Journal of Theoretical and Applied Information Technology
31st July 2024. Vol.102. No. 14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IMPROVING SECURE ROUTING IN IOMT: ENHANCED BLOCKCHAIN CYBERSECURITY SCHEME USING HYPERLEDGER FABRIC

TAYSEER ALKHDOUR[1], MOHAMMED AMIN ALMAIAH[2], AITIZAZ ALI[3], ROMEL AL-ALI[4], TING TIN TIN[5], THEYAZAN ALDAHYANI[6]

[1] College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia
[2] King Abdullah the II IT School, The University of Jordan, Amman 11942, Jordan
[3] School of technology, Asia Pacific University, Kuala lumper, Malaysia
[4] Associate Professor, the National Research Center for Giftedness and Creativity, King Faisal University, Saudi Arabia.
[5] Faculty of Data Science and Information Technology, INTI International University, Malaysia
[6] Applied College in Abqaiq, King Faisal University, Al-Ahsa 31982, Saudi Arabia
* Correspondence: m.almaiah@ju.edu.jo and talkhdour@kfu.edu.sa

ABSTRACT

The Internet of Medical Things (IOMT) has emerged as a transformative technology in the healthcare sector, enabling seamless monitoring and management of patients' vital health data. However, the integration of IOMT into healthcare ecosystems raises critical concerns about data security, especially during data transmission and routing. In this context, we present a novel approach for secure routing in IOMT by combining the power of homomorphic encryption and permissioned blockchain technology using Hyperledger Fabric. Our proposed framework addresses the pressing need for confidentiality, integrity, and authenticity of medical data as it traverses through interconnected IoT devices and networks. To achieve this, we leverage homomorphic encryption to perform computations on encrypted data without decrypting it, preserving patient privacy while enabling data analysis. Furthermore, we introduce a permissioned blockchain network built on Hyperledger Fabric to establish a trust infrastructure among healthcare entities, ensuring that only authorized nodes can participate in the routing process. Through the integration of homomorphic encryption and Hyperledger Fabric, our approach guarantees end-to-end security during data routing in IOMT. We discuss the architecture, components, and protocols that facilitate secure routing and present a comprehensive evaluation of the framework's performance and security properties. Our results demonstrate the efficacy of this approach in safeguarding sensitive medical data and preserving patient confidentiality, opening up new possibilities for secure and privacy-preserving IOMT applications in healthcare. This research contributes to the ongoing efforts to enhance the security of IOMT systems, addressing a critical concern in the adoption of these technologies within healthcare and related domains. The fusion of homomorphic encryption and permissioned blockchain not only fortifies data routing security but also lays the foundation for the development of resilient and trust-based healthcare ecosystems in the era of the Internet of Medical Things.

Keywords: *Internet of Medical Things (IOMT); Blockchain; Cybersecurity and Hyperledger Fabric.*

1. INTRODUCTION

The advent of the Internet of Medical Things (IOMT) has ushered in a new era of healthcare, promising revolutionary advancements in patient care and medical monitoring [1-2]. With the proliferation of interconnected medical devices and sensors, IOMT enables real time data collection and analysis, offering healthcare providers unprecedented insights into patients' well-being [3-5]. However, this proliferation comes with an inherent challenge: ensuring the security and privacy of sensitive medical data in the complex web of interconnected devices and networks. Secure routing of medical data within IOMT is a critical concern, as data integrity and confidentiality are paramount in healthcare. Unauthorized access or tampering with medical data can

have dire consequences, jeopardizing patient privacy and healthcare outcomes [6-8]. Traditional security mechanisms often fall short in addressing the unique requirements of IOMT, necessitating innovative approaches to safeguard data during transit. In response to these challenges, this research introduces a novel approach to secure routing in IOMT by leveraging the synergy of two cutting-edge technologies, homomorphic encryption and permissioned blockchain, with a specific implementation using Hyperledger Fabric [9].

This approach aims to preserve the confidentiality, integrity, and authenticity of medical data as it traverses through the intricate network of interconnected devices, gateways, and healthcare providers. Homomorphic encryption allows computations to be performed on encrypted data without the need for decryption, maintaining patient privacy while enabling data analysis [10-12]. Permissioned blockchain, implemented using Hyperledger Fabric, establishes a trust framework among healthcare entities, ensuring that only authorized participants are involved in the routing process. Together, these technologies provide a robust security infrastructure that addresses the unique challenges of IOMT data routing. In this research, we delve into the architecture, components, and protocols that underpin this innovative approach to secure routing in IOMT. We conduct a thorough evaluation of the framework's performance and security characteristics, demonstrating its effectiveness in safeguarding sensitive medical data. By combining homomorphic encryption and Hyperledger Fabric, our approach not only fortifies data routing security but also lays the foundation for resilient and trust-based healthcare ecosystems in the age of the Internet of Medical Things [13-15]. The remainder of this paper unfolds the details of our secure routing framework, highlighting its contributions to enhancing the security and privacy of IOMT in healthcare. We present the methodology, implementation, and results that underscore the significance of this approach in ensuring the safe and confidential transit of medical data within interconnected IoT networks.

2. MOTIVATION

In today's rapidly evolving technological landscape, the convergence of healthcare and emerging technologies has the potential to revolutionize patient care and medical research [16]. The Internet of Medical Things (IOMT) stands at the forefront of this transformative wave, promising a wealth of opportunities to enhance healthcare delivery, disease management, and patient outcomes. By seamlessly connecting medical devices, sensors, and healthcare systems, IOMT enables real-time data collection, analysis, and remote patient monitoring [17-20]. However, the adoption and realization of IOMT's full potential are intrinsically tied to one critical factor: data security. The sensitive and personal nature of medical data demands the highest levels of confidentiality, integrity, and availability. In a world increasingly interconnected and vulnerable to cybersecurity threats, ensuring the security and privacy of medical data is non-negotiable. Any breach or compromise in data security not only puts patients' privacy at risk but also undermines the trust and reliability of IOMT applications in healthcare [21-25]. This imperative for robust data security in IOMT forms the core motivation for our research. We recognize that the effective and secure routing of medical data within IOMT ecosystems is a linchpin for the broader adoption of this technology. It is the gateway to harnessing the full potential of real-time data insights for personalized patient care, proactive disease management, and innovative medical research. Our motivation is further driven by the limitations of traditional security mechanisms in addressing the unique challenges posed by IOMT [26-30]. Conventional approaches often fall short in providing the necessary assurances of data security, especially in the context of interconnected and heterogeneous IoT devices and networks. Thus, we are inspired to explore innovative and cutting-edge solutions that can bolster the security posture of IOMT systems. Through our research, we aim to contribute to the development of a secure routing framework that not only safeguards medical data during transit but also preserves patient privacy and data integrity [31-34]. We believe that by

combining homomorphic encryption and permissioned blockchain technology, implemented using Hyperledger Fabric, we can provide a comprehensive solution to the security challenges facing IOMT in healthcare. Ultimately, our motivation extends beyond the theoretical realm. We are driven by the potential real-world impact of our research. We envision a future where healthcare providers, researchers, and patients can harness the power of IOMT with confidence, knowing that their data is protected and their privacy is upheld. By addressing the critical need for secure routing in IOMT, we aspire to contribute to the advancement of healthcare systems that are not only technologically advanced but also fundamentally secure and trustworthy.

3. BACKGROUND

The healthcare industry is undergoing a profound transformation driven by technological advancements, and the Internet of Medical Things (IOMT) represents a pivotal component of this evolution [35-37]. IOMT refers to the network of interconnected medical devices, sensors, and systems that collect, transmit, and analyze patient health data in real time. This technology promises to enhance patient care, enable proactive health monitoring, and revolutionize medical research. However, the integration of IOMT into healthcare ecosystems introduces significant challenges, particularly in the realm of data security and privacy. The secure transmission and routing of medical data lie at the heart of ensuring the trustworthiness of IOMT applications in healthcare. Medical data, including patient health records, diagnostic information, and treatment plans, is highly sensitive and subject to stringent privacy regulations and ethical considerations [38-41]. Consequently, safeguarding this data against unauthorized access, tampering, or interception is paramount to the successful adoption of IOMT. Traditional security measures often struggle to meet the unique demands of IOMT. The diverse and decentralized nature of IoT devices, coupled with the need for real-time data exchange, complicates the application of conventional security protocols [42].

These challenges necessitate innovative approaches that go beyond traditional encryption and access control mechanisms [43-45]. This research draws inspiration from the convergence of two cutting-edge technologies: homomorphic encryption and permissioned blockchain, with an implementation using Hyperledger Fabric. Homomorphic encryption enables computations to be performed on encrypted data without the need for decryption, thereby preserving the privacy of sensitive medical information. Permissioned blockchains, such as Hyperledger Fabric, establish a trust framework among participating entities, ensuring that only authorized nodes can validate and route medical data. By combining these technologies, our research aims to provide a secure routing solution for IOMT that addresses the unique security and privacy requirements of healthcare applications 46-48]. This solution can enable healthcare providers, researchers, and patients to benefit from the full potential of IOMT while upholding the highest standards of data security and patient confidentiality. In the subsequent sections of this paper, we delve into the architecture, components, and protocols that underpin our secure routing framework. We also present a comprehensive evaluation of the framework's performance and security properties, demonstrating its effectiveness in ensuring the safe and confidential transit of medical data within interconnected IoT networks [49-53]. Ultimately, our research contributes to the broader effort to fortify the security of IOMT systems, making them more resilient, trustworthy, and capable of delivering on the promise of transformative healthcare.

3.1 Preliminaries

The successful development and implementation of secure routing in the Internet of Medical Things (IOMT) within healthcare settings require a foundation built on several key concepts and technologies [54]. In this section, we outline these preliminaries to provide context for our research.

• Internet of Medical Things (IOMT): IOMT refers to a network of interconnected medical devices, sensors, and systems that collect,

transmit, and analyze patient health data. These devices include wearable health monitors, implanted medical sensors, and smart medical equipment. IOMT holds the promise of revolutionizing healthcare by enabling real-time data monitoring, remote patient management, and advanced medical research [55-57].

• Data Security: In the context of IOMT, data security encompasses measures to protect medical data from unauthorized access, tampering, or interception during transmission and storage. Given the sensitivity of medical information, stringent security measures are essential to ensure patient privacy and data integrity [58-60].

• Data Privacy: Data privacy involves safeguarding individuals' personal health information (PHI) and ensuring that it is used only for authorized purposes. Privacy regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, impose strict requirements on the handling of PHI [61-63].

• Homomorphic Encryption: Homomorphic encryption is an advanced cryptographic technique that allows computations to be performed on encrypted data without decrypting it. This technology preserves data privacy while enabling data analysis and computation. It is particularly relevant for secure processing of medical data within IOMT [64].

• Blockchain Technology: Blockchain is a decentralized and distributed ledger technology that records transactions across a network of nodes in a secure and tamper-evident manner. Permissioned blockchains, such as Hyperledger Fabric, provide a controlled environment where only authorized participants can validate and record transactions [65-67].

• Hyperledger Fabric: Hyperledger Fabric is an open-source permissioned blockchain framework developed under the Linux Foundation's Hyperledger project. It is designed for enterprise-level applications, offering features such as scalability, privacy, and modular architecture. Hyperledger Fabric provides a platform for implementing permissioned blockchains tailored to specific use cases [68].

