solution aims to provide fast, secure, and efficient transaction processing. This approach is particularly suited for MIoT environments characterized by high data volumes and stringent real-time requirements.

Description of simulation algorithm

In the simulation of the proposed model, five main algorithms are integral to the proposed blockchain-IoT system. These algorithms include the select_validator function, propagation_loss function, lora_gateway function, wearable_medical_device function, and run_simulation function. Each algorithm plays a critical role in the operation and simulation of the model. The following sections provide an overview of these algorithms:

Algorithm 1 : the select_validator function

Input: Set of stakes for all nodes (stakes)
Output: Index of the selected validator.
// Step 1: Calculate the total stake across all nodes
1. total_stake = sum(stakes)
// Step 2: Pick a random value within the total stake
2. pick = random(0, total_stake)
// Step 3: Initialize the current cumulative stake
3. current = 0
// Step 4: Iterate over each node's stake
4. **for** each node's stake in stakes
// Step 4.1: Update cumulative stake
5. current = current + stake
// Step 4.2: Check if cumulative stake exceeds the random pick
6. **if** current exceeds pick
7. **return** the index of the selected validator

8. **end if**
9. **end for**

According to Algorithm 1, the select_validator function implements the Proof of Stake (PoS) consensus mechanism to select a validator node based on the stake held by each node. It first calculates the total stake across all nodes and then generates a random number within this range. The function iterates through the nodes, progressively accumulating their stakes, and selects the first node whose cumulative stake surpasses the generated random number. This ensures a probabilistic yet stake-weighted selection, promoting fairness and reducing energy consumption compared to traditional Proof of Work (PoW) mechanisms. The PoS mechanism is chosen for its efficiency, making it particularly suitable for resource-constrained Medical IoT environments.

Algorithm 2 : the propagation_loss function

Input: distance: Distance between two nodes.
Output: propagation loss (loss).
// Step 1: Calculate path loss using a path loss model
1. loss = 20 * LOG10(distance / 1000) + 20 * LOG10(LORA_FREQUENCY / 10^6) + 92.45
// Step 2: Return the calculated propagation loss
2. **return** loss

Algorithm 2 outlines the propagation_loss function, which computes the propagation loss of a LoRa signal using a specified path loss model. This function uses logarithmic calculations to estimate signal attenuation as a function of distance and operating frequency. By incorporating these parameters, it provides an accurate assessment of the signal strength degradation over distance, ensuring reliable communication analysis within the LoRa network.

Algorithm 3 :the lora_gateway function

Input: gateway_id: ID of the gateway processing the transaction. node_queue: Queue of incoming nodes waiting for processing. latencies: List of latencies for recorded transactions. transaction_count: Number of processed transactions. stored_count: Number of successfully stored transactions. data_volume: Total volume of data stored after transaction processing
Output: Updated latencies, transaction count, stored transaction count, and data volume after transaction processing.
1. **while** True
2. **if** node_queue is empty
3. **wait** for 1 time unit
4. **continue**
5. **end if**
6. **extract** node_id, start_time, frequency, bandwidth, spreading_factor, and payload **from** node_queue
7. Calculate distance (random value between 1 and 2000 meters)
8. Calculate propagation loss with propagation loss function
9. Calculate received_power = transmission_power – propagation_loss
10. **if** received power is adequate
11. Select a validator using select_validator function
12. Create the blockchain transaction
13. **Try** to send the transaction:
14. Calculate latency
15. Add latency to latencies list
16. Increment transaction_count
17. **if** validated transaction status
18. Increment stored_count
19. Add size of payload to data_volume
20. Reward the validator
21. **else**
22. Penalize the validator
23. **end if**
24. **exception**
25. Penalize the validator
26. **end try**
27. **else**
28. Print transmission lost message
29. **end if**
30 Wait for 1 time unit
31. **end while**

Algorithm 3 describes the lora_gateway function, which models the behavior of a LoRa gateway in the network. The function processes data by dequeuing it from a node queue, calculates propagation loss using a path loss model based on the distance, and simulates signal reception. Upon receiving a strong enough signal, it validates and stores transactions on the blockchain using a PoS mechanism. Conversely, if the signal strength is inadequate, it records transmission failures attributed to weak signal reception, ensuring a comprehensive simulation of gateway operations.

Algorithm 4: the wearable_medical_device function

Input: gateway_id: ID of the gateway processing the transaction. node_queue: Queue of incoming nodes waiting for processing. latencies: List of latencies for recorded transactions. transaction_count: Number of processed transactions. stored_count: Number of successfully stored transactions. data_volume: Total volume of data stored after transaction processing.
Output: Data packets sent to gateways and updated sent_count after each transmission.
1. **while** True
// Collect medical data
2. heart_rate = random(60,100)
3. body_temperature = random(36.0,37.5)
4. oxygen_level = random(95,100)
// Create payload from collected data
5. data = (heart_rate, body_temperature, oxygen_level)
//Set transmission parameters
7. start_time = current_time
8. frequency = 868e6 // 868 MHz
9. bandwidth = 125e3 // 125 kHz
10. spreading_factor = 7
11. gateway_id = node_id % 5
//Append the data packet to the selected gateway
12. append(node_id, start_time, frequency, bandwidth, spreading_factor, payload) to gateways[gateway_id]
//Increment the count of sent data packets for the node
13. sent_count[node_id] += 1
//wait for interval time units before the next transmission
14. Wait(interval)
15. **end while**

Algorithm 4 defines the wearable_medical_device function, which emulates the operation of the wearable

medical device by periodically generating medical data such as heart rate, body temperature, and oxygen levels. This data is encoded into a payload and transmitted to a LoRa gateway, replicating real-time health monitoring scenarios.

Algorithm 5: the run_simulation function

Input: num_nodes: The number of IoT nodes in the simulation.
Output: Average latency, total sent packets, total stored packets, packet loss ratio, and storage throughput.
// Step 1: Start the processes for each gateway
8. **for** each gateway_id in range(5)
9. execute lora_gateway function
10. **end for**
// Step 3: Start node processes
11. **for** each node_id in range(num_nodes)
12. execute wearable_medical_device function
13. **end for**
// Step 4: Run the simulation (in 1 hour)
14. run(3600)
// Step 5: Calculate and return metrics
15. avg_latency = mean(latencies)
16. total_sent = sum(sent_count)
17. total_stored = sum(stored_count)
18. plr = (total_sent - total_stored) / total_sent if total_sent > 0 else 0
19. total_data_stored = sum(data_volume)
20. storage_throughput = total_data_stored / 3600
// Step 6: Return the calculated metrics
21. **return** avg_latency, total_sent, total_stored, plr, storage_throughput

As per algorithm 5, the run_simulation function coordinates the simulation of IoT nodes and LoRa gateways over a defined period. It initializes the necessary data structures and processes each node and gateway using SimPy. The function tracks and aggregates performance metrics such as latency, storage throughput, PLR and success rate. Upon completion, it computes and displays the simulation results, offering insights into system performance.

