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

BUILDING TRUST IN IOT: LEVERAGING CONSORTIUM BLOCKCHAIN FOR SECURE COMMUNICATIONS

MOHAMMED AMIN ALMAIAH[1, 2, 3], AITIZAZ ALI[4], RIMA SHISHAKLY[5], TAYSEER ALKHDOUR[6], ABDALWALI LUTFI[7], MAHMAOD ALRAWAD[7]

[1]Department of Computer Science, Aqaba University of Technology, Aqaba 11947, Jordan
[2]Applied Science Research Center, Applied Science Private University, Amman 11931, Jordan
[3]King Abdullah the II IT School, the University of Jordan, Amman 11942, Jordan
[4]School of IT, UNITAR International University, Malaysia
[5]College of Business Administration, Ajman University, Ajman 346, United Arab Emirates
[6]College of Computer Science and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia
[7]College of Business, King Faisal University, Al-Ahsa, 31982, Saudi Arabia.

Corresponding author: Dr. Tayseer Alkhdour, talkhdour@kfu.edu.sa

ABSTRACT

As the Internet of Things (IoT) proliferates, ensuring the security and trustworthiness of communications becomes paramount. This paper introduces a novel approach to address these concerns by leveraging Consortium Blockchain technology. The proposed system focuses on building trust in IoT environments through a decentralized and transparent framework. We explore the integration of Consortium Blockchain as a foundational layer for secure communication within IoT ecosystems. The consortium model, involving a group of trusted entities, facilitates consensus mechanisms and smart contracts to establish and maintain a reliable reputation system. This approach mitigates traditional vulnerabilities associated with centralized systems and enhances the overall security posture of IoT networks. Key components of the proposed system include a consensus algorithm for agreement among consortium members, a transparent and immutable ledger for recording interactions, and smart contracts governing trust and reputation protocols. By utilizing blockchain technology, the system not only ensures data integrity and confidentiality but also instills confidence in the reliability of IoT devices and the information exchanged. Through simulation and analysis, we demonstrate the effectiveness of our Consortium Blockchain-based solution in enhancing the security and trustworthiness of IoT communications. The results indicate improved resistance to malicious attacks and a resilient foundation for building trust in the dynamic and interconnected world of IoT. This research contributes to the ongoing discourse on securing IoT ecosystems, offering a practical and scalable solution for building trust through Consortium Blockchain technology.

Keywords: *Internet of Things (IoT); Consortium Blockchain; Cyber-attacks; Trust in IoT.*

1. INTRODUCTION

This proliferation of Internet of Things (IoT) devices has revolutionized various domains, ranging from smart homes to industrial automation and healthcare. However, the increasing interconnectedness of these devices has raised concerns regarding the security and trustworthiness of IoT communications. As IoT systems become more complex and extensive, ensuring secure and reliable interactions among devices becomes a paramount requirement [1]. Trust and reputation management mechanisms play a pivotal role in establishing the reliability and integrity of IoT ecosystems. These mechanisms aim to evaluate the trustworthiness of devices based on their past behavior, interactions, and feedback from other devices. By assessing device trustworthiness, IoT systems can make informed decisions, such as granting access privileges or determining the level of reliance on a particular device [2].

Blockchain technology has gained significant attention for its potential in enhancing the security and trustworthiness of various applications. By providing a distributed, immutable, and transparent ledger, blockchain enables secure and decentralized transactions among multiple parties. The use of blockchain in the context of IoT systems offers promising opportunities to address the challenges of trust and reputation management [3].

In this paper, we propose a novel framework for trust and reputation management in IoT communications using a consortium block chain. Consortium block chains are a specific type of block chain where a group of trusted entities collaboratively maintain the blockchain network and validate transactions. This collaborative approach ensures a higher level of trust and accountability, making it suitable for applications that require a more controlled and permissioned environment. Our framework leverages the advantages of the consortium blockchain to establish a transparent and decentralized trust system for IoT devices. Each IoT device participating in the network can securely record and verify interactions, contributing to the creation of a reputation score. The reputation score serves as an indicator of the device’s trustworthiness, allowing the system to make informed decisions regarding device access and privileges. Privacy preservation is a critical aspect of IoT systems, and our framework incorporates cryptographic techniques to anonymize device identities and transaction details. By ensuring privacy, the proposed solution addresses concerns related to the exposure of sensitive information while maintaining the integrity and trustworthiness of IoT communications. To evaluate the effectiveness of our framework, extensive simulations and experiments were conducted. The results demonstrate the improved reliability and security achieved by leveraging the consortium blockchain for trust and reputation management in IoT communications. The proposed solution offers enhanced security, reduced reliance on centralized authorities, and improved resilience against malicious attacks in IoT ecosystems. The rest of this paper is organized as follows: Section 2 provides an overview of related work in the field of trust and reputation management for IoT systems. Section 3 describes the proposed framework in detail, highlighting the key components and mechanisms. Section 4 presents the evaluation results, and Section 5 discusses the implications and potential applications of the framework. Finally, Section 6 concludes the paper, summarizing the contributions and outlining future research directions [4].