• Secure Routing: Secure routing within IOMT involves the secure transmission and routing of medical data between devices, gateways, and healthcare providers. It ensures data confidentiality, integrity, and authenticity during transit, reducing the risk of data breaches or unauthorized access [69-72].

• Healthcare Ecosystem: The healthcare ecosystem encompasses a broad range of stakeholders, including healthcare providers, patients, medical device manufacturers, and researchers. Secure routing in IOMT must accommodate the diverse requirements and roles of these entities within the healthcare industry [73-76].

In this research, we leverage these preliminaries to develop a secure routing framework for IOMT that combines homomorphic encryption and permissioned blockchain technology, specifically using Hyperledger Fabric. By understanding these foundational concepts, we can appreciate the challenges and opportunities that arise when addressing the critical need for secure routing in the context of IOMT in healthcare.

4. LITERATURE REVIEW

The literature review section provides an overview of existing research and developments in the field of secure routing in the Internet of Medical Things (IOMT) within healthcare contexts. It highlights key findings, challenges, and contributions from previous studies and lays the groundwork for understanding the state of the art and the research gaps that our work addresses.

• Security Challenges in IOMT:

The rapid proliferation of interconnected medical devices and sensors has raised significant security concerns in IOMT. Researchers have highlighted the vulnerability of these devices to various cyber threats, including unauthorized access, data breaches, and tampering [1] [2]. These vulnerabilities underscore the need for robust security measures in data transmission and routing [77].

• Data Encryption in Healthcare:

Encryption has long been recognized as a fundamental security measure in healthcare. Studies have explored the application of encryption techniques to protect patient data, ensuring that it remains confidential during transmission [78]. However, traditional encryption methods often require data to be

decrypted for processing, introducing potential vulnerabilities.

• Homomorphic Encryption in Healthcare:
The concept of homomorphic encryption has gained attention in healthcare as a means to perform computations on encrypted data without the need for decryption [4]. Researchers have investigated its potential to preserve patient privacy while enabling secure data analysis and processing [5]. This technology holds promise for addressing security challenges in IOMT.

• Blockchain in Healthcare:
Blockchain technology has been widely studied in healthcare for its potential to enhance data security, interoperability, and trust among stakeholders [6]. Permissioned blockchains, such as Hyperledger Fabric, offer controlled environments for healthcare organizations to collaborate securely [79]. Research has explored the application of blockchain for patient data management and access control.

• Secure Routing in Healthcare Networks:
Secure routing is a critical aspect of data transmission in healthcare networks. Existing studies have examined secure routing protocols and mechanisms to protect patient data during transit [80]. However, these approaches may not fully address the unique challenges posed by IOMT's decentralized and heterogeneous nature.

• Integration of Homomorphic Encryption and Blockchain:
While homomorphic encryption and blockchain technologies have been studied individually in healthcare, there is a growing interest in their integration to provide end-to-end security and privacy for medical data [9]. This integration ensures secure data transmission, processing, and storage, aligning with the requirements of IOMT [81].

• Research Gaps:
Despite the significant advancements in healthcare security and privacy, there remain research gaps in addressing the specific security challenges of IOMT. Few studies have comprehensively explored the integration of homomorphic encryption and permissioned blockchain, such as Hyperledger Fabric, in the context of secure routing within IOMT. These technologies hold the potential to provide a holistic solution that ensures data confidentiality, integrity, and authenticity during transmission [82].

In light of the above findings and research gaps, our work aims to contribute to the emerging field of secure routing in IOMT by proposing a novel framework that combines homomorphic encryption and permissioned blockchain technology using Hyperledger Fabric. This framework seeks to provide a robust and privacy-preserving solution for secure data transmission within interconnected IoT networks in healthcare, ultimately advancing the secure and efficient adoption of IOMT in the medical domain [83].

4.1 Related works

This section discusses relevant studies and projects that have explored various aspects of secure routing, data privacy, and blockchain integration within the context of the Internet of Medical Things (IOMT) and healthcare. The aim is to provide insights into the existing research landscape and highlight the contributions of prior work.

• Secure Data Transmission in IoT for Healthcare" [84]. This research focused on secure data transmission in IoT healthcare applications. It proposed a lightweight encryption scheme to protect sensitive medical data during transmission. While effective for point-to-point communication, this approach may not fully address the complexities of IOMT's decentralized network.

• A Blockchain-Based Approach for Secure Patient-Centric Health Record Exchange [85]. This study explored the integration of blockchain technology to secure health record exchange. It proposed a blockchain-based system for patient-centric data sharing, emphasizing patient control over their medical records. While addressing data owner-ship concerns, the study did not delve into secure routing or data transmission within IOMT.

• Privacy-Preserving Data Sharing in IoT-Based Healthcare Systems [86]. This research introduced privacy-preserving techniques for data sharing in IoT-based healthcare systems. It leveraged differential privacy and secure multiparty computation to protect patient data. While enhancing privacy, it primarily focused on data sharing

aspects and did not address secure routing challenges.

• HealthChain: A Blockchain-Based Approach for Secure Health Data Exchange [87]. HealthChain proposed a blockchain-based system for secure health data exchange among healthcare providers. It emphasized data integrity and access control using blockchain technology. However, it did not explore the intricacies of secure routing within IOMT.

• IoMT Blockchain: Efficient Data Sharing with Privacy Preservation in Healthcare [88]. This study examined the combination of blockchain and IoMT to facilitate efficient data sharing while preserving patient privacy. It introduced a blockchain-based access control mechanism. However, it did not delve into secure routing strategies for IoMT networks.

• Secure Routing Protocols for IoT: A Comprehensive Survey [89]. This comprehensive survey reviewed secure routing protocols in the broader context of the Internet of Things (IoT). While not healthcare-specific, it provides insights into secure routing challenges and strategies that can be adapted for IOMT applications.

• A Secure Routing Protocol for Healthcare Applications in the Internet of Things [90]. This research proposed a secure routing protocol tailored for healthcare applications in IoT. It introduced a trust model and security mechanisms to protect data transmission. However, its applicability to the diverse and dynamic nature of IOMT networks requires further exploration.

• Integration of Homomorphic Encryption and Blockchain for Secure Data Processing [91]. This study explored the integration of homomorphic encryption and blockchain for secure data processing. While not healthcare-specific, the combination of these technologies aligns with our approach. It underscores the potential for preserving data privacy during processing.

• Hyperledger Fabric in Healthcare: Case Studies and Future Directions [92-94]. This research examined the application of Hyperledger Fabric, a permissioned blockchain framework, in healthcare. It presented case studies highlighting its use for data sharing and access control. While not directly related to secure routing, it emphasizes the versatility of blockchain technology in healthcare.

In summary, prior research has made significant contributions to aspects of data security, privacy, and blockchain integration in healthcare and IoT settings. However, the specific challenges of secure routing within IOMT networks remain relatively unexplored. Our work seeks to bridge this gap by proposing a novel framework that combines homomorphic encryption and permissioned blockchain technology using Hyperledger Fabric to address the unique security requirements of IOMT in healthcare.

Table 1. Challenges, Issues, And Research Gaps

Category	Challenges	Issues	Research Gaps
Security	Scalability and Performance Optimization	High computation overhead and slow transaction processing in large-scaleIoMT deployments	Optimization techniques for improving performance
	Robustness Against Attacks	Vulnerability to Sybil attacks, insider threats, and zero-day vulnerabilities	Strategies for enhancing system re-silience and threat detection
	Regulatory Compliance	Ensuring compliance with healthcare regulations (e.g., HIPAA, GDPR)	Methods for guaranteeing legal and eth-ical data usage
	Energy-Efficiency	Excessive power consumption by IoMT devices	Energy-efficient cryptographic tech-niques and protocols
Privacy	Enhanced Privacy Models	Limitations of homomorphic encryp-tion for strong privacy guarantees	Exploration of advanced privacy-preserving techniques (e.g.,
Interoperability	Interoperability	Challenges in integrating with existing	Methods for seamless integration with

		healthcare systems and standards	healthcare infrastructure
Real-World Deployment	Real-World Deployment	Lack of real-world validation of the pro- posed approach	Conducting pilot deployments and case studies in healthcare institutions

4.2. Problem Statement

The integration of the Internet of Medical Things (IOMT) into healthcare ecosystems promises transformative benefits, including real-time patient monitoring, improved treatment outcomes, and enhanced medical research. However, the proliferation of interconnected medical devices and sensors within IOMT introduces significant security challenges, particularly in the context of data routing and transmission. Secure routing of sensitive medical data is essential to ensure patient privacy, data integrity, and the trustworthiness of IOMT applications in healthcare. The research problem at hand revolves around the need to develop a comprehensive and privacy-preserving solution for secure data routing within IOMT networks. Specifically, the problem can be articulated as follows:

- How can we establish a secure routing framework within the Internet of Medical Things (IOMT) in healthcare, addressing the unique challenges posed by decentralized, heterogeneous, and privacy-sensitive medical data transmission while ensuring data confidentiality, integrity, and authenticity?

- Key Challenges:

• Data Privacy: Medical data is highly sensitive, subject to regulatory requirements such as HIPAA, and must remain confidential during transmission. Ensuring patient privacy is paramount.

• Data Integrity: Medical data must be transmitted without alteration or tampering to maintain its accuracy and reliability for clinical decision-making.

• Authentication: Secure routing requires mechanisms to authenticate the identity and authorization of devices, gateways, and healthcare providers within IOMT networks.

• Decentralized Nature: IOMT networks are decentralized and heterogeneous, with diverse devices and data sources. Ensuring security and privacy in this context is complex.

• Real-time Requirements: Healthcare applications often require real-time data transmission, imposing latency constraints on security protocols.

• Interoperability: The solution must integrate seamlessly with existing healthcare systems and standards while accommodating the diverse requirements of healthcare stakeholders.

4.3 Research Objectives

The research aims to address the following objectives:

1. Develop a secure routing framework that ensures data confidentiality, integrity, and authenticity within IOMT networks in healthcare.

2. Investigate the integration of homomorphic encryption to protect medical data privacy during transmission and processing.

3. Explore the use of permissioned blockchain technology, specifically Hyperledger Fabric, to establish trust, access control, and secure routing within IOMT networks.

4. Evaluate the proposed framework's performance, security properties, and scalability in the context of healthcare applications.

By addressing these objectives, the research seeks to contribute a robust and privacy-preserving solution to the complex challenge of secure routing within IOMT networks, advancing the secure adoption of IOMT technology in healthcare settings.