These algorithms contribute to creating a robust and reliable blockchain-IoT system designed to secure data storage and facilitate real-time monitoring in healthcare IoT systems.

V. Simulation Scenarios, Results and Discussion

In this section, we illustrate the performance of the proposed model in comparison with existing approaches. This section is structured into two sub-sections: simulation environment and comparative analysis.

A. Simulation Environment

To assess the performance of the proposed architecture, we designed two distinct scenarios that focus on key performance metrics, including latency, storage throughput, packet loss rate (PLR), and success rate. The specific parameters used for evaluating the architecture's performance across these scenarios are detailed in Table 1.

The simulation leverages the power of Python, a versatile and widely-used programming language known for its readability and extensive libraries, to model an IoT medical data storage system based on blockchain technology. SimPy simulator, a discrete event simulation library in Python, is used to manage and coordinate the actions over time of entities such as wearable medical devices and LoRa gateways. Web3.py facilitates interaction with the Ethereum blockchain by connecting to a local Ganache node and sending simulated transactions, integrating blockchain elements into the simulation. NumPy is used to generate random data necessary for the simulation, perform complex mathematical calculations, and analyze statistics, providing efficient manipulation of data arrays. Matplotlib is employed to create graphical visualizations of the simulation results, such as average latencies, and other performance metrics, making it easier to interpret the simulation outcomes. The simulation is conducted in the JupyterLab environment, an interactive and flexible interface for Python development. All experiments were executed on a computing system with an Intel Core i7-8700T CPU @ 2.40 GHz and 8 GB of DDR4 RAM running on the Windows 10 operating system, simulating the two scenarios specified in Table 1.

Our proposed model has been compared with other existing traditional approaches, such as [39], [43] and [44]. The simulation focuses on evaluating the amount of data stored in the blockchain. For this purpose, the parameters used are characterized by the following specifics: each data packet measures 50 bytes (the typical size of an IoT data packet), the network consists of 4 to 512 nodes, with each node transmitting a data packet every 120 seconds. Over a one-hour period, this results in a total data volume of 750 KB when 512 IoT devices each send 50-byte packets every 120 seconds. Each IoT data packet is integrated into the blockchain through a separate transaction.

TABLE I
The simulation configuration for the proposed model

Parameter	Scenario 1	Scenario 2
Simulator	Simpy	Simpy
Simulation Time	60 min	60 min
Blockchain platform	Ganache(Ethereum)	Ganache(Ethereum)
Transmission range diameter	2 km	2 km
Number of Lora gateway	5	5
Number of WMD Nodes	4, 8 , 16 , 32	64, 128, 256, 512
IoT data sending time	120 second	120 second
Block size	1 MB	1 MB
Payload size	50 bytes	50 bytes

B. Comparative Analysis

In this sub-section, the details of the simulation results are discussed in detail. The proposed approch is compared with the previous works, [39], [42] and [43]. The main sets of parameters that are taken into account for comparison are latency, storage throughput, PLR, and success rate.

Average latency

Our architecture primarily focuses on measuring the average latency for each data packet accepted into the blockchain, encompassing both validation and inclusion in a block, as well as transaction storage throughput. As clearly illustrated in Figure 3 and Figure 4, we carefully analyze the average latency of data packet acceptance. Each step, from initial validation to final block inclusion, impacts this metric. The increased duration of the validation process results from the sequential handling of data packets sent by WMD nodes before they are securely integrated into the blockchain. This approach ensures a precise and detailed evaluation of performance, which is crucial for managing data flow effectively and maintaining high standards of reliability and operational efficiency. We can examine the average latency associated with each performance test is depicted in Figure 3 and Figure 4.

After evaluating the performance, we observed the following latency results. In Figure 3, for 4 WMD blockchain nodes, the average latency was measured at 54 ms. This latency increased to 327 ms when 32 WMD blockchain nodes were involved. In Figure 4, the average latency was found to be 0.65 seconds with 64 WMD blockchain nodes and rose to 4.79 seconds with 512 WMD blockchain nodes. These results highlight a significant increase in latency as the number of WMD nodes in the blockchain increases, illustrating the direct impact of workload on system performance. According to the results presented in Figures 3 and 4, as well as in the existing traditional approaches [42] , [39] and [43], which also utilize blockchain technology, the proposed model demonstrates a better average latency. This is achieved through optimized transaction handling and efficient block inclusion processes, ensuring scalability and reliability in large-scale IoT networks. While traditional approaches exhibit higher latency under similar conditions, our model maintains a balance between security, performance, and scalability, making it particularly suitable for critical applications such as healthcare IoT environments