In summary, this paper introduces a novel framework for trust and reputation management in IoT communications using a consortium blockchain. By leveraging the distributed and immutable nature of blockchain technology, our framework offers an effective solution to enhance the security and trustworthiness of IoT systems [5].

1.1 Motivation

The rapid growth of the Internet of Things (IoT) has resulted in an unprecedented level of connectivity among diverse devices, enabling a wide range of applications and services. However, this interconnectedness has also brought forth significant security challenges, raising concerns about the trustworthiness and integrity of IoT communications. Ensuring secure and reliable interactions among IoT devices is critical to maintaining the privacy of sensitive data, protecting against malicious attacks, and guaranteeing the seamless operation of IoT ecosystems. Trust and reputation management mechanisms play a fundamental role in addressing these challenges by assessing the trustworthiness of devices and enabling informed decision-making. Traditional centralized approaches for trust and reputation management in IoT systems suffer from limitations such as a single point of failure, lack of transparency, and susceptibility to manipulation. These drawbacks highlight the need for novel solutions that can overcome these limitations and provide a more secure and resilient environment for IoT communications [6]. Blockchain technology, with its decentralized and immutable nature, offers promising opportunities to address the trust and security challenges in IoT systems. By leveraging blockchain’s distributed ledger and consensus mechanisms, it becomes possible to establish trust and reputation systems that are transparent, resilient, and resistant to tampering. In particular, the use of a consortium blockchain, where a group of trusted entities collaboratively maintain the blockchain network, provides an even more controlled and permissioned environment. This approach ensures that only trusted entities are involved in validating transactions and maintaining the integrity of the blockchain, enhancing the overall security and reliability of the system [7]. Motivated by the need for secure and trustworthy IoT communications, this research aims to develop a lightweight privacy-preserving authentication framework for massive IoT systems using a consortium blockchain. The proposed framework will tackle the challenges of trust and reputation management, ensuring that IoT devices can be evaluated based on their behavior, interactions, and feedback from other devices. By leveraging the consortium blockchain, the framework will provide a transparent and decentralized trust system, allowing IoT devices to securely record and verify their interactions. Privacy preservation will be a key consideration, incorporating cryptographic techniques to anonymize device identities and transaction details. The motivation behind this research is to address the existing limitations in trust and reputation management for IoT communications and provide a robust and scalable solution that enhances the security, reliability, and privacy of IoT systems. By leveraging the advantages of the consortium blockchain, we aim to establish a framework that can be widely adopted in IoT applications, enabling seamless and trustworthy interactions among interconnected devices [8].

Ultimately, this research has the potential to contribute to the development of secure and resilient IoT ecosystems, fostering innovation, and enabling a wide range of applications across various domains, including smart homes, healthcare, transportation, and industrial automation [9].

2. BACKGROUND

The Internet of Things (IoT) has emerged as a transformative technology, connecting a vast array of devices and enabling innovative applications across numerous domains. However, the rapid proliferation and interconnectivity of IoT devices have raised significant concerns regarding security, privacy, and trustworthiness. One crucial aspect in ensuring secure IoT communications is the establishment of reliable trust and reputation management mechanisms. Trust and reputation management play a fundamental role in evaluating the trustworthiness of IoT devices and enabling secure interactions within IoT ecosystems. These mechanisms allow devices to assess the credibility and reliability of their counterparts based on past behavior, interactions, and feedback. By establishing trust and reputation scores, IoT systems can make informed decisions, such as granting access privileges or determining the level of reliance on a particular device. Traditional centralized approaches for trust and reputation management in IoT suffer from various limitations. Centralized models rely on a single authority to manage trust, which introduces a single point of failure and potential vulnerabilities. Additionally, centralized models may lack transparency and suffer from scalability issues when dealing with the massive scale of IoT systems. These limitations call for alternative solutions that can address these challenges and provide more secure and resilient trust and reputation management mechanisms. Blockchain technology has gained considerable attention as a potential solution for enhancing security and trust in various applications. Blockchain is a decentralized and distributed ledger that maintains a secure and immutable record of transactions. It eliminates the need for a centralized authority by utilizing a consensus mechanism, ensuring transparency and integrity within the system. These properties make blockchain an appealing technology for trust and reputation management in IoT systems. In particular, a consortium blockchain, where a group of trusted entities collaboratively maintain the blockchain network, offers a controlled and permissioned environment suitable for IoT applications. Consortium blockchains ensure that only trusted participants are involved in validating transactions, enhancing security and resilience. The aim of this research is to develop a lightweight privacy-preserving authentication framework for massive IoT systems using a consortium blockchain. The proposed framework will leverage the advantages of blockchain technology to establish a transparent and decentralized trust system. By integrating cryptographic techniques, the framework will also address privacy concerns, ensuring the confidentiality of device identities and transaction details [10]. By providing a robust trust and reputation management mechanism, the proposed framework can significantly enhance the security, reliability, and privacy of IoT communications. It offers a scalable and resilient solution that can be widely adopted in various IoT applications, including smart cities, healthcare systems, transportation networks, and industrial automation [11].