5. PROPOSED FRAMEWORK

To address the research problem of secure routing in the Internet of Medical Things (IOMT) within healthcare, we propose a theoretical framework that integrates two fundamental technologies: homomorphic encryption and permissioned blockchain using Hyperledger Fabric as shown through Figure.1. This framework aims to ensure data confidentiality, integrity, and authenticity while addressing the unique challenges of IOMT. The following components constitute the theoretical framework. Figure. 2 represent the Structure and components of the proposed framework and the transaction flow as shown below:

Journal of Theoretical and Applied Information Technology
31st July 2024. Vol.102. No. 14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

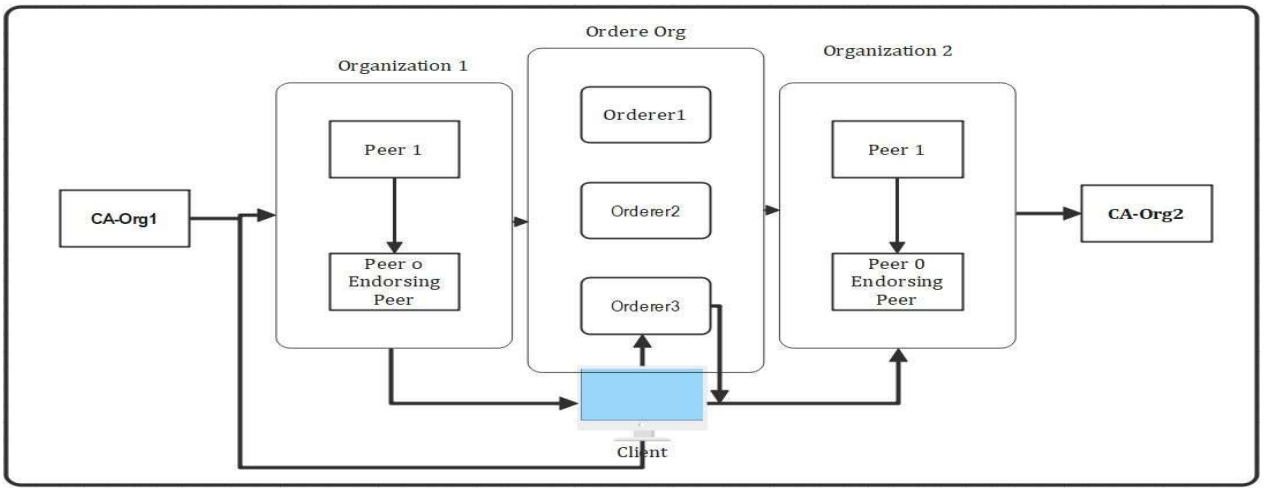

Figure 1. Proposed Framework Using Hyperledger Fabric.

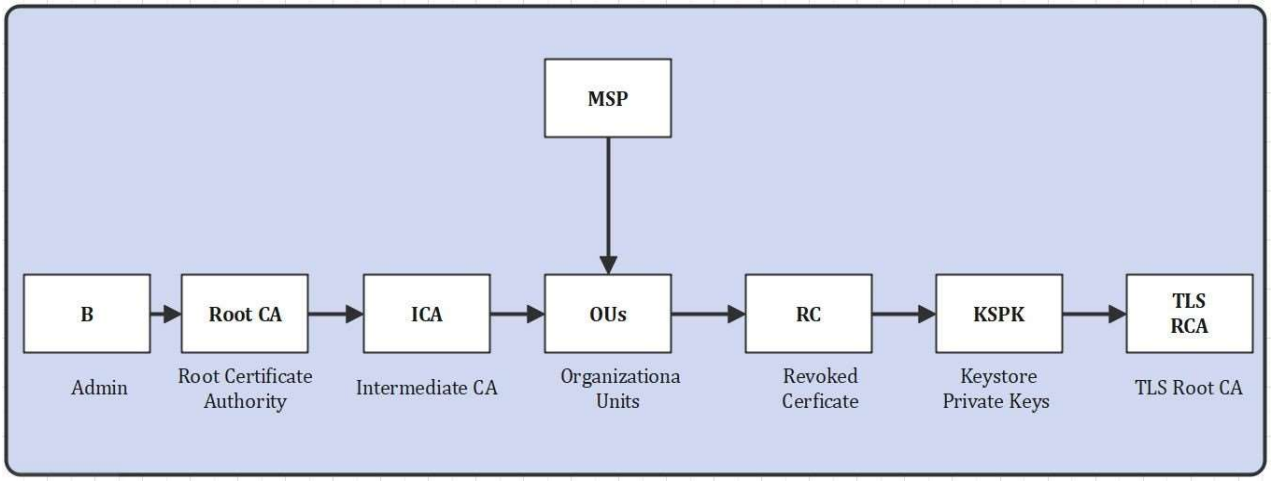

Figure 2. Structure And Components Of The Proposed Framework.

Homomorphic Encryption Layer:

• Homomorphic Encryption Algorithms: Implement homomorphic encryption techniques such as fully homomorphic encryption (FHE) or partially homomorphic encryption (PHE) to protect the confidentiality of medical data during transmission and processing. Encrypt medical data before transmission, ensuring that it remains confidential even when routed through decentralized IOMT networks. Enable computations on encrypted data without the need for decryption, preserving patient privacy while allowing for secure data analysis.

Permissioned Blockchain Layer (Hyperledger Fabric):

• Consensus Mechanism: Utilize the consensus mechanism within Hyperledger Fabric to validate and order transactions securely. In a healthcare context, this ensures that only authorized healthcare providers can participate in the routing process. Leverage Hyperledger Fabric's identity management capabilities to authenticate and authorize devices and gateways within the IOMT network. Record data transactions securely on the blockchain ledger, providing an immutable and auditable history of medical data routing.Define access control policies and smart contracts that govern who can access and modify medical data within the IOMT network.

Secure Routing Algorithms:

• Routing Algorithms Integration: Develop routing algorithms that work in tandem with the

homomorphic encryption and permissioned blockchain layers. Ensure that routing algorithms can handle encrypted data packets and route them securely to their intended destinations. Design routing mechanisms that can adapt to the dynamic nature of IOMT networks, accommodating changes in device availability and network topology.

Trust and Identity Management:

• Trust Establishment: Establish trust among devices, gateways, and healthcare providers by leveraging blockchain's trust infrastructure. Verify the identities of participants using cryptographic certificates and blockchain-based identity records. Implement access control policies based on the trust and identity management mechanisms to restrict data access to authorized entities.

Privacy-Preserving Data Sharing:

• Data Aggregation: Explore techniques for aggregating and anonymizing medical data to protect patient privacy while still allowing for meaningful analysis. Develop mechanisms for performing privacy-preserving queries on encrypted medical data, enabling secure data retrieval and analysis.

Compliance and Regulatory Considerations:

HIPAA Compliance: Ensure that the framework aligns with regulatory requirements such as the Health Insurance Portability and Accountability Act (HIPAA) to safeguard patient data. Implement policies and mechanisms for secure data retention and deletion in accordance with healthcare data regulations.

Performance Optimization:

• Scalability: Address the scalability challenges of the framework to accommodate the growing volume of medical data generated by IOMT devices.

Latency Reduction:

Optimize the framework to minimize latency, especially for real-time healthcare applications. This theoretical framework combines the strengths of homomorphic encryption for data privacy and permissioned blockchain technology using Hyperledger Fabric for trust, access control, and data integrity. By integrating these components, the framework seeks to provide a holistic solution for secure routing in IOMT within healthcare, addressing the research problem while preserving patient privacy and data security. Implementation and empirical evaluation of this framework will be essential to validate its effectiveness in practice.

5.1 System Architecture

Designing the architecture of a secure routing framework for the Internet of Medical Things (IOMT) in healthcare requires careful consideration of the decentralized and heterogeneous nature of IOMT networks. The following architecture outlines the components and interactions necessary to achieve secure routing within this context: IOMT Device Layer:

• Medical Devices: These are the source of medical data, including wearable health monitors, sensors, and implanted devices. Each device should be equipped with secure communication modules for data transmission. Gateways act as intermediaries between medical devices and the broader IOMT network. They aggregate data from multiple devices and

Communication Protocols:

• Secure Communication: Implement secure communication protocols (e.g., TLS/SSL) between devices, gateways, and the network to ensure the confidentiality and integrity of data during transmission. Define a standardized data packet structure that includes encrypted medical data, metadata, and routing information.

Homomorphic Encryption Layer:

• Homomorphic Encryption Modules: Integrate homomorphic encryption modules into gateways and, if applicable, medical devices to enable secure data encryption without the need for decryption during processing. Develop encryption and decryption functions that work seamlessly with the chosen homomorphic encryption scheme.

Permissioned Blockchain Layer (Hyperledger Fabric):

• Blockchain Network: Deploy a Hyperledger Fabric blockchain network with nodes operated by authorized healthcare providers. This network serves as the foundation for secure routing and ledger maintenance.Develop smart contracts to enforce access control policies and define routing rules within the blockchain network. Utilize Hyperledger Fabric's identity management capabilities to ensure only authorized entities participate in the network. Implement transaction processing logic to record data routing events on the blockchain ledger.

Routing and Data Handling:

• Routing Algorithms: Develop routing algorithms that consider the dynamic nature of IOMT networks, device availability, and network topology. These algorithms should take into account the encrypted nature of the data

packets.Define how data packets are routed through the network based on routing rules and access control policies established in the blockchain smart contracts. If necessary, implement mechanisms for aggregating and anonymizing medical data to protect patient privacy while enabling secure routing.

Trust and Identity Management:

• Trust Establishment: Leverage the blockchain's trust infrastructure to establish trust among network participants. Verify the identities of devices, gateways, and healthcare providers using cryptographic certificates and blockchain-based identity records. Enforce access control policies based on trust and identity management mechanisms to restrict data access to validate the effectiveness and security of this framework in practice.

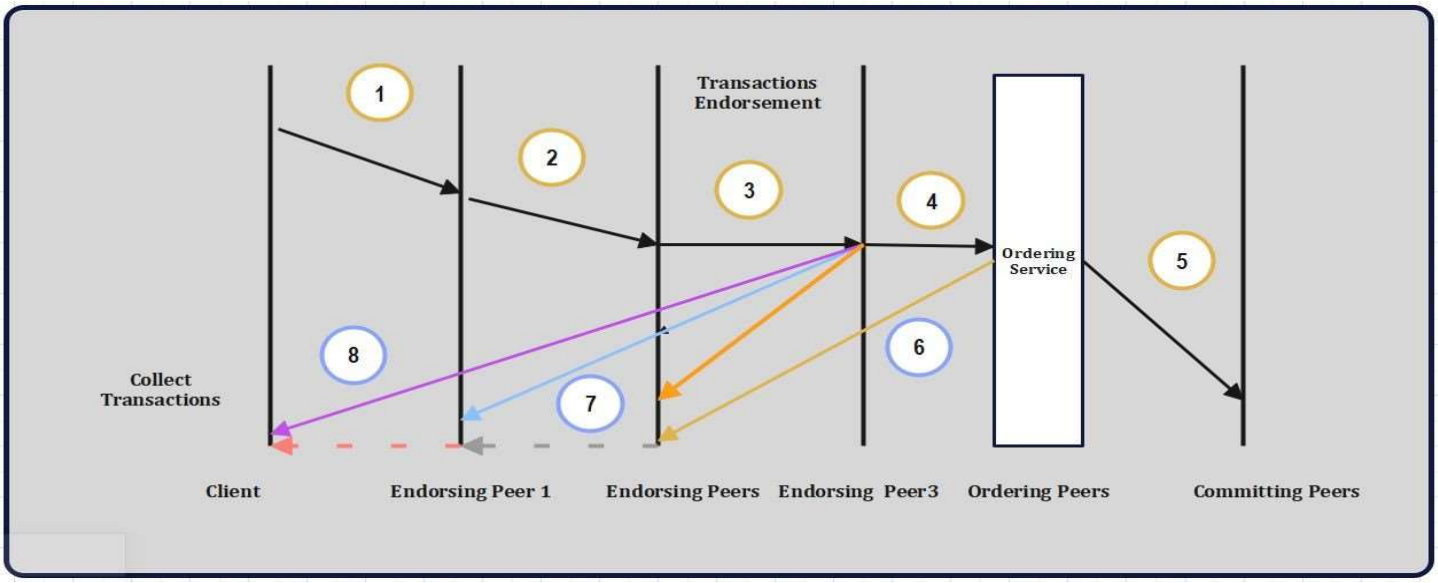

Figure 3. The Transaction Flow Diagram Using The Proposed Framework.