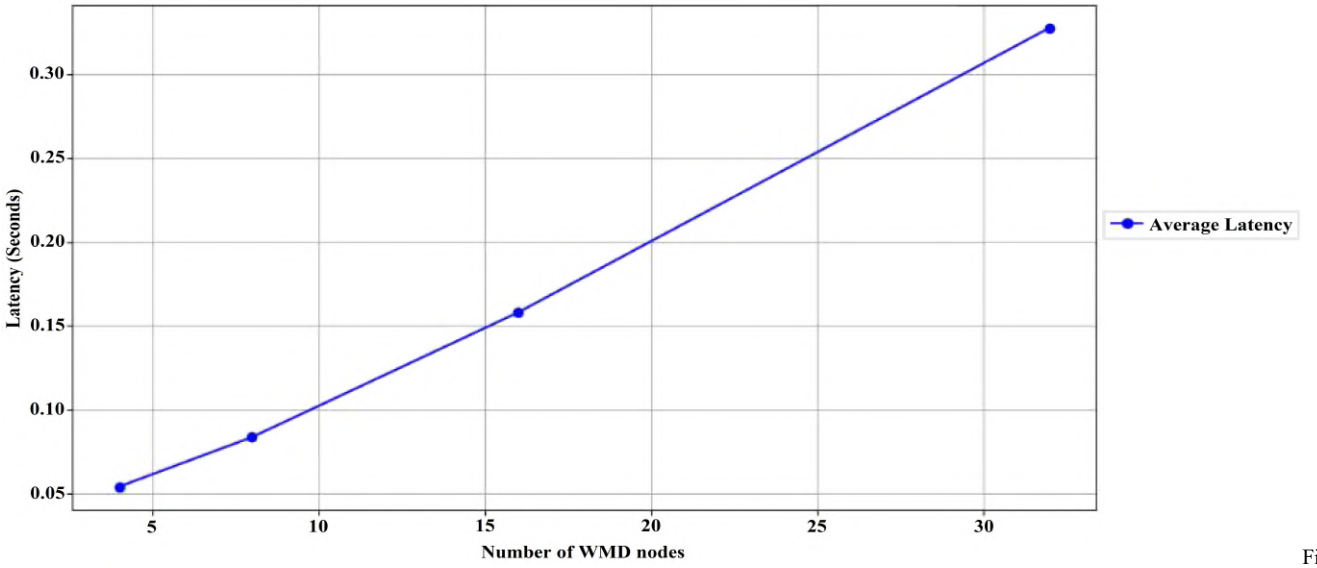

Fig 3: Average latency metric for scenario1

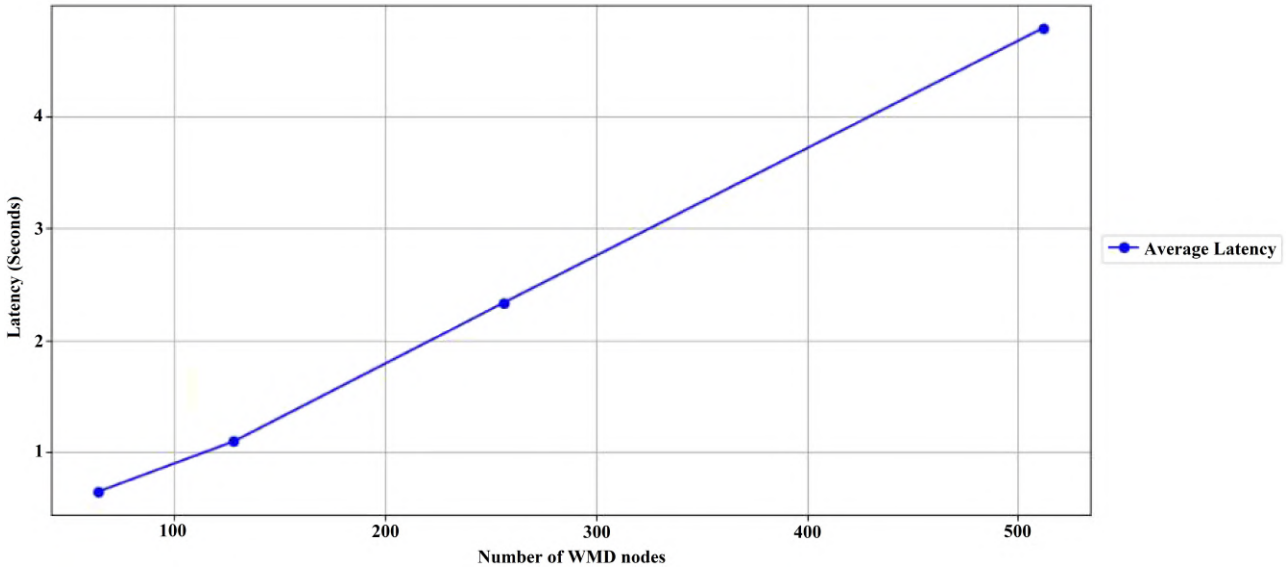

Fig 4: Average latency metric for scenario2

Storage Throughput

Our proposed architecture also evaluates storage throughput by analyzing the capacity of the blockchain to handle data storage efficiently as the number of blockchain nodes increases. This metric measures the rate at which transactions are stored in the blockchain over time, reflecting the system's ability to process and record data under varying workloads.

Figures 5 and 6 illustrate the transaction storage throughput, which measures data storage capacity within the blockchain architecture for both scenarios. In Figure 5, the initial storage throughput is recorded at 0.83 bytes/second. This throughput increases to 6.67 bytes/second with 32 WMD blockchain nodes. Figure 6 further demonstrates that the storage throughput reaches 13.33 bytes/second with 64 WMD blockchain nodes and expands to 106.71 bytes/second with 512 WMD blockchain nodes. These findings highlight the scalability challenges and performance variations associated with increasing node counts, providing crucial insights into the system's transaction processing capabilities under different loads. Compared to the traditional approaches cited previously [39], [42] and [43], which also rely on blockchain technology, the proposed model demonstrates superior scalability and storage efficiency. Traditional approaches exhibit a lower storage throughput due to less optimized transaction inclusion mechanisms, particularly as the number of nodes increases. By contrast, our model ensures consistent improvements in throughput as the network grows, emphasizing its ability to manage high transaction volumes effectively in large-scale IoT networks while maintaining robust performance.