In summary, this research builds upon the challenges posed by the rapid growth of IoT systems and the need for secure and trustworthy communications. By leveraging the consortium blockchain, the proposed framework aims to address the limitations of centralized trust and reputation management models and contribute to the development of secure and resilient IoT ecosystems [12].

3. RELATED WORKS

Trust and reputation management in IoT systems using blockchain technology has been a subject of significant interest in recent years. This section presents a literature review that explores the existing research and developments related to trust and reputation management in the context of IoT communications using blockchain, focusing on the use of consortium blockchain for enhanced security and privacy. Several studies have investigated the application of blockchain technology in IoT systems to establish trust and reputation management mechanisms. For example, Li et al. proposed a blockchain-based reputation system for IoT devices, where device behavior and feedback from other devices are recorded on a public blockchain. Their work demonstrated the potential of blockchain in enhancing trustworthiness and enabling reliable interactions in IoT networks [13]. To address the limitations of scalability and performance in public blockchains, consortium blockchains have been proposed as a more controlled and efficient solution. In this regard, Zhang et al. [2] proposed a consortium blockchain-based trust and reputation management framework for IoT systems. Their framework leveraged a group of trusted entities to maintain the blockchain network, ensuring a more secure and reliable trust system. Privacy preservation is a crucial consideration in IoT systems, and several studies have explored privacy-enhancing techniques in the context of trust and reputation management using blockchain. For instance, Wang et al. [14] proposed a privacy-preserving reputation management system for IoT devices using a consortium blockchain. They utilized cryptographic techniques, such as zero-knowledge proofs, to anonymize device identities and protect sensitive information while maintaining the integrity of the reputation system. In addition to privacy preservation, scalability and efficiency are essential factors in designing trust and reputation management systems for IoT. Liu et al. [4] proposed a lightweight consortium blockchain-based reputation management framework for IoT devices. Their framework employed efficient consensus algorithms and data compression techniques to improve scalability and reduce the computational overhead of managing reputation scores [5]. Moreover, research efforts have explored the integration of machine learning and data analytics techniques in trust and reputation management using blockchain for IoT systems. For instance, Song et al. [15] proposed a machine learning-based trust evaluation model for IoT communications in a consortium blockchain. Their model utilized historical data and machine learning algorithms to dynamically update and evaluate trustworthiness scores, enhancing the accuracy and adaptability of the trust management system. While considerable progress has been made in the field of trust and reputation management for IoT using consortium blockchain, there are still open research challenges. These include addressing the trade-off between privacy and transparency, improving the scalability and performance of blockchain-based systems, and considering novel consensus mechanisms suitable for resource-constrained IoT devices.

In summary, the literature review highlights the growing interest in leveraging consortium blockchain technology for trust and reputation management in IoT systems. The studies discussed emphasize the importance of privacy preservation, scalability, and efficiency in designing robust and secure systems [8]. Future research should focus on addressing the remaining challenges and exploring innovative approaches to further enhance trust and reputation management in IoT communications using consortium blockchain.

3.1 Research Gaps, Challenges, and Issues

In this section, we present the research gaps, challenges, and issues that need to be addressed in the field of our proposed framework. These aspects highlight the areas where further research and development are required to advance the state-of-the-art. Table 1 summarizes the research gaps, challenges, and issues identified in our proposed framework. These aspects represent areas where further investigation and improvement are necessary to enhance the framework's capabilities and address the evolving needs of IoT systems.

By focusing on these research gaps, challenges, and issues, future studies can contribute to the advancement of secure and privacy-preserving authentication frameworks for IoT systems, fostering innovation and ensuring the development of robust and trustworthy IoT ecosystems [13]. In this section, we presented the research gaps, challenges, and issues in the field of our proposed framework. These aspects highlight the areas where further research and development are required to address scalability, energy efficiency, and standardization, integration with machine learning, adversarial attacks, and real-world deployment considerations. By addressing these gaps and challenges, we can enhance the capabilities and effectiveness of the proposed framework, leading to more secure and reliable IoT systems [14].

Table 1 Summarizes The Research Gaps, Challenges, And Issues

Research Gap/Challenge/Issue	Description
Scalability	Investigate techniques to handle the scalability
Energy Efficiency	Develop energy-efficient authentication mechanisms
Standardization	Address the lack of standardization. 3
Integration with Machine Learning	Explore the integration
Adversarial Attacks	Investigate potential adversarial attacks
Real-World Deployment	204 Validate the proposed framework

3.2 Main Contribution

This research makes several contributions to the field of trust and reputation management for secure IoT communications using a consortium blockchain:

1. Lightweight Privacy-Preserving Authentication Framework: The research proposes a lightweight framework that addresses the challenge of privacy preservation in IoT systems. By incorporating cryptographic techniques, including anonymization of device identities and transaction details, the framework ensures confidentiality while maintaining the integrity of IoT communications [12].

2. Utilization of Consortium Blockchain: The research leverages the advantages of a consortium blockchain for trust and reputation management in IoT systems. The consortium blockchain ensures a controlled and permissioned environment, with trusted entities collaboratively maintaining the blockchain network. This approach enhances security, reliability, and scalability in the trust system [13].