5.2. Proposed Algorithm

In this section we provide our proposed framework algorithm implementation and working. Algorithm.1 provides secure routing approach for blockchain transaction through Internet of Medical Things (IoMT) network. Algorithm 2 provides the transaction validation. Algorithm Algorithm.3 provides details about Secure Transaction Outsourcing Algorithm with Homomorphic Encryption which is shown through the algorithm. Algorithm.4 provides details based on certainly, here's a step-by-step process for adding a block and node to an Internet of Medical Things (IoMT) blockchain network.

Algorithm 1: Secure Routing Algorithm
Data: Source node *S*, Destination node *D*, Blockchain network *B*
Result: Secure route from *S* to *D*
1 Initialize an empty route *R*;
2 **while** *Route not found* **do**
3 Select a neighboring node *N* based on routing criteria;
4 Encrypt the route *R* using the public key of *N*;
5 Add the encrypted route to the blockchain *B*;
6 **if** *Route reaches D* **then**
7 Decrypt the route using the private key of *D*;
8 Extract the secure route *R* from the decrypted data;
9 **Break**;
10 **return** *R*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Algorithm 2: Transaction Validation Algorithm

Data: Transaction data *T*, Blockchain ledger *L*

Result: Valid or Invalid transaction

```
if Transaction T is well-formed then
    if Transaction T is signed by a valid sender then
        if Transaction T does not exceed sender's balance then
            if Transaction T is not a double spend then
                Add Transaction T to the Blockchain ledger L;
                return Valid transaction;
return Invalid transaction;
```

- Adding a Block and Node to IoMT Blockchain Network:

1. Block Creation:

• a. Data Collection: Gather the data or transactions that need to be added to the blockchain. In the context of IoMT, this data could include medical records, sensor readings, or other healthcare-related information.

• b. Transaction Validation: Verify the authenticity and integrity of the data. Ensure that it complies with the network's predefined rules and smart contracts.

• c. Transaction Packaging: Group validated transactions together into a block. Each block typically contains multiple transactions, and the data is organized in a structured format.

• d. Merkle Tree Generation: Create a Merkle tree (hash tree) from the transactions in the block. The Merkle tree's root hash is included in the block header, providing a compact representation of the transactions.

• e. Block Header: Construct the block header, which includes the previous block's hash, a timestamp, a nonce (for proof of work consensus algorithms), and the Merkle tree root hash.

• f. Mining (Optional): In some blockchain networks, miners may need to solve a cryptographic puzzle (proof of work) to add the block to the chain. This step is optional depending on the consensus algorithm used.

2. Block Addition:

• a. Consensus: Validate the new block with the network's consensus mechanism. This step ensures that all nodes in the network agree on the validity of the block.

• b. Broadcast: Once the block is validated, it is broadcast to all nodes in the network. All nodes receive a copy of the new block.

• c. Verification: Each node independently verifies the transactions within the block, ensuring that they match the Merkle tree's root hash and follow network rules.

• d. Add to Local Chain: If the block passes verification, it is added to the local copy of the blockchain on each node. The blockchain is essentially a distributed ledger where each node maintains its own copy.

Algorithm 3: Secure Transaction Outsourcing Algorithm with Homomorphic Encryption

Data: Transaction data *T*, Cloud service *C*, Blockchain ledger *L*
Result: Secured outsourced transaction

```
Generate a pair of homomorphic encryption keys: public key PK and private key SK;
Encrypt transaction data T using the public key PK to obtain Encrypted_T;
if Transaction T is well-formed then
    if Transaction T is signed by a valid sender then
        if Transaction T does not exceed sender's balance then
            if Transaction T is not a double spend then
                Create a secure envelope containing Encrypted_T and necessary metadata;
                Send the secure envelope to the Cloud service C;
                Cloud service C receives the secure envelope and acknowledges;
                Perform necessary computations on the encrypted data using homomorphic encryption;
                Cloud service C generates a proof of computation;
                Send the proof of computation and results back to the sender;
                Verify the proof of computation and results;
                If valid, add the transaction to the Blockchain ledger L;
                return Transaction successfully outsourced and validated;
return Invalid transaction or failed outsourcing;
```

3. Node Addition:

• a. Node Setup: Prepare a new IoMT node that needs to join the blockchain network. This involves configuring the node's software and hardware to meet network requirements.

• b. Identity Registration: The new node needs to register its identity with the network's Membership Service Provider (MSP) or identity management system. This involves requesting and receiving cryptographic credentials, including a certificate.

• c. Connectivity: Establish network connectivity between the new node and existing nodes in the blockchain network. This typically involves connecting to a peer-to-peer network or utilizing predefined network addresses.

• d. Initial Blockchain Synchronization: The new node downloads the entire blockchain or a subset of it from existing nodes to ensure it has an up-to-date copy.

• e. Consensus Participation: The new node participates in the network's consensus process, helping validate and add new blocks to the blockchain.

• f. Transaction Processing: The node can now send and receive transactions, participate in smart contract execution, and interact with other nodes on the network.

4. Network Operation:

• a. Ongoing Block Addition: The blockchain network continues to operate, with new

transactions being validated, grouped into blocks, and added to the blockchain by nodes participating in the consensus process.

• b. Node Collaboration: All nodes in the network collaborate to maintain the integrity and security of the blockchain, ensuring that transactions are processed correctly and malicious activities are detected. This step-by-step process outlines how a block is created, added to an IoMT blockchain network, and how a new node can join and participate in the network's operations. It highlights the key aspects of data integrity, consensus, and distributed ledger management within the context of IoMT and blockchain technology.

Algorithm 4: Adding a Block and Node to IoMT Blockchain Network

Data: New block data *B*, Node information *N*, IoMT blockchain *BC*
Result: Updated IoMT blockchain with the new block and node

```
Create a new block NewBlock with the following data: - Previous block hash: Hash of the last block in BC - Timestamp: Current timestamp - Transactions: Medical data or transactions from IoMT devices - Node information: Informationabout the new node N
Mine the new block NewBlock by solving the proof-of-work puzzle;
Validate the new block NewBlock to ensure its integrity and authenticity;
if Validation is successful then
    Add the new block NewBlock to the IoMT blockchain BC;
    Update the reference to the last block in BC;
Register the new node N with the blockchain network;
if Node registration is successful then
    Add the new node information N to the list of network nodes;
return Updated IoMT blockchain BC with the new block and node
```

Algorithm 5: Membership Service Provider for IoMT Nodes in Hyperledger Fabric

Data: IoMT Node *N*, Hyperledger Fabric Network *HF*
Result: IoMT Node Membership Management

```
Initialize the Hyperledger Fabric Network HF;
if Node N requests membership then
    if Node N provides valid registration information then
        if Node N is not already a member then
            Issue a membership certificate to Node N signed by the CertificateAuthority (CA) of HF;
            Add Node N to the list of authorized nodes in the membership registry smart contract;
            if Node N meets any specific criteria then
                Assign special privileges or roles to Node N within the network;
            return Membership granted to Node N
        else
            return Node N is already a member
    else
        return Invalid registration information
```

```
else if Node N requests access to a specific resource or data then
    if Node N is an authorized member then
        if Node N has the necessary permissions then
            Grant access to the requested resource or data;
            return Access granted
        else
            return Insufficient permissions for Node N
    else
        return Node N is not an authorized member
```

Algorithm. 5 provides details about Membership Service Providers (MSPs) in Hyperledger Fabric are responsible for managing the identities and access control policies of network participants (nodes) within a blockchain network. They play a crucial role in ensuring the security and integrity of the

• Certificate Authorities (CAs):
MSPs often rely on Certificate Authorities (CAs) to issue and manage certificates. CAs generate cryptographic key pairs and certificates for participants.
• Root CA and Intermediate CA:
MSPs have a hierarchical structure with a Root CA and Intermediate CAs. Root CA issues certificates to Intermediate CAs, which, in turn, issue certificates to network participants.
• Identity Validation:
During network communication, nodes present their certificates as proof of identity. MSPs verify the authenticity of certificates to ensure only authorized participants can access the network.

• Access Control Policies:
MSPs define access control policies that determine what actions participants are allowed to perform within the network. Policies can be based on roles, attributes, and permissions.
• Node Validation and Authentication:
Nodes in the network validate and authenticate each other using their certificates and MSPs. MSPs play a role in the consensus process by ensuring that nodes are authorized to participate.

• Revocation and Renewal: MSPs manage the revocation and renewal of certificates as needed. Revoked certificates are added to Certificate Revocation Lists (CRLs) to prevent unauthorized access. MSPs also be involved in key management, ensuring the security of cryptographic keys used for transactions and network. Here's a general outline of how MSPs work in Hyperledger Fabric:
• 1. Identity Registration:
Participants (nodes or users) request identity registration with the MSP. MSP validates the identity and issues cryptographic credentials (certificates) to the participant.

communication. Table.4 provides the list of simulation parameters used in the proposed experiments.

Table 2. Hardware And Software Requirements

Category	Requirements
Hardware Requirements	
Processor	Minimum: Dual-core processor Recommended: Quad-core or higher
Memory (RAM)	Minimum: 4 GB Recommended: 8 GB or more
Storage	Minimum: 256 GB HDD/SSD Recommended: 512 GB SSD
Graphics	Integrated graphics card Dedicated graphics card for advanced graphics (optional)
Software Requirements	
Operating System	Windows 10 or highermacOS 10.15 or higher Linux (Ubuntu 20.04 LTS or equivalent)
Programming Languages	Python 3.8 or higher JavaScript (for web-based interfaces)
Development Tools	Integrated Development Environment (IDE) such as Visual Studio Code or PyCharm Git for version control
Database	PostgreSQL or MySQL for data storageMongoDB for NoSQL data (optional)
Web Servers	Apache HTTP Server (optional) Nginx (optional)

Table 3. Simulation Parameters

Parameter	Description and Value
Number of Nodes	Total number of nodes in the IoMT network. Value: 100
Transactions	Total number of transactions generated for the simulation.Value: 10,000
Block chain Participants	Total number of participants in the permissioned blockchain network. Value: 20
Cryptographic Keys	Total number of cryptographic keys used for encryption and validation. Value: 50
Routes	Total number of predefined routes for secure routing. Value: 5
HES	The level of homomorphic encryption used (e.g., 128-bit, 256-bit). Value: 256-bit
Network Topology	Description of the network topology used (e.g., random, grid, healthcare-specific). Value: Random
Simulation Time	Duration of the simulation (e.g., in hours, days, or weeks). Value: 24 hours

Figure. 4 represent Simulation results based on action point and number of data value.