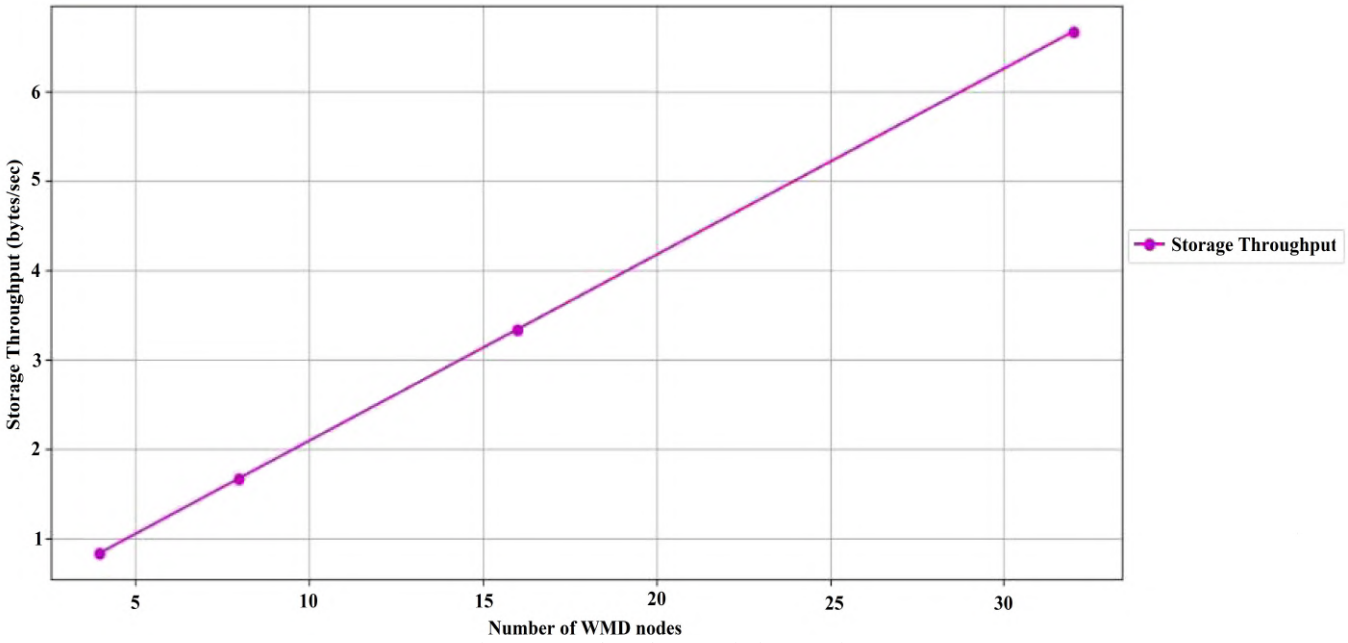

Fig 5: Storage throughput metric for scenario1

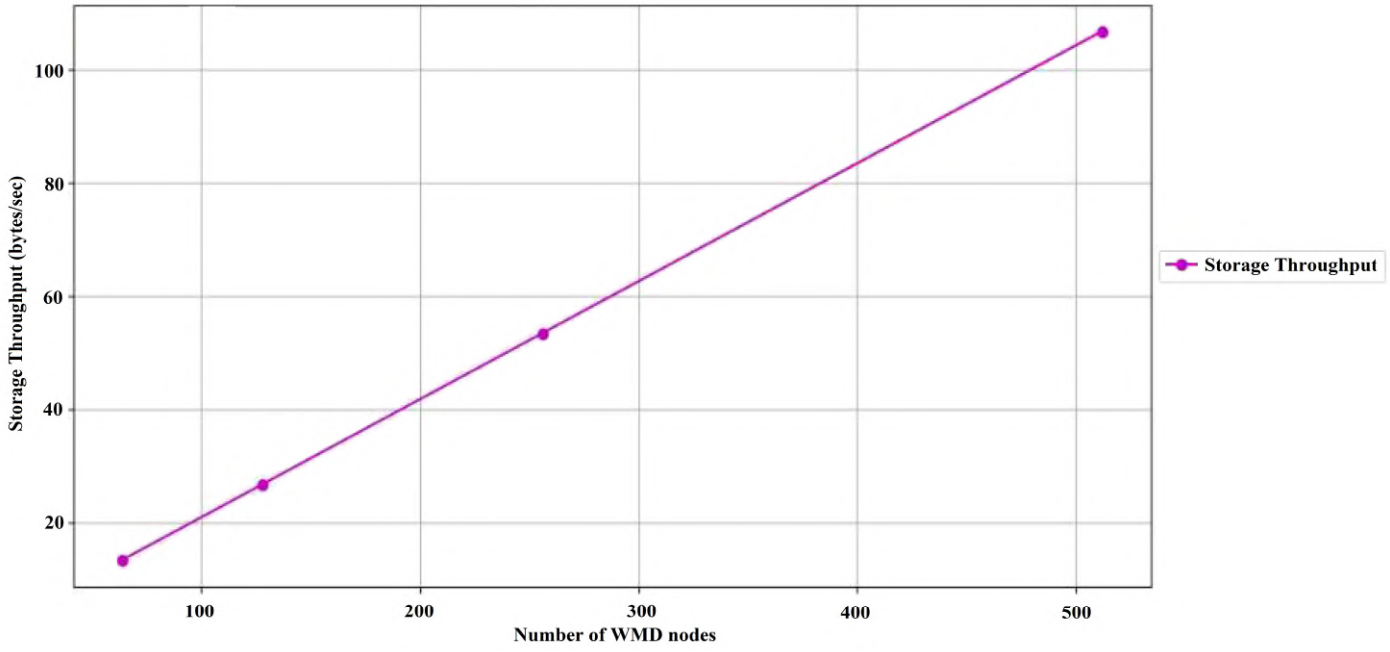

Fig 6: Storage throughput metric for scenario2

Packet Loss Rate

The Packet Loss Rate evaluates the percentage of transactions or data packets sent by WMD nodes that fail to reach their intended destination in the blockchain network. This metric is crucial for assessing the reliability of data transmission and identifying potential issues such as congestion or malicious node interference. In our simulation results over the tow scenarios, illustrated in Figure 7 and Figure 8, the proposed architecture achieves a 0% Packet Loss Rate, even as the number of WMD nodes increases significantly from 4 to 512 nodes. This result underscores the efficiency and reliability of the proposed blockchain model, which ensures that every transaction is successfully delivered and securely stored. Compared to traditional methods [39], [42] and [43], which exhibit packet loss rates ranging from 20% to 30%, the proposed architecture demonstrates superior performance, ensuring data integrity and consistency.

Success Rate

The Success Rate measures the proportion of transactions successfully stored in the blockchain relative to the total number of transactions initiated by WMD nodes. This metric reflects the system's ability to handle data transmission efficiently, even under challenging conditions such as node failures, network congestion, or malicious activities.

In our scenarios, transactions refer to the data packets sent by the blockchain WMD nodes. During our simulation, as shown in Figures 9 and 10, we conducted approximately 120 transactions with 4 blockchain WMD nodes, and 768,000 transactions with 512 blockchain WMD nodes. The proposed model achieves a 100% success rate across various scenarios, demonstrating its ability to securely store all sent transactions without loss or modification. This achievement highlights the robustness and reliability of the blockchain architecture in managing data flow effectively, even in large-scale deployments. In comparison, traditional approaches such as [39], [42], and [43] exhibit lower success rates, ranging between 70% and 80%, further validating the efficiency of the proposed approach in ensuring seamless data storage.