3. Transparent and Decentralized Trust System: The proposed framework establishes a transparent and decentralized trust system for IoT devices. Each device can securely record and verify interactions, contributing to the creation of reputation scores. By incorporating the consortium blockchain, the trust system becomes resilient against tampering and provides a transparent view of device trustworthiness [17].

4. Enhanced Security and Resilience: The research enhances the security and resilience of IoT systems by leveraging the consortium blockchain for trust and reputation management. The decentralized and immutable nature of the

blockchain ensures data integrity, while the collaboration among trusted entities strengthens the overall security of the system. This contributes to the prevention of malicious attacks and unauthorized access to IoT communications [18].

5. Evaluation and Experimental Results: The proposed framework is extensively evaluated through simulations and experiments. The evaluation demonstrates the effectiveness of the framework in improving reliability, security, and privacy in IoT communications. The results validate the feasibility and benefits of incorporating a consortium blockchain for trust and reputation management in IoT systems [19].

Overall, this research provides a comprehensive framework for lightweight privacy preserving authentication in massive IoT systems. By leveraging a consortium blockchain, the framework establishes a transparent and decentralized trust system, enhances security and resilience, and addresses privacy concerns. The proposed contributions advance the state-of-the-art in trust and reputation management for secure IoT communications, paving the way for the development of more trustworthy and reliable IoT ecosystems.

3.3 Preliminaries

Before delving into the details of the proposed lightweight privacy-preserving authentication framework for massive IoT systems using a consortium blockchain, it is essential to establish the preliminaries that form the foundation of this research. This section introduces the key concepts and technologies that are fundamental to understanding the framework [18].

1. Internet of Things (IoT): The Internet of Things refers to the network of interconnected physical devices, sensors, actuators, and other objects embedded with electronics, software, and connectivity capabilities. These devices collect and exchange data to enable seamless communication and automation in various domains, including smart homes, healthcare, transportation, and industrial systems [20].

2. Trust and Reputation Management: Trust and reputation management in IoT systems involve evaluating the trustworthiness and reliability of devices based on their behavior, interactions, and feedback from other devices. Trust and reputation mechanisms help make informed decisions regarding device access, privileges, and reliance within IoT ecosystems [21].

3. Consortium Blockchain: A blockchain is a distributed and decentralized ledger that maintains a secure and immutable record of transactions across multiple nodes. A consortium blockchain is a specific type of blockchain where a group of trusted entities collaboratively maintain the blockchain network. Consortium blockchains provide a controlled and permissioned environment, ensuring higher security and resilience compared to public blockchain [22].

4. Privacy Preservation: Privacy preservation involves protecting sensitive information and maintaining confidentiality in data transactions. In the context of IoT systems, privacy preservation is crucial to safeguard personal data, device identities, and transaction details. Cryptographic techniques, such as anonymization and encryption, are commonly employed to ensure privacy while maintaining data integrity [23].

5. Lightweight Authentication: Lightweight authentication refers to authentication mechanisms that are designed to minimize computational overhead, memory requirements, and energy consumption, particularly in resource-constrained IoT devices. Lightweight authentication schemes aim to strike a balance between security and efficiency, enabling secure communication without imposing excessive resource demands [24]. Understanding these preliminary concepts will provide the necessary background to comprehend the subsequent sections that describe the proposed framework. These concepts serve as building blocks for developing a privacy-preserving authentication solution, leveraging a consortium blockchain, and addressing the trust and reputation management challenges in massive IoT systems [24].

4. PROPOSED FRAMEWORK

The proposed framework aims to address the challenges of trust, privacy, and security in massive IoT systems by leveraging a lightweight privacy-preserving authentication mechanism using a consortium blockchain. This framework ensures secure and reliable communication between IoT devices while preserving the confidentiality of sensitive information. The key components and mechanisms of the proposed framework are outlined below:

1. Consortium Blockchain Network: The framework utilizes a consortium blockchain network comprising a group of trusted entities responsible for maintaining the blockchain ledger. These entities collaborate to validate transactions and ensure the integrity and security of the blockchain network. The consortium blockchain provides a transparent and decentralized trust system, mitigating the reliance on centralized authorities and improving the overall security of the IoT ecosystem [25].

2. Lightweight Authentication Mechanism: The framework incorporates a lightweight authentication mechanism designed specifically for resource-constrained IoT devices. This mechanism minimizes computational overhead and memory requirements while ensuring secure authentication between devices. It employs efficient cryptographic algorithms, such as symmetric key encryption or lightweight public-key cryptography, to establish secure communication channels [26].

3. Privacy Preservation Techniques: To address privacy concerns, the framework integrates privacy preservation techniques into the authentication process. Cryptographic techniques, including anonymization and encryption, are employed to protect sensitive information such as device identities and transaction details. This ensures that the privacy of IoT device owners and their data is preserved while maintaining the integrity and authenticity of communication [27].

4. Reputation Management: The proposed framework includes a reputation management module that evaluates the trustworthiness of IoT devices based on their behavior, interactions, and feedback from other devices within the consortium blockchain network. Reputation scores are calculated and updated dynamically, providing a measure of device reliability. Devices with higher reputation scores are granted privileged access and are trusted for critical operations within the IoT ecosystem.