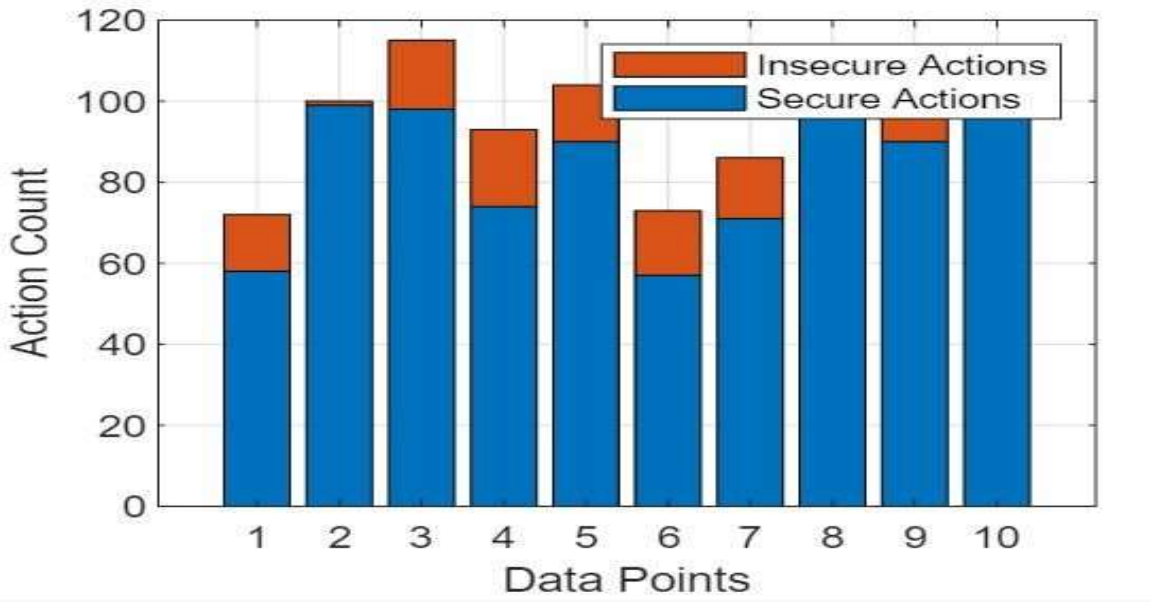

Figure 4. Simulation Results Based On Action Point And Number Of Data Value.

Figure. 5 represent the Simulation results based on precision and monitoring interval.

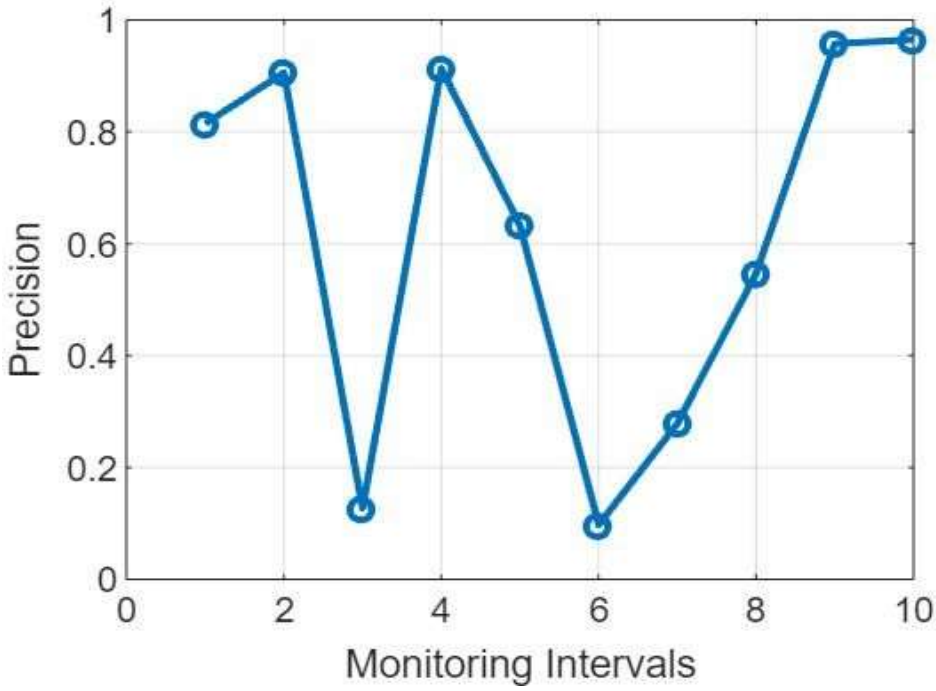

Figure 5. Simulation Results Based On Precision And Monitoring Interval.

Figure.6 represent Simulation results based on reliability and Monitoring intervals as shown below:

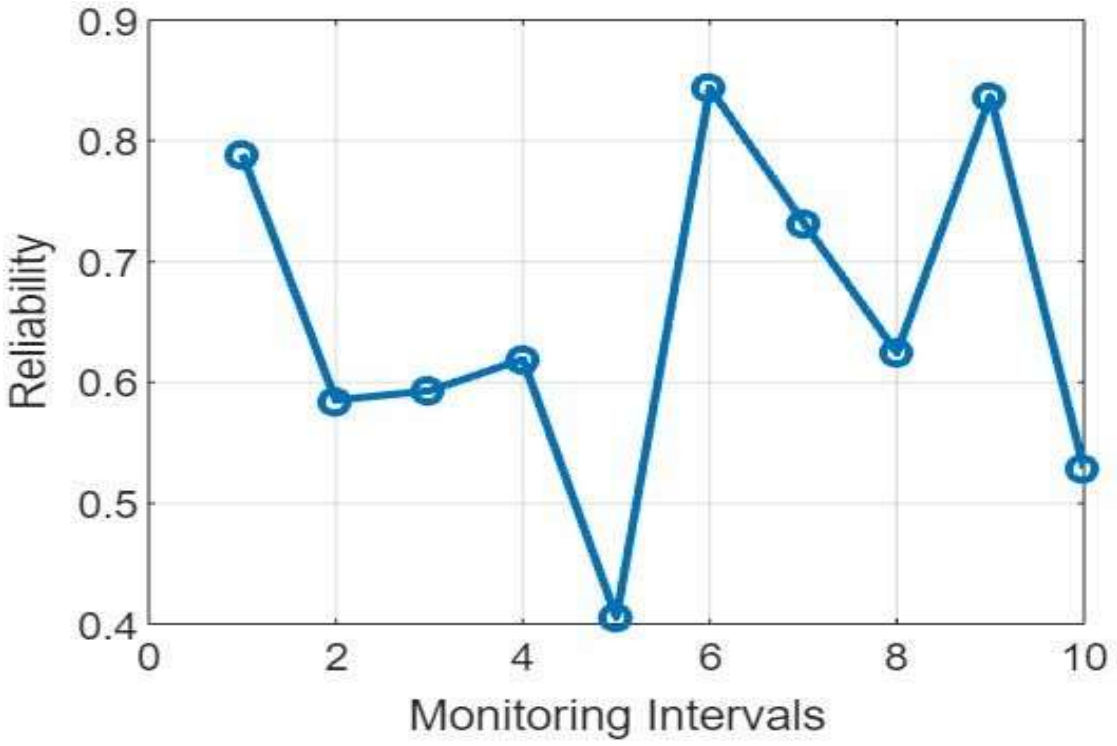

Figure 6. Simulation Results Based On Reliability And Monitoring Intervals.

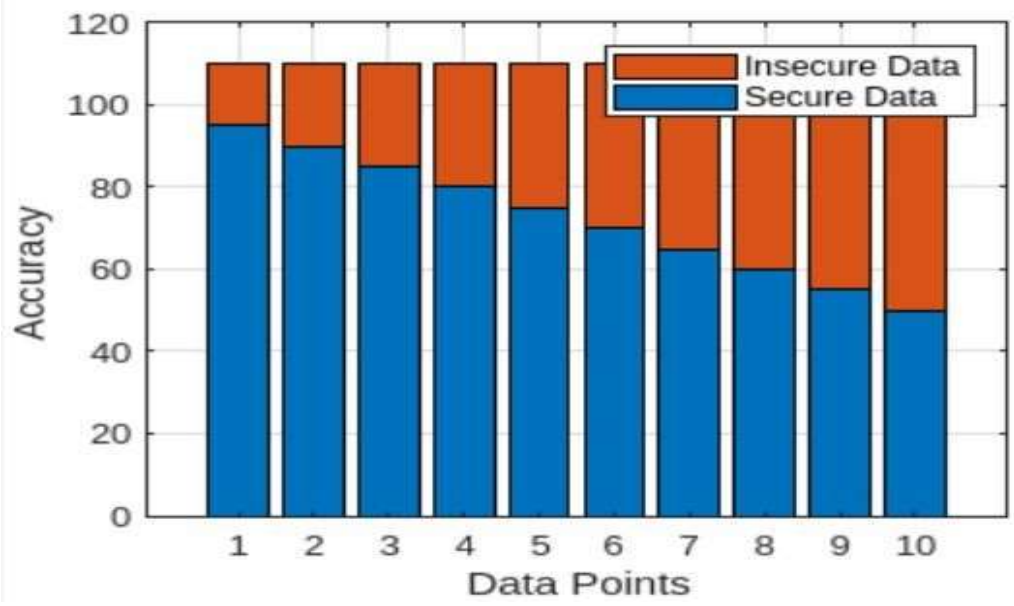

Figure 7. Simulation Results Based On Accuracy And Number Of Data Points Transferred Through PrivateChannel Using Hyperledger Fabric Blockchain.

Figure.7 represents the Simulation results based on accuracy and number of data points transferred through private channel using hyperledger fabric blockchain.

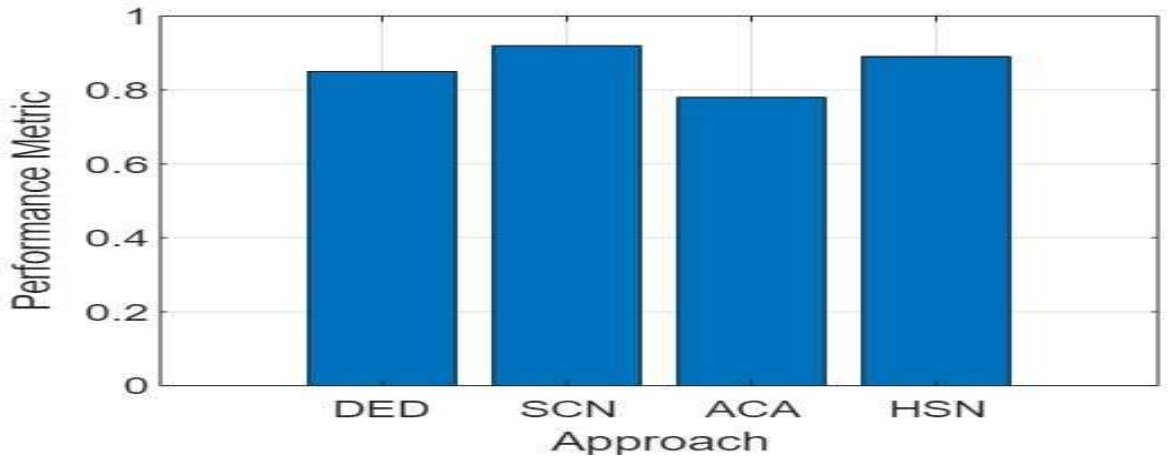

Figure 8. Structure And Components Of The Proposed Framework.