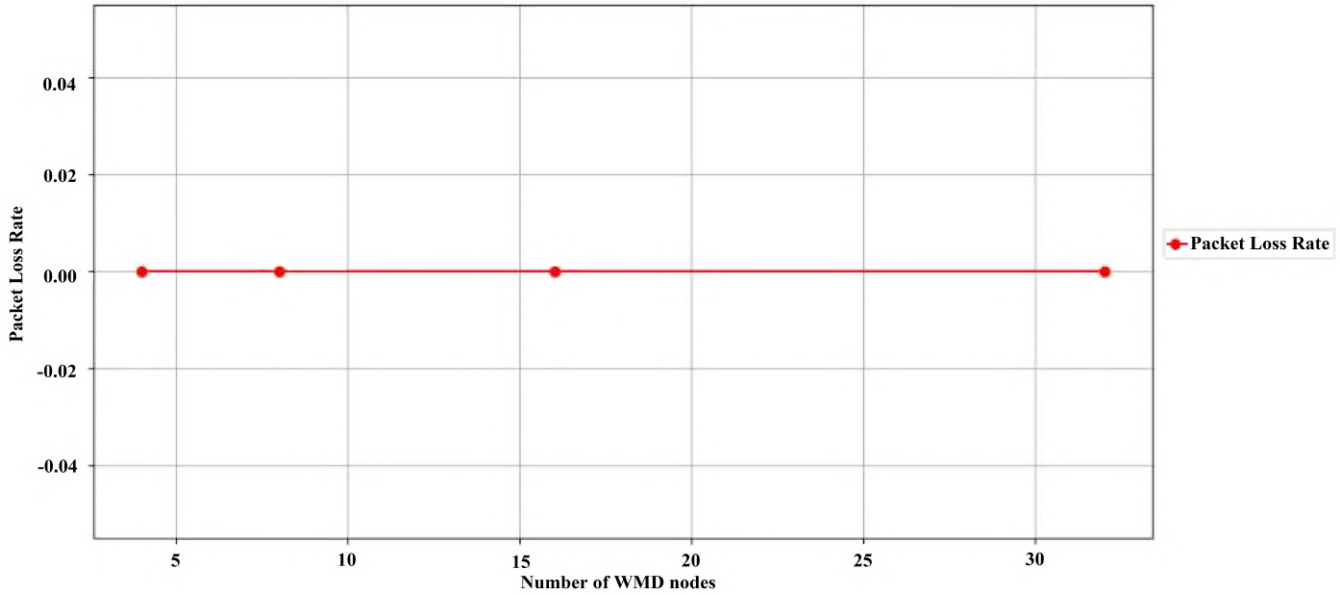

Fig 7: Packet loss rate metric for scenario1

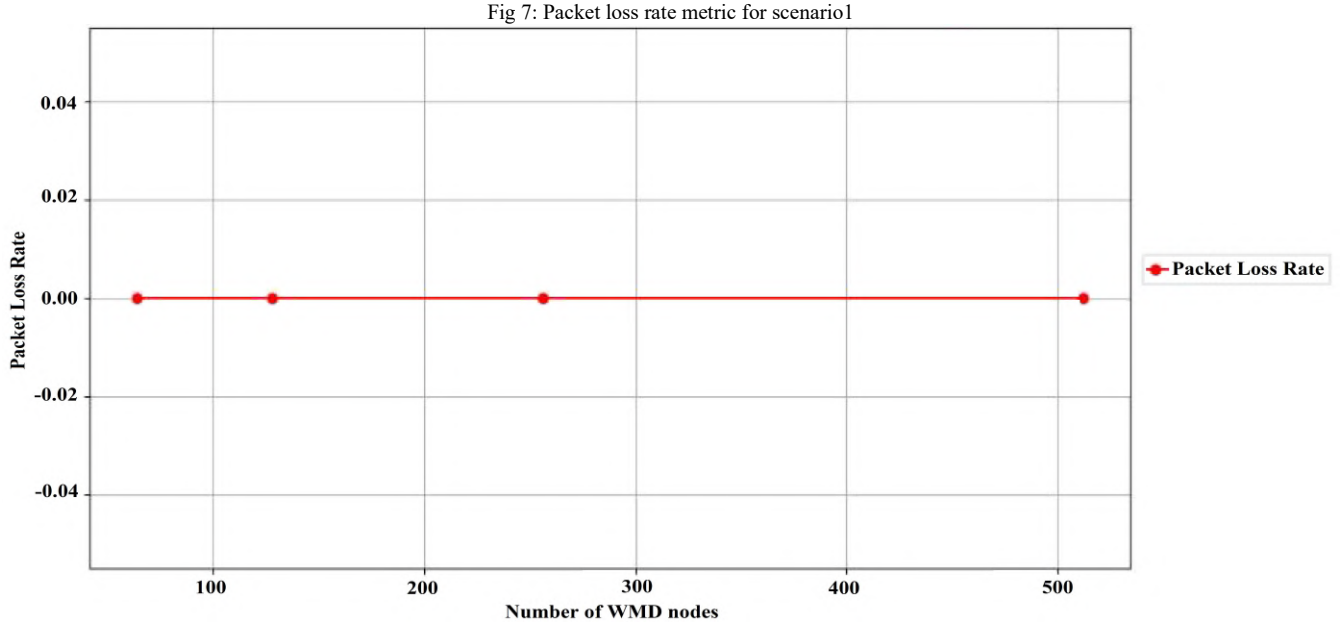

Fig 8: Packet loss rate metric for scenario2

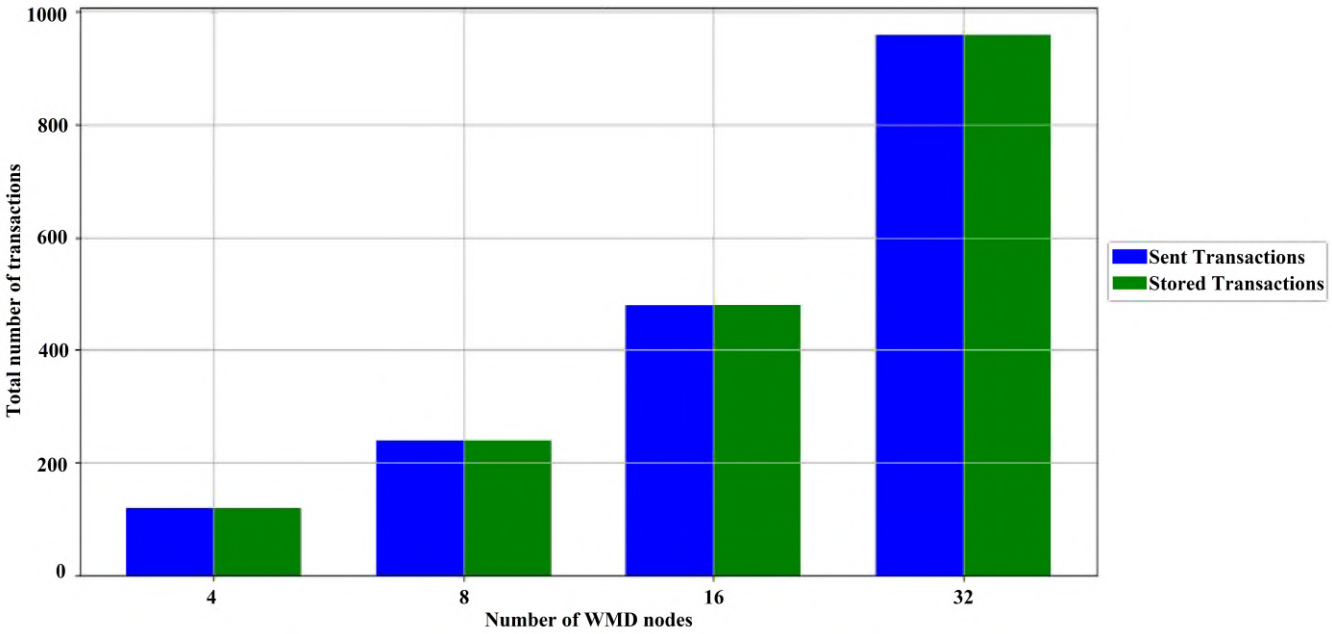

Fig 9: Send and stored transactions per WMD for scenario1

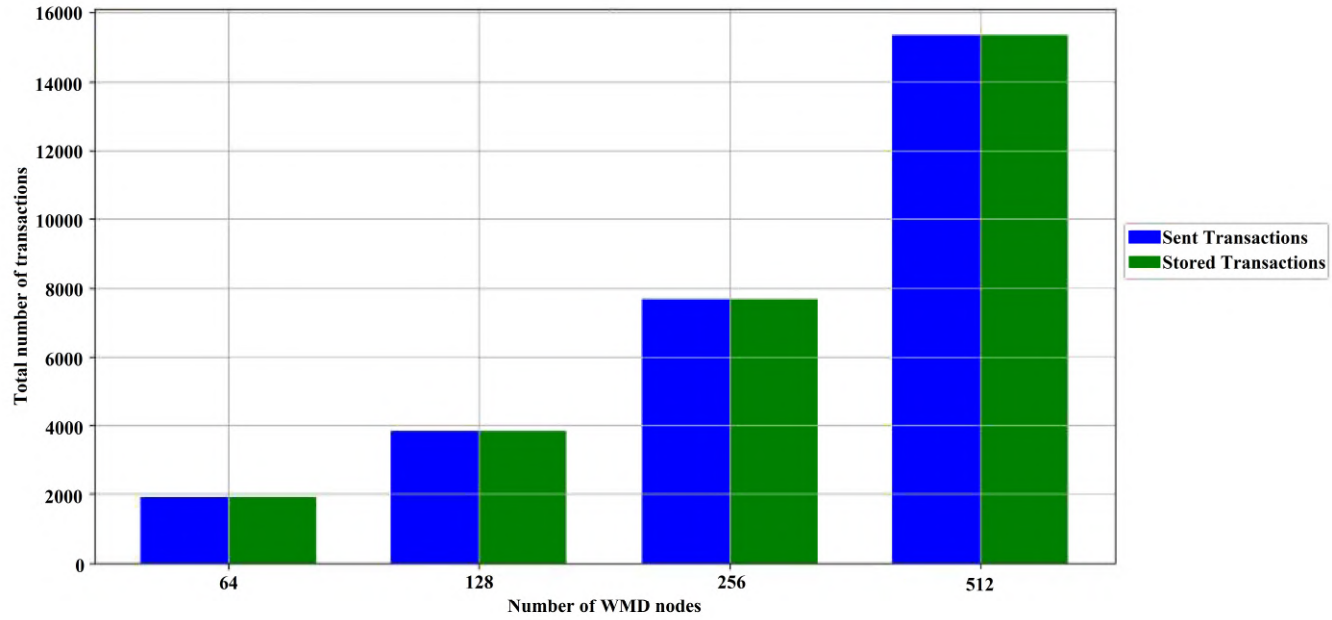

Fig 10: Send and stored transactions per WMD for scenario2

In addition, our study of the blockchain model through a series of simulations and evaluations has revealed several critical performance aspects in healthcare IoT environments. By analyzing metrics such as data storage capacity, average latency, transaction storage throughput, packet loss rate, and success rate, we provided a comprehensive assessment of the system's reliability and operational efficiency.

The findings confirm the system's robust data storage capabilities, as evidenced by the storage throughput, which increased from 0.83 bytes/second with 4 nodes to 106.71 bytes/second with 512 nodes, highlighting scalability under high workloads. In contrast, the approaches in [39], [42], and [43] exhibit lower storage throughput growth due to inefficient consensus mechanisms, limiting their ability to scale effectively.

Notably, the packet loss rate remained consistent at 0% across all scenarios, even when the number of transactions scaled significantly from 120 to 768,000. This result underscores the system's reliability in ensuring complete transaction delivery and storage. By contrast, the models in [39], [42] and [43] exhibit packet loss rates between 20% and 30% due to network congestion and inefficient routing, making our approach significantly more reliable for critical healthcare applications.

Additionally, the success rate was observed at 100%, affirming the model's ability to securely store all transmitted transactions, even under extensive scalability tests. Traditional approaches struggle to maintain such reliability, as noted in [39], [42] and [43], where success rates vary between 70% and 80% due to failures in transaction finalization and consensus inefficiencies.

These results demonstrate the model's effectiveness in integrating IoT data packets with the blockchain while revealing opportunities for optimization to address challenges such as increasing latency with node expansion. The system’s high reliability, combined with its scalability potential, makes it a promising solution for healthcare IoT

applications, where data integrity, security, and operational resilience are paramount.

VI. Conclusion and Future Directions