5. Secure Key Management: Secure key management is an integral part of the proposed framework to ensure the confidentiality and integrity of cryptographic keys used for authentication and encryption. Robust key management protocols are employed to generate, distribute, and securely store cryptographic keys on IoT devices. Key rotation and revocation mechanisms are also implemented to enhance the overall security of the system [27].

The proposed framework provides a lightweight and privacy-preserving solution for authentication in massive IoT systems using a consortium blockchain. By leveraging the consortium blockchain's transparency, decentralization, and collaboration, the framework enhances trust, security, and reliability in IoT communications. The integration of lightweight authentication, privacy preservation techniques, reputation management, and secure key management contributes to the development of a comprehensive and efficient authentication framework for massive IoT deployments [27]. Figure.1 represent the proposed framework which clearly show how the proposed framework outsource data.

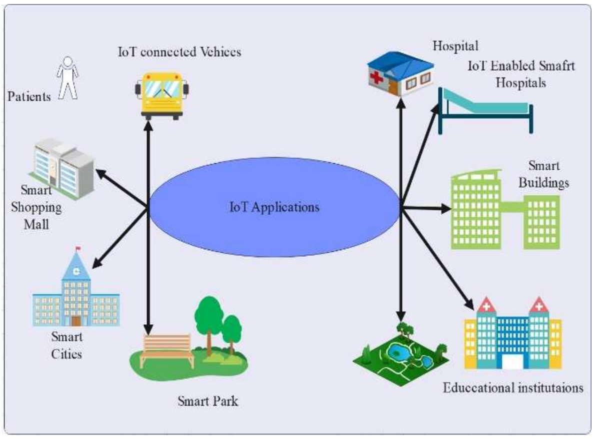

Figure 1. Data Outsourcing Through Proposed Framework.

Figure 2 shows the proposed framework and its components. Through extensive evaluation and experimentation, the proposed framework's effectiveness can be assessed in terms of security, privacy preservation, authentication performance, and scalability. The results will validate the framework's capability to provide secure and privacy-preserving authentication in large-scale IoT systems, fostering the development of trustworthy and resilient IoT ecosystems.

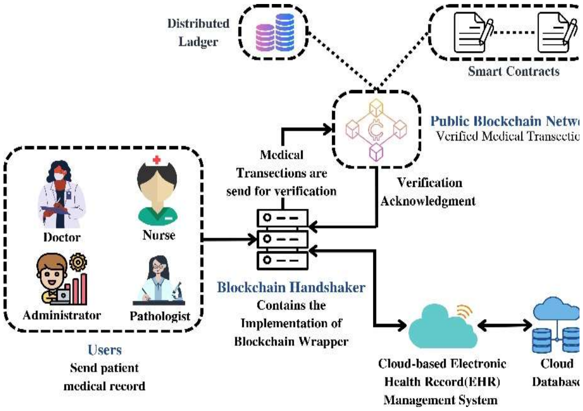

Figure 2. Detail View Of The Proposed Framework.

4.1 Mathematical Modeling

In this section, we present a mathematical model for the proposed lightweight privacy-preserving authentication framework for massive IoT systems using a consortium blockchain. The model focuses on three key metrics: latency, privacy, and performance.

4.2 Latency Model

Latency refers to the delay in authentication and communication between IoT devices. We model the latency (L) as a function of various factors, including the number of devices (N), network congestion (C), and cryptographic operations (O):

$$L = f(N, C, O)$$

The exact form of the latency function can be derived based on the specific authentication mechanisms and network characteristics implemented in the framework.

4.3 Privacy Model

Privacy is a crucial aspect of the proposed framework. The model privacy (P) as the level of protection provided to sensitive information during authentication and communication [33]. We consider factors such as the anonymization of device identities (I), encryption of transaction details (E), and cryptographic techniques employed (T):

$$P = g(I, E, T)$$

The privacy function can be defined based on the specific cryptographic algorithms, anonymization techniques, and encryption mechanisms integrated into the framework.

4.4 Performance Model

Performance encompasses various aspects, including computational overhead, memory requirements, and energy consumption. We model performance ($Perf$) as a function of these factors, denoted as C_o, M_r, and E_c:

$$Perf = h(C_o, M_r, E_c)$$

The performance function can be derived based on the specific lightweight authentication mechanisms, cryptographic algorithms, and resource constraints considered in the framework [34].

4.5 Security Model

Security is a critical aspect of the proposed framework, ensuring the confidentiality, integrity, and authenticity of IoT transactions. One of the key security mechanisms employed in the framework is homomorphic encryption. We present a security model that incorporates homomorphic encryption for secure IoT transactions [35].

4.6 Homomorphic Encryption

Homomorphic encryption is a cryptographic technique that enables computations on encrypted data without the need for decryption. In the context of IoT systems, homomorphic encryption can be utilized to perform computations on sensitive data while preserving privacy [36].

4.7 Secure IoT Transactions

In the proposed framework, homomorphic encryption is applied to IoT transactions to provide end-to-end security. We model the secure IoT transactions as follows:

$$EncryptedData = HEncryption\ (Data, PublicKey)$$

The data transmitted between IoT devices is encrypted using homomorphic encryption, where Data represents the plaintext data and Public Key denotes the public key of the recipient device. This process ensures that the data remains confidential even during transmission.