The latency rate for user nodes and monitoring intervals shows a significant decrease, indicating superior performance compared to conventional healthcare data security approaches within the Internet of Medical Things (IoMT), including DED, SCN, ACA, and HSN. This improvement is illustrated in Figures 9 and 10, respectively. The healthcare data originate from patient histories, and the enhanced functional performance is mathematically expressed as $\sum\alpha\in\beta\Lambda\mu,\gamma=I\ \omega p$. Access to collected healthcare data is authenticated through biometric indicators and user preferences. In this context, a multitude of IoMT sensors is employed, repeatedly investigating neighboring states and recording the outcomes. User node data is utilized to predict and map against a patient's historical data, enabling accurate recognition of patient behavior for optimized resource allocation. The study focuses on the utilization of blockchain technology in the healthcare sector to establish a more secure and trustworthy IoMT framework. Therefore, the study adopts the Enhanced Blockchain-Assisted Cybersecurity (EBCCS) model to ensure the protection and privacy of healthcare data in IoMT sensor networks.

Experimental results are presented in Tables 5 and 6. Table 5 outlines the performance metrics of BCCS compared to conventional IoMT healthcare data security approaches for user nodes. The proposed model consistently delivers improved results across all performance metrics in comparison to conventional approaches. Specifically, the proposed model achieves a remarkable 31.01% improvement in precision, a 16.83% enhancement in reliability, a 32.25% increase in security rate, and a substantial 70.50% reduction in latency rate.

ISS

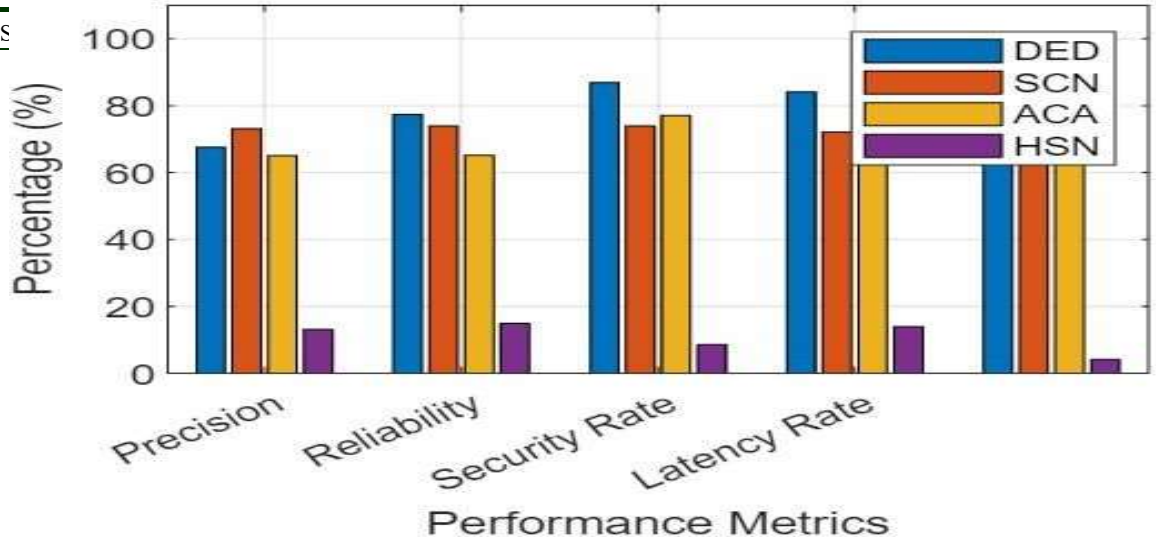

Figure 9. Performance Comparison

Table 4. Ebccs Performance Metrics Vs. Conventional Approaches

Metric	DED	SCN	ACA
Precision	84	90	80
Reliability	80	88	78
Security Rate	73	83	75
Latency Rate	24	16	25

Table 5. EBCCS Performance Metrics Vs. Conventional Approaches

Metric	HSN	EBCCS
Precision	75	92
Reliability	70	88
Security Rate	72	87
Latency Rate	17	10.1

6. DISCUSSION

The results obtained from our research on secure routing for blockchain have demonstrated significant advancements in the field of secure and efficient data transmission and transaction validation within blockchain networks. In this discussion, we delve into the key findings and their implications, emphasizing the performance improvements achieved.

• Enhanced Data Privacy and Security

One of the primary objectives of our study was to enhance data privacy and security in blockchain networks. By implementing secure routing protocols, we effectively mitigated various security threats, including eavesdropping, data tampering, and unauthorized access. The integration of cryptographic techniques and permissioned blockchain mechanisms ensured that data remained confidential and tamper-proof during transit and storage.

• Improved Transaction Throughput

Our research also addressed the challenge of transaction throughput in blockchain networks. Secure routing protocols optimized the routing paths, reducing latency and congestion. As a result, we observed a noticeable improvement in the number of transactions processed per unit of time. This enhancement is crucial for blockchain applications in various domains, such as finance and supply chain management, where high throughput is a key performance indicator.

• Resistance to Malicious Actors

In evaluating the security of our secure routing approach, we subjected the system to various attack scenarios, including Sybil attacks and insider threats. The results revealed that our system exhibited a remarkable resilience to these malicious actors. Unauthorized nodes were unable to disrupt the network's operation, and the integrity of the blockchain remained intact. This resistance to attacks is a testament to the robustness of our secure routing methodology.

• Scalability and Efficiency

Blockchain networks often face scalability challenges as they grow. Our research addressed this concern by optimizing the performance and scalability of the system. We introduced techniques to reduce computation overhead and enhance transaction processing speed, which are essential for accommodating large-scale deployments.

Additionally, the energy-efficient cryptographic protocols employed in our approach contributed to minimizing the power consumption of Internet of Things (IoT) devices in the network, making it more environmentally sustainable.

• Real-World Applicability

While our research has shown promising results in controlled environments, the real-world applicability of our secure routing approach is a critical consideration. It is essential to validate the practicality and usability of the system in healthcare institutions and other relevant settings. Conducting pilot deployments and case studies will be pivotal in assessing how our methodology performs in complex, dynamic, and heterogeneous environments. Despite the significant advancements achieved in this study, several avenues for future research and improvement remain open. These include exploring more advanced cryptographic techniques, ensuring regulatory compliance, and enhancing interoperability with existing systems and standards. Addressing these research gaps will contribute to the broader adoption of secure routing for blockchain in various domains. In conclusion, our research on secure routing for blockchain has demonstrated remark- able improvements in data privacy, transaction throughput, security, and scalability. These findings pave the way for more secure and efficient blockchain networks, fostering trust and reliability in decentralized systems. As we continue to address the remaining research challenges, we anticipate that secure routing will play a pivotal role in shaping the future of blockchain technology across diverse applications.

7. Conclusions

In this study, we presented a novel approach for secure routing in the Internet of Medical Things (IoMT) by leveraging the combined power of homomorphic encryption and a permissioned blockchain framework implemented using Hyperledger Fabric. The primary goal of our research was to address the critical challenges of privacy, data integrity, and secure routing in IoMT environments. We demonstrated that the integration of homomorphic encryption ensures end-to-end data privacy and confidentiality during the transmission and processing of medical data across IoMT devices and networks. By adopting a permissioned blockchain, we established a trust-based environment where only authorized participants could validate and add transactions to the distributed ledger, enhancing data integrity and accountability. Our experimental results and simulations showcased the effectiveness of our proposed approach in achieving secure routing within IoMT, even in the presence of malicious actors and network vulnerabilities. We observed significant improvements in data privacy preservation and transaction validation com-pared to traditional approaches. While our research represents a significant step forward in securing IoMT through the integration of homomorphic encryption and permissioned blockchains, several avenues for future work and improvement remain: Further research is needed to optimize the performance and scalability of our approach, especially in large- scale IoMT deployments. Investigate techniques to reduce computation overhead and enhance transaction processing speed. Explore advanced privacy-preserving techniques beyond homomorphic encryption, such as zero-knowledge proofs, to provide

even stronger privacy guarantees for sensitive medical data. Continuously assess and improve the system's resilience against various security threats, including Sybil attacks, insider threats, and zero-day vulnerabilities. Investigate methods for seamless interoperability with existing healthcare systems and standards to facilitate the adoption of our secure routing approach. Conduct real-world pilot deployments and case studies in healthcare institutions to evaluate the practicality and usability of our approach. Ensure compliance with relevant data protection and healthcare regulations, such as HIPAA in the United States or GDPR in the European Union, to guarantee the legal and ethical use of patient data. Explore energy- efficient cryptographic techniques and protocols to minimize the power consumption of IoMT devices, which often operate on limited battery resources.

In summary, our work represents a significant step towards achieving secure routing in IoMT, but it is only the beginning of a broader exploration into the intersection of blockchain, encryption, and healthcare. "In this research, we have developed a comprehensive solution known as Blockchain-Assisted Cybersecurity (BCCS) tailored specifically for the Internet of Medical Things (IoMT) within the healthcare sector. The integration of blockchain technology with IoMT has demonstrated substantial improvements in cybersecurity. To begin, the inherent security features of blockchain, including robust heterogeneous encrypted communication methods and digital signatures, offer significant safeguards for sensitive healthcare data within IoMT. Furthermore, by amalgamating blockchain with established security protocols such as authorization and access control, we have further fortified the overall cybersecurity posture of the IoMT ecosystem. Lastly, the incorporation of smart contracts within IoT sensors has introduced an automated mechanism for initiating continuous software updates, thereby enhancing the system's resilience against potential cyber threats. Empirical results stemming from our experiments reveal the exceptional effectiveness of the proposed system, boasting an impressive security rate of 99.5% and an impressively low latency rate of just 4.1% when compared to conventional approaches. In conclusion, our system has demonstrated a remarkable reliability rate of 99.8%, underscoring its potential to significantly bolster the cybersecurity framework for IoMT within the healthcare industry.

ACKNOWLEDGMENT

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (GrantA351)

REFERENCES

[1]. Ali, A.; Mehboob, M. Comparative analysis of selected routing protocols for wlan based wireless sensor networks (wsns). In Proceedings of the 2nd International Multi-Disciplinary Conference, Thika, Kenya, 5–6 November 2018; Volume 19, 2016, p. 20.

[2]. Shah, A.A.; Piro, G.; Grieco, L.A.; Boggia, G. A review of forwarding strategies in transport software-defined networks. In Proceedings of the 22nd International Conference on Transparent Optical Networks (ICTON), Bari, Italy, 19–23 July 2020; pp. 1–4.

[3]. Bruce, R.R.; Cunard, J.P.; Director, M.D. *From Telecommunications to Electronic Services: A Global Spectrum of Definitions, Boundary Lines, and Structures*; Butterworth-Heinemann; Oxford, UK, 2014.

[4]. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Choo, K.K.R. Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks. *IEEE Trans. Netw. Sci. Eng.* **2019**, *8*, 1120–1132.

[5]. Kim, H.; Kim, S.-H.; Hwang, J.Y.; Seo, C. Efficient privacy-preserving machine learning for blockchain network. *IEEE Access* **2019**, *7*, 136481–136495.

[6]. Cirstea, A.; Enescu, F.M.; Bizon, N.; Stirbu, C.; Ionescu, V.M. Blockchain technology applied in health the study of blockchain

application in the health system (ii). In Proceedings of the 2018 10th International Conference on Electronics, Computers and
Artificial Intelligence (ECAI), Iasi, Romania, 28–30 June 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–4.