In conclusion, our research introduces a novel model that leverages blockchain technology to manage and securely store the vast amounts of data generated by wearable MIoT devices. By utilizing blockchain's inherent features such as immutability, decentralization and consensus mechanisms, our model distributes data storage across a network, eliminating the need for centralized storage entities. This architecture addresses the resource limitations of wearable MIoT devices while ensuring robust system functionality, guarantees both security and efficiency in data management and communication. Moreover, our model is adaptable to various wireless communication protocols, allowing for scalability without the need for retrofitting.

The analysis demonstrates that the proposed approach significantly outperforms traditional methods. Specifically, it shows improved average latency, storage throughput, and PLR. This performance enhancement underscores the effectiveness of blockchain technology in the medical IoT domain.

As future work, we aim to conduct extensive real-world testing of the proposed model to assess its scalability and efficiency under practical operating conditions. Our objective is to employ application-specific techniques leveraging blockchain technology for enhanced and more rigorous testing. Several potential avenues for these techniques include:

Load Testing: We will subject the system to heavy loads to evaluate its performance under stress conditions. This will involve simulating high volumes of data transactions and assessing how the architecture handles increased demand.

Security Analysis: Conducting thorough security assessments to identify and address potential vulnerabilities and attack vectors. We will explore techniques such as penetration testing and vulnerability scanning to fortify the system against malicious threats.

Fault Tolerance Evaluation: Assessing the system's ability to maintain functionality in the presence of faults or failures. This will involve simulating various failure scenarios and evaluating how the architecture responds and recovers from such events.

Scalability Testing: Examining how the system scales as the number of IoT devices and data transactions increases. We will analyze performance metrics such as latency and throughput to understand the system's scalability limits and identify potential bottlenecks.

Integration with IoT Ecosystems: Exploring seamless integration with existing IoT ecosystems and protocols. This will involve interoperability testing to ensure compatibility and smooth operation within diverse IoT environments.