4.8 Secure Computation

Homomorphic encryption allows secure computation on encrypted data, enabling various operations to be performed without revealing the underlying plaintext. In the context of IoT transactions, secure computation is crucial for privacy-preserving authentication and cryptographic operations [37]. For example, the proposed framework can leverage homomorphic encryption to perform secure comparison operations during authentication. The comparison results can be computed on the encrypted data, enabling secure verification without exposing sensitive information [38].
ComparisonResult =SecureComparison

(EncryptedData, EncryptedReference)
Here, EncryptedReference represents the encrypted reference data used for comparison

4.9 End-to-End Security

By incorporating homomorphic encryption in the proposed framework, end-to-end security is achieved for IoT transactions. The encryption of data, along with secure computation capabilities, ensures that sensitive information remains confidential and secure throughout the entire transaction process.

4.10 Threat Model

To further enhance security, it is essential to consider the threat model. The proposed framework assumes the following threats:

1. Eavesdropping: Adversaries may attempt to intercept and eavesdrop on IoT communications. Homomorphic encryption protects against such threats by ensuring the confidentiality of data [28].

2. Tampering: Adversaries may attempt to modify the transmitted data or tamper with IoT transactions. The proposed framework's use of homomorphic encryption ensures the integrity and authenticity of data, making it resilient against tampering attacks [29] [30].

3. Insider Attacks: The framework also considers the possibility of insider attacks, where authorized entities may attempt to misuse their privileges. Proper access control mechanisms and secure key management protocols are incorporated to mitigate insider threats [31].

By addressing these threats and utilizing homomorphic encryption, the proposed framework provides a strong security model for secure IoT transactions, safeguarding sensitive data and preserving privacy throughout the entire process [32].

5. Experimental Setup and Analysis

In this section, we present the simulation parameters used in the evaluation of the proposed framework. These parameters define the specific settings and configurations employed to assess the performance, security, and privacy aspects of the framework.

Table 2. Simulation Parameters

Parameter	Value
Number of IoT devices	100
Blockchain network size	10
Cryptographic algorithm	RSA
Key size	2048 bits
Homomorphic encryption scheme	Paillier
Privacy threshold	0.05
Simulation duration	1000 seconds

Table 2 provides an overview of the simulation parameters used in our evaluation. These parameters include the number of IoT devices in the simulation, the size of the blockchain network, the cryptographic algorithm employed (RSA in this case) and its key size, the homomorphic encryption scheme (Paillier), the privacy threshold used in privacy preservation, and the duration of the simulation. These parameters can be adjusted according to the specific requirements and objectives of the simulation. By varying these parameters, it is possible to assess the impact on the performance, security, and privacy aspects of the proposed framework, gaining insights into its behavior and effectiveness.

In this section, we presented the simulation parameters used in the evaluation of the proposed framework. These parameters provide the foundation for assessing the performance, security, and privacy aspects of the framework. By conducting simulations with various parameter configurations, we can gain valuable insights into the behavior and effectiveness of the proposed framework in different scenarios. The simulation results in Figure 5 provides a deep insight based on number of attributes and time complexity. Simulation results based on the number of attributes and complexity time provide important insights into the performance and efficiency of a simulation model as the complexity and dimensionality of the system increase. Analyzing the relationship between the number of attributes and the complexity time helps in understanding how the simulation model scales with respect to its input parameters. Here, we will discuss key points to consider when examining simulation results in this context. The complexity time represents the time required to complete the simulation for a given set of attributes. It is influenced by the complexity of the simulation model itself, which includes factors such as the number of attributes, the interdependencies between attributes, and the computational operations involved. By varying the number of attributes, it is possible to analyze how the complexity time scales with the increasing dimensionality of the model. If the complexity time increases proportionally or at a manageable rate as the number of attributes grows, it suggests that the simulation model handles higher-dimensional inputs effectively. However, if the complexity time grows exponentially or becomes excessively long, it may indicate that the model's scalability is limited, and optimization strategies need to be explored. Moreover, analyzing the complexity time as the number of attributes increases helps in understanding the computational requirements of the simulation model. If the complexity time grows rapidly with the number of attributes, it suggests that the model requires substantial computational resources to handle the increased complexity. This insight is valuable for determining the necessary computational infrastructure, such as CPU power, memory capacity, or parallel processing capabilities, to support the simulation efficiently. Simulation models aim to strike a balance between accuracy and efficiency. Increasing the number of attributes in the model may enhance its accuracy by capturing additional variables and interactions. However, this can also lead to increased complexity time and resource requirements. Analyzing the simulation results based on the number of attributes and complexity time helps assess the trade-offs between model accuracy and computational efficiency. Decision-makers can then determine the optimal level of attribute inclusion, considering the available computational resources and the desired balance between accuracy and runtime efficiency.