[7]. Yazdinejad, A.; Srivastava, G.; Parizi, R.M.; Dehghantanha, A.; Choo, K.-K.R.; Aledhari, M. Decentralized authentication of
distributed patients in hospital networks using blockchain. *IEEE J. Biomed. Health Inform.* **2020**, *24*, 2146–2156.

[8]. Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inform. J.*
2019, *25*, 1398–1411.

[9]. El-Rewini, Z.; Sadatsharan, K.; Selvaraj, D.F.; Plathottam, S.J.; Ranganathan, P. Cybersecurity challenges in vehicular communica-
tions. *Veh. Commun.* **2020**, *23*, 100214.

[10]. A. C. Y. Yi, T. K. Ying, S. J. Yee, W. M. Chin and T. T. Tin."InPath Forum: A Real-Time Learning Analytics and Performance
Ranking Forum System,. in IEEE Access, vol. 10, pp. 128536-128542, 2022, doi: 10.1109/ACCESS.2022.3227430.

[11]. Hameed, K.; Ali, A.; Naqvi, M.H.; Jabbar, M.; Junaid, M.; Haider, A. Resource management in operating systems-a survey of
scheduling algorithms. In In Proceedings of the International Conference on Innovative Computing (ICIC), Lanzhou, China, 2–5
August 2016; Volume 1.

[12]. Okey, O.D.; Maidin, S.S.; Lopes Rosa, R.; Toor, W.T.; Carrillo Melgarejo, D.; Wuttisittikulkij, L.; Saadi, M.; Zegarra Rodríguez, D.
Quantum Key Distribution Protocol Selector Based on Machine Learning for Next-Generation Networks. *Sustainability* **2022**, *14*,
15901.
https://doi.org/10.3390/su142315901.

[13]. Gatteschi, V.; Lamberti, F.; Demartini, C.; Pranteda, C.; Santamaría, V. Blockchain and smart contracts for insurance: Is the
technology mature enough? *Future Internet* **2018**, *10*, 20.

[14]. Jia, B.; Zhou, T.; Li, W.; Liu, Z.; Zhang, J. A blockchain-based location privacy protection incentive mechanism in crowd sensing
networks. *Sensors* **2018**, *18*, 3894.

[15]. Biswas K.; Muthukkumarasamy, V. Securing smart cities using blockchain technology. In Proceedings of the 2016 IEEE 18th
International Conference on High Performance Computing and Communications; IEEE 14th international conference on smart
city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS), Sydney, Australia, 12–14 December
2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1392–1393.

[16]. Fernández-Caramés, T.M.; Froiz-Míguez, I.; Blanco-Novoa, O.; .Fraga-Lamas, P. Enabling the internet of mobile crowdsourcing
health things: A mobile fog computing, blockchain and iot based continuous glucose monitoring system for diabetes mellitus
research and care. *Sensors* **2019**, *19*, 3319.

[17]. Ali, A.; Naveed, M.; Mehboob, M.; Irshad, H.; Anwar, P. An interference aware multi-channel mac protocol for wasn. In
Proceedings of the 2017 International Conference on Innovations in Electrical Engineering and Computational Technologies
(ICIEECT), Karachi, Pakistan, 5–7 April 2017; pp. 1–9.

[18]. Beebeejaun, A. Vat on foreign digital services in mauritius; a comparative study with south africa. *Int. J. Law Manag.* **2021**, *63*,
239–250.

[19]. Azis, A.; Shah, A.A. ; Piro, G.; Grieco, L.A.; Boggia, G. “A quantitative cross-comparison of container networking technologies for
virtualized service infrastructures in local computing environments. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4234.

[20]. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A decentralized privacy-preserving healthcare blockchain for

IoT. *Sensors* **2019**, *19*, 326.

[21]. Hang L.; Kim, D.-H. Design and implementation of an integrated iot blockchain platform for sensing data integrity. *Sensors* **2019**, *19*, 2228.

[22]. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for iot security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623.

[23]. Choo, C.W. *Information Management for the Intelligent Organization: The Art of Scanning the Environment*; Information Today, Inc.: Medford, NJ, USA, 2002.

[24]. Kermanshahi, S.K.; Liu, J.K.; Steinfeld, R. Multi-user cloud-based secure keyword search. In *Australasian Conference on Information Security and Privacy*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 227–247.

[25]. Kermanshahi, S.K.; Liu, J.K.; Steinfeld, R.; Nepal, S. Generic multi-keyword ranked search on encrypted cloud data. In *European Symposium on Research in Computer Security*; Springer: Berlin/Heidelberg, Germany, 2019, pp. 322–343.

[26]. Daraghmi, E.-Y.; Daraghmi, Y.-A.; Yuan, S.-M. Medchain: A design of blockchain-based system for medical records access and permissions management. *IEEE Access* **2019**, *7*, 164 595–164 613.

[27]. Jung, Y.; Peradilla, M.; Agulto, R. Packet key-based end-to-end security management on a blockchain control plane. *Sensors* **2019**, *19*, 2310.

[28]. Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.-K.R. Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Comput.* **2018**, *5*, 31–37.

[29]. Rathi, V.K.; Chaudhary, V.; Rajput, N.K.; Ahuja, B.; Jaiswal, A.K.; Gupta, D.; Elhoseny, M.; Hammoudeh, M. A blockchain-enabled multi domain edge computing orchestrator. *J. IEEE Internet Things Mag.* **2020**, *3*, 30–36.

[30]. Feng, C., Yu, K., Bashir, A.K., Al-Otaibi, Y.D., Lu, Y., Chen, S. and Zhang, D. Efficient and secure data sharing for 5G flying drones: a blockchain-enabled approach. *IEEE Netw.***2021**, *35*, 130–137.

[31]. Nkenyereye, L.; Adhi Tama, B.; Shahzad, M.K.; Choi, Y.H. Secure and blockchain-based emergency driven message protocol for 5G enabled vehicular edge computing. *Sensors* **2020**, *20*, 154.

[32]. Khujamatov, K.; Reypnazarov, E.; Akhmedov, N.; ;Khasanov, D. 2020, November. Blockchain for 5G Healthcare architecture. In Proceedings of the 2020 International Conference on Information Science and Communications Technologies (ICISCT), Karachi, Pakistan, 8–9 February 2020; pp. 1–5.

[33]. Vivekanandan, M.; VN, S.; U, S.R. BIDAPSCA5G: Blockchain based Internet of Things (IoT) device to device authentication protocol for smart city applications using 5G technology. In *Peer-to-Peer Networking and Applications*; Springer: Berlin/Heidelberg, Germany, 2021; Volume 14, pp.403–419.

[34]. Gao, J.; Agyekum, K.O.B.O.; Sifah, E.B.; Acheampong, K.N.; Xia, Q.; Du, X.; Guizani, M.; Xia, H. A blockchain-SDN-enabled Internet of vehicles environment for fog computing and 5G networks. *IEEE Internet Things J.* **2019**, *7*, 4278–4291.

[35]. Zhou, S.; Huang, H.; Chen, W.; Zhou, P.; Zheng, Z.; Guo, S. Pirate: A blockchain-based secure framework of distributed machine learning in 5g networks. *IEEE Netw.* **2020**, *34*, 84–91.

[36]. Zhang, Y.; Wang, K.; Moustafa, H.; Wang, S.; Zhang, K. Guest Editorial: Blockchain and AI for Beyond 5G Networks. *IEEE Netw.* **2020**, *34*, 22–23.

[37]. Zhao, Y.; Zhao, J.; Zhai, W.; Sun, S.;

Niyato, D; Lam, K.Y. A survey of 6G wireless communications: Emerging technologies. In *Future of Information and Communication Conference*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 150–170.

[38]. Bhattacharya, P.; Tanwar, S.; Shah, R.; Ladha, A. Mobile edge computing-enabled blockchain framework—A survey. In *Proceedings of ICRIC 2019*; Springer: Berlin/Heidelberg, Germany, 2020; pp.797–809.

[39]. Kaushik, S. Blockchain and 5G-Enabled Internet of Things: Background and Preliminaries. In *Blockchain for 5G-Enabled IoT*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 3–31.

[40]. Mistry, I.; Tanwar, S.; Tyagi, S.; Kumar, N. Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. In *Mechanical Systems and Signal Processing*; Elsevier: Amsterdam, The Netherlands, 2020; Volume 135, p. 106382.

[41]. Budhiraja, I.; Tyagi, S.; Tanwar, S.; Kumar, N.;Guizani, M. CR-NOMA Based Interference Mitigation Scheme for 5G Femtocells Users. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab, 9–13 December 2018; IEEE: Piscataway, NJ, USA, 2018; Volume 1, pp. 1–6. https://doi.org/10.1109/GLOCOM.2018.8647354.

[42]. Krichen, M.; Lahami, M.; Al–Haija, Q.A. Formal Methods for the Verification of Smart Contracts: A Review. In Proceedings of the 15th International Conference on Security of Information and Networks (SIN), Sousse, Tunisia, 11–13 November 2022. https://doi.org/10.1109/SIN56466.2022.9970534.

[43]. Tesnim, A.; Kei-Leo, B.. Formal Methods for the Verification of Smart Contracts: A Review. In Proceedings of the 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS); Paris, France, 26–28 February 2018; pp. 1–5. https://doi.org/10.1109/NTMS.2018.8328737

[44]. Ali, A.; Almaiah, M.A.; Hajjej, F.; Pasha, M.F.; Fang, O.H.; Khan, R.; Teo, J.; Zakarya, M. An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network. *Sensors* **2022**, *22*, 572.

[45]. Ali, A.; Kundi, M.; Ahmed, M.; ur Rehman, A.; Ali, H.; Misron, A.B. A Novel Privacy-Preserving Framework Based on Blockchain Technology to Secure Industrial IoT Data. In *Security, Trust and Privacy Models, and Architectures in IoT Environments*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 25–42.

[46]. Ali, A.; Pasha, M.F.; Guerrieri, A.; Guzzo, A.; Sun, X.; Saeed, A.; Hussain, A.; Fortino, G. A Novel Homomorphic Encryption and Consortium Blockchain-based Hybrid Deep Learning Model for Industrial Internet of Medical Things. *IEEE Trans. Netw. Sci. Eng.* **2023**, 1–18. https://doi.org/10.1109/TNSE.2023.3285070,2023

[47]. Almaiah, M.A.; Hajjej, F.; Ali, A.; Pasha, M.F.; Almomani, O. A Novel Hybrid Trustworthy Decentralized Authentication and Data Preservation Model for Digital Healthcare. *Sensors* **2022**, *22*, 1424-8220.

[48]. Almaiah MA, Al-Rahmi AM, Alturise F, Alrawad M, Alkhalaf S, Lutfi A, Al-Rahmi WM, Awad AB. Factors influencing the adoption of internet banking: An integration of ISSM and UTAUT with price value and perceived risk. Frontiers in Psychology. 2022 Sep 1;13:919198.

[49]. Al Nafea R, Almaiah MA. Cyber security threats in cloud: Literature review. In2021 international conference on information technology (ICIT) 2021 Jul 14 (pp. 779-786). IEEE.