By pursuing these avenues of research, we aim to validate and refine the proposed architecture, paving the way for its practical deployment in real-world healthcare settings. Additionally, we will explore novel approaches and optimizations to further enhance the scalability, efficiency, and security of blockchain-based data storage for wearable MIoT devices.

References

[1] L. Liu and Z. Li, "Permissioned Blockchain and Deep Reinforcement Learning Enabled Security and Energy Efficient Healthcare Internet of Things," IEEE Access, vol. 10, pp. 53640–53651, 2022, doi: 10.1109/ACCESS.2022.3176444.

[2] N. Tariq, A. Qamar, M. Asim, and F. A. Khan, "Blockchain and Smart Healthcare Security: A Survey," Procedia Computer Science, vol. 175, pp. 615–620, 2020, doi: 10.1016/j.procs.2020.07.089.

[3] M. A. Mohammed, M. Boujelben, and M. Abid, "A Novel Approach for Fraud Detection in Blockchain-Based Healthcare Networks Using Machine Learning," Future Internet, vol. 15, no. 8, p. 250, 2023, doi: 10.3390/fi15080250.

[4] X. Xiang, M. Wang, and W. Fan, "A Permissioned Blockchain-Based Identity Management and User Authentication Scheme for E-Health Systems," IEEE Access, vol. 8, pp. 171771–171783, 2020, doi: 10.1109/ACCESS.2020.3022429.

[5] A. A. Yaseen, K. Patel, A. A. Yassin, A. J. Aldarwish, and H. A. Hussein, "Secure Electronic Healthcare Record Using Robust Authentication Scheme," IAENG International Journal of Computer Science, vol. 50, no. 2, pp. 468-476, 2023.

[6] A. Kumar et al., "A Novel Decentralized Blockchain Architecture for the Preservation of Privacy and Data Security against Cyberattacks in Healthcare," Sensors, vol. 22, no. 15, p. 5921, 2022, doi: 10.3390/s22155921.

[7] M. Zarour et al., "Ensuring data integrity of healthcare information in the era of digital health," Healthcare Tech Letters, vol. 8, no. 3, pp. 66–77, 2021, doi: 10.1049/htl2.12008.

[8] T. Hovorushchenko, A. Moskalenko, and V. Osyadlyi, "Methods of medical data management based on blockchain technologies," J Reliable Intell Environ, vol. 9, no. 1, Art. no. 1, 2023, doi: 10.1007/s40860-022-00178-1.

[9] M. Kumar, H. Raj, N. Chaurasia, and S. S. Gill, "Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0," Internet of Things and Cyber-Physical Systems, vol. 3, pp. 309–322, 2023, doi: 10.1016/j.iotcps.2023.05.006.

[10] A. J, D. P. Isravel, K. M. Sagayam, B. Bhushan, Y. Sei, and J. Eunice, "Blockchain for healthcare systems: Architecture, security challenges, trends and future directions," Journal of Network and Computer Applications, vol. 215, p. 103633, 2023, doi: 10.1016/j.jnca.2023.103633.

[11] Z. Wenhua, F. Qamar, T.-A. N. Abdali, R. Hassan, S. T. A. Jafri, and Q. N. Nguyen, "Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends," Electronics, vol. 12, no. 3, Art. no. 3, 2023, doi: 10.3390/electronics12030546.

[12] T. Emad Ali, F. Imad Ali, M. A. Abdala, A. H. Morad, G. Gódor, and D. Z. Alwahab, "Blockchain-Based Deep Reinforcement Learning System for Optimizing Healthcare," Infocommunications journal, vol. 16, no. 3, Art. no. 3, 2024, doi: 10.36244/ICJ.2024.3.9.

[13] S. Fugkeaw, L. Wirz, and L. Hak, "Secure and Lightweight Blockchain-Enabled Access Control for Fog-Assisted IoT Cloud Based Electronic Medical Records Sharing," IEEE Access, vol. 11, pp. 62998–63012, 2023, doi: 10.1109/ACCESS.2023.3288332.

[14] R. G. Sonkamble, A. M. Bongale, S. Phansalkar, A. Sharma, and S. Rajput, "Secure Data Transmission of Electronic Health Records Using Blockchain Technology," Electronics, vol. 12, no. 4, Art. no. 4, 2023, doi: 10.3390/electronics12041015.

[15] A. Musamih et al., "A Blockchain-Based Approach for Drug Traceability in Healthcare Supply Chain," IEEE Access, vol. 9, pp. 9728–9743, 2021, doi: 10.1109/ACCESS.2021.3049920.

[16] J. S. Jadhav and J. Deshmukh, "A review study of the blockchain-based healthcare supply chain," Social Sciences & Humanities Open, vol. 6, no. 1, Art. no. 1, 2022, doi: 10.1016/j.ssaho.2022.100328.

[17] A. Rizzardi, S. Sicari, J. F. Cevallos M., and A. Coen-Porisini, "IoT-driven blockchain to manage the healthcare supply chain and protect medical records," Future Generation Computer Systems, vol. 161, pp. 415–431, 2024, doi: 10.1016/j.future.2024.07.039.

[18] S. K. Jena, B. Kumar, B. Mohanty, A. Singhal, and R. C. Barik, "An advanced blockchain-based hyperledger fabric solution for tracing fraudulent claims in the healthcare industry," Decision Analytics Journal, vol. 10, p. 100411, 2024, doi: 10.1016/j.dajour.2024.100411.

[19] S. Jeong, J.-H. Shen, and B. Ahn, "A Study on Smart Healthcare Monitoring Using IoT Based on Blockchain," Wireless Communications and Mobile Computing, vol. 2021, no. 1, p. 9932091, 2021, doi: 10.1155/2021/9932091.

[20] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," International Journal of Intelligent Networks, vol. 2, pp. 130–139, 2021, doi: 10.1016/j.ijin.2021.09.005.

[21] F. Li, X. Yu, R. Ge, Y. Wang, Y. Cui, and H. Zhou, "BCSE: Blockchain-based trusted service evaluation model over big data," Big Data Min. Anal., vol. 5, no. 1, pp. 1–14, 2022, doi: 10.26599/BDMA.2020.9020028.

[22] A. B. Haque, A. Muniat, P. R. Ullah, and S. Mushsharat, "An Automated Approach towards Smart Healthcare with Blockchain and Smart Contracts," in 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India: IEEE, pp. 250–255, 2021. doi: 10.1109/ICCCIS51004.2021.9397158.

[23] C. Pujari et al, "A Novel Method of Secure Child Adoption Using Blockchain Technology," IAENG International Journal of Applied Mathematics, vol. 53, no. 4, pp. 1531-1539, 2023.