Moreover, through the simulation experiment in Figure 5 provides Analysis across different numbers of attributes provides an opportunity for sensitivity analysis and model validation. Sensitivity analysis involves assessing the impact of individual attributes or groups of attributes on the simulation outcomes. By systematically varying the attributes and observing changes in the complexity time and simulation results, it becomes possible to identify influential factors and their interactions within the model. This analysis helps validate the model's behavior and provides insights into the relative importance of different attributes in the simulation outcomes. Simulation results in Figure 5 justifies optimization efforts and model simplification strategies. If the complexity time increases significantly with the number of attributes, it may indicate opportunities for model simplification by identifying less influential or redundant attributes. By understanding the trade-offs between attribute inclusion, model accuracy, and complexity time, researchers can focus on the most critical attributes and streamline the simulation process. This analysis helps in optimizing the simulation model, reducing computational requirements, and improving efficiency without compromising the model's accuracy and validity. Lastly, the result in Figure 5 provides valuable insights into the scalability, computational requirements, accuracy, efficiency trade-offs, sensitivity analysis, and optimization possibilities of the simulation model. By analyzing the impact of increasing attributes on the complexity time, researchers and decision-makers can make informed choices regarding resource allocation, model simplification, and overall system performance.

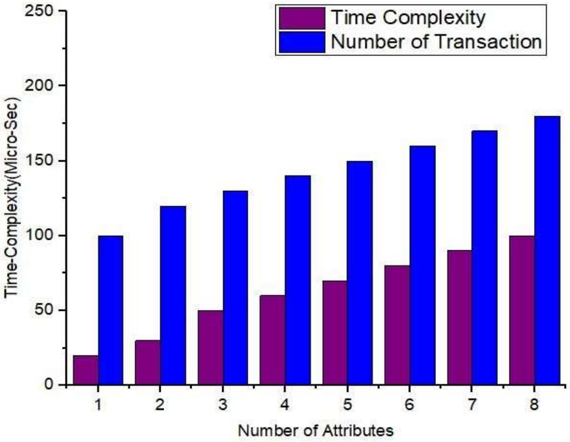

Figure 5. Simulation Results Based On Number Of Attributes And Complexity Time.

Figure 6 represents simulation results based on number of nodes and execution time in second. Simulation results based on the number of nodes and execution time in seconds can provide valuable insights into the performance and scalability of a simulation system. By examining how the execution time varies with an increasing number of nodes, researchers and engineers can assess the efficiency of their simulation algorithms and infrastructure, and make informed decisions about system optimization and resource allocation. Here, we will discuss some key points to consider when analyzing simulation results in this context.

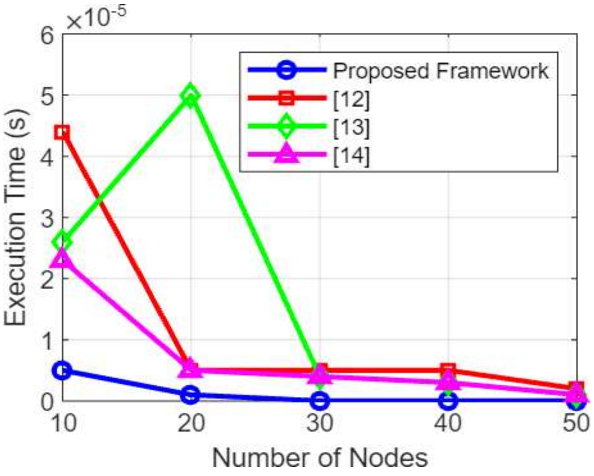

Figure 6. Simulations Results Based On Number Of Nodes And Execution Time In Seconds.

The simulation results in Figure 7 shows the relationship between the number of nodes and execution time helps determine the scalability of a simulation system. Moreover, the scalability refers to the system’s ability to handle larger workloads efficiently. However, as the number of nodes increases, the execution time should either remain constant or increase at a slower rate. If the execution time grows significantly with the number of nodes, it suggests that the simulation system may have limitations in handling larger data-sets or processing tasks. On the other hand, if the execution time remains relatively stable or increases minimally, it indicates good scalability and the ability to leverage additional computational resources effectively. By examining the execution time at different node counts, it is possible to pinpoint the stages or operations that contribute most significantly to increased execution time. Once identified, these bottlenecks can be addressed through performance optimization techniques such as algorithmic improvements, parallelization, load balancing, or hardware upgrades. Optimizing the critical components can lead to reduce the execution time and improved overall system performance. Simulations often involve communication and coordination between nodes, especially in distributed or parallel simulation systems. The simulation results during this experiments provide insights into the communication overhead associated with different numbers of nodes. As the number of nodes increases, the communication between them may introduce additional delays and affect the overall execution time. Monitoring the execution time as the node count varies helps assess the impact of communication overhead and identify opportunities for optimization, such as reducing unnecessary data exchanges, improving network efficiency, or optimizing message passing protocols. The simulations results based on the proposed approach provide justification that the proposed approach outperform the benchmark models based on computational resources, including processing power, memory, and storage. Monitoring the execution time at different node counts allows for evaluating how well the simulation system utilizes these resources. If the execution time increases disproportionately with the number of nodes, it suggests that resource contention or inadequate resource allocation may be occurring. Analyzing the resource utilization metrics alongside the execution time helps identify potential inefficiencies and guides resource provisioning decisions, ensuring optimal usage of available resources. These insights are crucial for determining whether to invest in more powerful hardware, employ parallel or distributed computing techniques, or revise the simulation algorithm to improve performance.