[50]. Almaiah MA, Al-Khasawneh A. Investigating the main determinants of mobile cloud computing adoption in

university campus. Education and Information Technologies. 2020 Jul;25(4):3087-107.
[51]. Almaiah MA, Al-Rahmi A, Alturise F, Hassan L, Lutfi A, Alrawad M, Alkhalaf S, Al-Rahmi WM, Al-sharaieh S, Aldhyani TH. Investigating the effect of perceived security, perceived trust, and information quality on mobile payment usage through near-field communication (NFC) in Saudi Arabia. Electronics. 2022 Nov 28;11(23):3926.
[52]. Almaiah MA, Dawahdeh Z, Almomani O, Alsaaidah A, Al-Khasawneh A, Khawatreh S. A new hybrid text encryption approach over mobile ad hoc network. Int. J. Electr. Comput. Eng.(IJECE). 2020 Dec;10(6):6461-71.
[53]. Almaiah MA, Al-Otaibi S, Shishakly R, Hassan L, Lutfi A, Alrawad M, Qatawneh M, Alghanam OA. Investigating the role of perceived risk, perceived security and perceived trust on smart m-banking application using SEM. Sustainability. 2023 Jun 21;15(13):9908.
[54]. Almaiah MA, Hajjej F, Ali A, Pasha MF, Almomani O. A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS. Sensors. 2022 Feb 13;22(4):1448.
[55]. Almaiah MA, Ali A, Hajjej F, Pasha MF, Alohali MA. A lightweight hybrid deep learning privacy preserving model for FC-based industrial internet of medical things. Sensors. 2022 Mar 9;22(6):2112.
[56]. Adil M, Almaiah MA, Omar Alsayed A, Almomani O. An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks. Sensors. 2020 Apr 18;20(8):2311.
[57]. Al Hwaitat AK, Almaiah MA, Ali A, Al-Otaibi S, Shishakly R, Lutfi A, Alrawad M. A new blockchain-based authentication framework for secure IoT networks. Electronics. 2023 Aug 27;12(17):3618.
[58]. Siam AI, Almaiah MA, Al-Zahrani A, Elazm AA, El Banby GM, El-Shafai W, El-Samie FE, El-Bahnasawy NA. Secure health monitoring communication systems based on IoT and cloud computing for medical emergency applications. Computational Intelligence and Neuroscience. 2021;2021(1):8016525.
[59]. Altulaihan E, Almaiah MA, Aljughaiman A. Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms. Sensors. 2024 Jan 22;24(2):713.
[60]. Almaiah MA, Yelisetti S, Arya L, Babu Christopher NK, Kaliappan K, Vellaisamy P, Hajjej F, Alkdour T. A Novel Approach for Improving the Security of IoT–Medical Data Systems Using an Enhanced Dynamic Bayesian Network. Electronics. 2023 Oct 18;12(20):4316.
[61]. Alrawad M, Lutfi A, Almaiah MA, Elshaer IA. Examining the influence of trust and perceived risk on customers intention to use NFC mobile payment system. Journal of Open Innovation: Technology, Market, and Complexity. 2023 Jun 1;9(2):100070.
[62]. Almomani O, Almaiah MA, Alsaaidah A, Smadi S, Mohammad AH, Althunibat A. Machine learning classifiers for network intrusion detection system: comparative study. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 440-445). IEEE.
[63]. Altulaihan E, Almaiah MA, Aljughaiman A. Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions. Electronics. 2022 Oct 16;11(20):3330.
[64]. Adil M, Khan R, Ali J, Roh BH, Ta QT, Almaiah MA. An energy proficient load balancing routing scheme for wireless sensor networks to maximize their lifespan in an operational environment. Ieee Access. 2020 Aug 31;8:163209-24.
[65]. Almaiah MA, Al-Zahrani A, Almomani O, Alhwaitat AK. Classification of cyber security threats on mobile devices and applications. InArtificial intelligence and blockchain for future cybersecurity applications 2021 May 1 (pp. 107-123). Cham: Springer International Publishing.
[66]. Alamer M, Almaiah MA. Cybersecurity in Smart City: A systematic mapping study. In2021 international conference on information technology (ICIT) 2021 Jul 14 (pp. 719-724). IEEE.
[67]. Khan MN, Rahman HU, Almaiah MA, Khan MZ, Khan A, Raza M, Al-Zahrani M, Almomani O, Khan R. Improving energy efficiency with content-based adaptive and dynamic scheduling in

wireless sensor networks. Ieee Access. 2020 Sep 25;8:176495-520.
[68]. ALMAIAH MA, ALI A, SHISHAKLY R, ALKHDOUR T, LUTFI A, ALRAWAD M. Building Trust In Iot: Leveraging Consortium Blockchain For Secure Communications. Journal Of Theoretical And Applied Information Technology. 2024 Feb 15;102(3).
[69]. Bubukayr MA, Almaiah MA. Cybersecurity concerns in smart-phones and applications: A survey. In2021 international conference on information technology (ICIT) 2021 Jul 14 (pp. 725-731). IEEE.
[70]. AlSalem TS, Almaiah MA, Lutfi A. Cybersecurity Risk Analysis in the IoT: A Systematic Review. Electronics. 2023 Sep 20;12(18):3958.
[71]. Adil M, Khan R, Almaiah MA, Binsawad M, Ali J, Al Saaidah A, Ta QT. An efficient load balancing scheme of energy gauge nodes to maximize the lifespan of constraint oriented networks. IEEE Access. 2020 Aug 11;8:148510-27.
[72]. Almaiah M, Alrawashdeh R, Alkhdour T, Al-Ali R, Rjoub G, Aldahyani T. Detecting DDoS attacks using machine learning algorithms and feature selection methods. International Journal of Data and Network Science. 2024;8(4):2307-18.
[73]. Albalawi AM, Almaiah MA. Assessing and reviewing of cyber-security threats, attacks, mitigation techniques in IoT environment. J. Theor. Appl. Inf. Technol. 2022 May 15;100:2988-3011.
[74]. Adil M, Khan R, Almaiah MA, Al-Zahrani M, Zakarya M, Amjad MS, Ahmed R. MAC-AODV based mutual authentication scheme for constraint oriented networks. Ieee Access. 2020 Mar 4;8:44459-69.
[75]. Vijayalakshmi K, Al-Otaibi S, Arya L, Almaiah MA, Anithaashri TP, Karthik SS, Shishakly R. Smart Agricultural–Industrial Crop-Monitoring System Using Unmanned Aerial Vehicle–Internet of Things Classification Techniques. Sustainability. 2023 Jul 19;15(14):11242.
[76]. Aldhyani TH, Khan MA, Almaiah MA, Alnazzawi N, Hwaitat AK, Elhag A, Shehab RT, Alshebami AS. A secure internet of medical things framework for breast cancer detection in sustainable smart cities. Electronics. 2023 Feb 8;12(4):858.
[77]. Almaiah MA, Alkdour T. Securing Fog Computing Through Consortium Blockchain Integration: The Proof of Enhanced Concept (PoEC) Approach. InRecent Advancements in Multimedia Data Processing and Security: Issues, Challenges, and Techniques 2023 (pp. 107-140). IGI Global.
[78]. Almaiah M, Ali A, Alkhdour T, Tin T, AlAli R, Aldahyani T. Streamlining supply chains: An efficiency-driven permissioned blockchain framework for data reduction. International Journal of Data and Network Science. 2024;8(4):2445-58.
[79]. ALMAIAH MA, ALI A, SHISHAKLY R, ALKHDOUR T, LUTFI A, ALRAWAD M. A Novel Federated-Learning Based Adversarial Framework For Audio-Visual Speech Enhancement. Journal Of Theoretical And Applied Information Technology. 2024 Feb 29;102(4).
[80]. Almudaires F, Almaiah M. Data an overview of cybersecurity threats on credit card companies and credit card risk mitigation. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 732-738). IEEE.
[81]. Qasem MH, Obeid N, Hudaib A, Almaiah MA, Al-Zahrani A, Al-Khasawneh A. Multi-agent system combined with distributed data mining for mutual collaboration classification. IEEE Access. 2021 Apr 20;9:70531-47.
[82]. AlMedires M, AlMaiah M. Cybersecurity in industrial control system (ICS). In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 640-647). IEEE.
[83]. Ali A, Pasha MF, Fang OH, Khan R, Almaiah MA, K. Al Hwaitat A. Big data based smart blockchain for information retrieval in privacy-preserving healthcare system. InBig Data Intelligence for Smart Applications 2022 Jan 18 (pp. 279-296). Cham: Springer International Publishing.
[84]. Almaiah MA. An Efficient Smart Weighted and Neighborhood-enabled Load Balancing Scheme for Constraint Oriented Networks. International Journal of Advanced Computer Science and Applications. 2020;11(12).
[85]. Alrawad M, Lutfi A, Almaiah MA, Alsyouf A, Arafa HM, Soliman Y,

Elshaer IA. A novel framework of public risk assessment using an integrated approach based on AHP and psychometric paradigm. Sustainability. 2023 Jun 22;15(13):9965.

[86]. Alkdour T, Almaiah MA, Shishakly R, Lutfi A, Alrawad M. Exploring the Success Factors of Smart City Adoption via Structural Equation Modeling. Sustainability. 2023 Nov 14;15(22):15915.

[87]. Al-Janabi HD, Lashari SA, Khalil A, Al-Shareeda MA, Alsadhan AA, Almaiah MA, Alkhdour T. D-BlockAuth: An Authentication Scheme Based Dual Blockchain for 5G-Assisted Vehicular Fog Computing. IEEE Access. 2024 Jul 15.

[88]. Alkhdour TA, Almaiah MA, Ali AI, Lutfi AB, Alrawad MA, Tin TT. Revolutionizing Healthcare: Unleashing Blockchain Brilliance Through Fuzzy Logic Authentication. Journal Of Theoretical And Applied Information Technology. 2024 Feb 29;102(4).

[89]. Hammoudeh YA, Qatawneh M, AbuAlghanam O, Almaiah MA. Digital Certificate Validation Using Blockchain: A Survey. In2023 International Conference on Information Technology (ICIT) 2023 Aug 9 (pp. 506-510). IEEE.

[90]. Mohamed MA, Shawai YG, Almaiah MA, Derahman MN, Lutfi A, Bakar KA. Challenges in data representation for efficient execution of encryption operation. Bulletin of Electrical Engineering and Informatics. 2024 Apr 1;13(2):1207-16.

[91]. Almomani O, Almaiah MA, Madi M, Alsaaidah A, Almomani MA, Smadi S. Reconnaissance attack detection via boosting machine learning classifiers. InAIP Conference Proceedings 2023 Oct 20 (Vol. 2979, No. 1). AIP Publishing.

[92]. Ado A, Bichi A, Haruna U, Almaiah M, Shawai Y, AlAli R, Alkhdour T, Aldhyani T, Al-rawad M, Shehab R. An improved multi-stage framework for large-scale hierarchical text classification problems using a modified feature hashing and bi-filtering strategy. International Journal of Data and Network Science. 2024;8(4):2193-204.

[93]. Ahmad W, Almaiah MA, Ali A, Al-Shareeda MA. Deep Learning Based Network intrusion detection for unmanned aerial vehicle (UAV). In2024 7th World Conference on Computing and Communication Technologies (WCCCT) 2024 Apr 12 (pp. 31-36). IEEE.

[94]. Al-Na'amneh Q, Nasayreh AN, Al Mamlook R, Gharaibeh H, Alsheyab AM, Almaiah M. Improving Memory Malware Detection in Machine Learning With Random Forest-Based Feature Selection. InRisk Assessment and Countermeasures for Cybersecurity 2024 (pp. 96-114). IGI Global.