[24] Y. Qu et al., "Towards Privacy-Aware and Trustworthy Data Sharing Using Blockchain for Edge Intelligence," Big Data Min. Anal., vol. 6, no. 4, pp. 443–464, 2023, doi: 10.26599/BDMA.2023.9020012.

[25] T.-T. Kuo et al., "Blockchain-enabled immutable, distributed, and highly available clinical research activity logging system for federated COVID-19 data analysis from multiple institutions," Journal of the American Medical Informatics Association, vol. 30, no. 6, pp. 1167–1178, 2023, doi: 10.1093/jamia/ocad049.

[26] C. Antal, T. Cioara, I. Anghel, M. Antal, and I. Salomie, "Distributed Ledger Technology Review and Decentralized Applications Development Guidelines," Future Internet, vol. 13, no. 3, pp. 62, 2021, doi: 10.3390/fi13030062.

[27] K. Zhang et al., "Towards Privacy in Decentralized IoT: A Blockchain-Based Dual Response DP Mechanism," Big Data Min. Anal., vol. 7, no. 3, pp. 699–717, 2024, doi: 10.26599/BDMA.2024.9020023.

[28] A. Rghioui, S. Bouchkaren, and A. Khannous, "Blockchain-based Electronic Healthcare Information System Optimized for Developing Countries," IAENG International Journal of Computer Science, vol. 49, no. 3, pp. 833-847, 2022.

[29] S. Naz and S. U.-J. Lee, "Why the new consensus mechanism is needed in blockchain technology?," in 2020 Second International Conference on Blockchain Computing and Applications (BCCA), Antalya, Turkey: IEEE, pp. 92–99, 2020. doi: 10.1109/BCCA50787.2020.9274461.

[30] K. K. Ishak, N. A. M. Razali, N. A. Malizan, and G. Sulong, "Smart Cities' Cybersecurity and IoT: Challenges and Future Research Directions," IAENG International Journal of Computer Science, vol. 51, no. 7, pp. 725-737, 2024.

[31] A. Lakhan, O. Thinnukool, T. M. Groenli, and P. Khuwuthyakorn, "RBEF: Ransomware Efficient Public Blockchain Framework for Digital Healthcare Application," Sensors, vol. 23, no. 11, pp. 5256, 2023, doi: 10.3390/s23115256.

[32] F. M. Talaat and R. M. El-Balka, "Stress monitoring using wearable sensors: IoT techniques in medical field," Neural Comput & Applic, vol. 35, no. 25, pp. 18571–18584, 2023, doi: 10.1007/s00521-023-08681-z.

[33] Y. SABRI. "A Routing Protocol for The Wireless Body Area Sensor Network (WBASN)," IAENG International Journal of Computer Science, vol. 49, no. 2, pp. 279-285, 2022.

[34] J. Mabrouki, M. Azrour, D. Dhiba, Y. Farhaoui, and S. E. Hajjaji, "IoT-based data logger for weather monitoring using arduino-based wireless sensor networks with remote graphical application and alerts," Big Data Min. Anal., vol. 4, no. 1, pp. 25–32, 2021, doi: 10.26599/BDMA.2020.9020018.

[35] Y. Hu et al., "Design and Development of a BaaS System Based on Intelligent Scheduling and Operation Cloud-Edge Platform," IAENG International Journal of Computer Science, vol. 51, no. 3, pp. 222-231, 2024.

[36] B. Lashkari and P. Musilek, "A Comprehensive Review of Blockchain Consensus Mechanisms," IEEE Access, vol. 9, pp. 43620–43652, 2021, doi: 10.1109/ACCESS.2021.3065880.

[37] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, "Blockchain smart contracts: Applications, challenges, and future trends," Peer-to-Peer Netw. Appl., vol. 14, no. 5, pp. 2901–2925, 2021, doi: 10.1007/s12083-021-01127-0.

[38] P. Dullabh, L. Hovey, K. Heaney-Huls, N. Rajendran, A. Wright, and D. F. Sittig, "Application Programming Interfaces in Health Care: Findings from a Current-State Sociotechnical Assessment," Appl Clin Inform, vol. 11, no. 01, pp. 059–069, 2020, doi: 10.1055/s-0039-1701001.

[39] Z. Jingjing, S. Tao, et S. Yuxia. "Apihelper: Helping junior android programmers learn api usage," IAENG International Journal of Computer Science, vol. 47, no 1, pp. 92-97, 2020.

[40] X. Qi, Z. Zhang, C. Jin, and A. Zhou, "A Reliable Storage Partition for Permissioned Blockchain," IEEE Trans. Knowl. Data Eng., vol. 33, no. 1, pp. 14–27, 2021, doi: 10.1109/TKDE.2020.3012668.

[41] H. Huang, W. Miao, G. Min, J. Tian, and A. Alamri, "NFV and Blockchain Enabled 5G for Ultra-Reliable and Low-Latency Communications in Industry: Architecture and Performance Evaluation," IEEE Trans. Ind. Inf., vol. 17, no. 8, pp. 5595–5604, 2021, doi: 10.1109/TII.2020.3036867.

[42] I. H. Abdulqadder, S. Zhou, D. Zou, I. T. Aziz, and S. M. A. Akber, "Bloc-Sec: Blockchain-Based Lightweight Security Architecture for 5G/B5G Enabled SDN/NFV Cloud of IoT," in 2020 IEEE 20th International Conference on Communication Technology (ICCT), Nanning, China: IEEE, pp. 499–507, 2020. doi: 10.1109/ICCT50939.2020.9295823.

[43] A. Sharma, Sarishma, R. Tomar, N. Chilamkurti, and B.-G. Kim, "Blockchain Based Smart Contracts for Internet of Medical Things in e-Healthcare," Electronics, vol. 9, no. 10, p. 1609, 2020, doi: 10.3390/electronics9101609.

[44] M. El Khatib, H. M. Alzoubi, S. Hamidi, M. Alshurideh, A. Baydoun, and A. Al-Nakeeb, "Impact of Using the Internet of Medical Things on e-Healthcare Performance: Blockchain Assist in Improving Smart Contract," CEOR, vol. 15, pp. 397–411, 2023, doi: 10.2147/CEOR.S407778.

[45] M.Shraddha and S. Onkar, S., 2022. Blockchain technology in healthcare market research. URL: https://www.alliedmarketresearch.com/blockchain-technology-in-the-healthcare-market-A10259.

[46] Z. Elhadari, H. Zougagh, N. Idboufker, et al, "Survey on the Adoption of Blockchain Technology in Internet of Things Environments: Techniques, Challenges and Future Research Directions," IAENG International Journal of Computer Science, vol. 52, no 1, pp. 59-89, 2025.