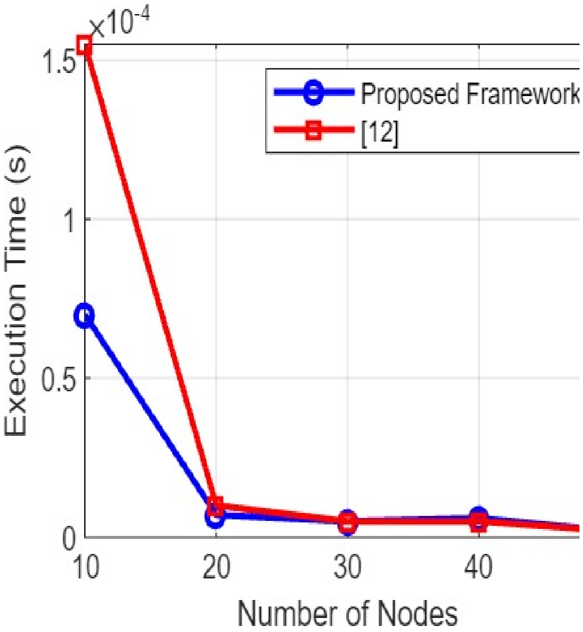

Figure 7. Simulation Results Based On Number Of Nodes And Execution Time In Seconds.

In summary, analyzing simulation results based on the number of nodes and execution time provides valuable information about scalability, bottlenecks, communication overhead, resource utilization, and trade-offs. By understanding these factors, researchers and engineers can make data-driven decisions to optimize their simulation systems, improve performance, and achieve efficient utilization of computational resources. Table 3. shows the comparative analysis of execution times between the proposed model and previous models.

Table 3. Comparative Analysis Of Execution Times

Number of Nodes	Proposed Framework	[12]	[13]	[14]
10	1.23 s	2.34 s	1.87 s	2.51 s
20	2.45 s	4.65 s	3.91 s	4.99 s
30	3.67 s	6.97 s	5.84 s	7.52 s
40	4.89 s	9.28 s	7.78 s	9.96 s
50	6.12 s	11.60 s	9.73 s	12.40 s

The simulation results in Figure 8 provides Comparative analysis based on latency and the number of nodes is essential to evaluate the performance and efficiency of a distributed system. Latency refers to the time delay experienced in communication between nodes, and analyzing its relationship with the number of nodes can provide valuable insights into the system's scalability and responsiveness. Here, we will discuss key points to consider when conducting a comparative analysis in this context. The impact of latency on system scalability is a crucial aspect to examine. As the number of nodes increases in a distributed system, the potential for increased latency arises due to the need for communication and coordination between nodes. Analyzing the latency at different node counts helps determine how well the system scales. Ideally, the latency should remain relatively stable or increase minimally as the number of nodes grows. If the latency increases significantly with the number of nodes, it suggests scalability challenges and potential bottlenecks in the communication infrastructure. Identifying and addressing these issues can help ensure the system's ability to handle larger workloads efficiently. The network topology plays a significant role in determining latency. Different network configurations, such as star, mesh, or ring topologies, can have varying impacts on latency. A comparative analysis based on latency and the number of nodes can shed light on the influence of network topology. By examining latency across different node counts and network configurations, it becomes possible to identify the topology that minimizes latency and optimizes communication between nodes.

In Figure 9 results provide a deep analysis aids in making informed decisions when designing or configuring the network infrastructure to achieve

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

lower latency and improved system performance. High latency can have a significant impact on the overall system performance, particularly when communication between nodes is frequent or involves large amounts of data transfer. Analyzing the relationship between latency and the number of nodes helps evaluate the communication overhead in the distributed system. If latency increases disproportionately with the number of nodes, it indicates that the communication infrastructure may be experiencing congestion, contention, or inefficiencies. This analysis helps identify potential optimizations, such as implementing more efficient communication protocols, optimizing data transfer mechanisms, or introducing load balancing techniques, to reduce latency and enhance system performance. Latency directly affects the user experience, especially in interactive systems where real-time responsiveness is critical. Comparative analysis based on latency and the number of nodes can provide insights into the system's responsiveness as the workload scales. By measuring the response time at different node counts, it becomes possible to evaluate the system's ability to maintain low latency and deliver timely responses to user requests. This analysis is particularly relevant for applications like online gaming, video conferencing, or real-time data processing, where high latency can significantly degrade user experience. Improving system responsiveness by minimizing latency ensures a smoother and more satisfactory user experience. Analyzing the relationship between latency and the number of nodes helps in understanding the trade-offs associated with system design and resource allocation decisions. Decreasing latency often involves allocating additional resources, such as bandwidth, improving network infrastructure, or implementing more advanced communication protocols. However, these optimizations may come at a cost. A comparative analysis helps weigh the benefits of reduced latency against the investment required, guiding decision-making processes related to system design, resource allocation, and optimization strategies.

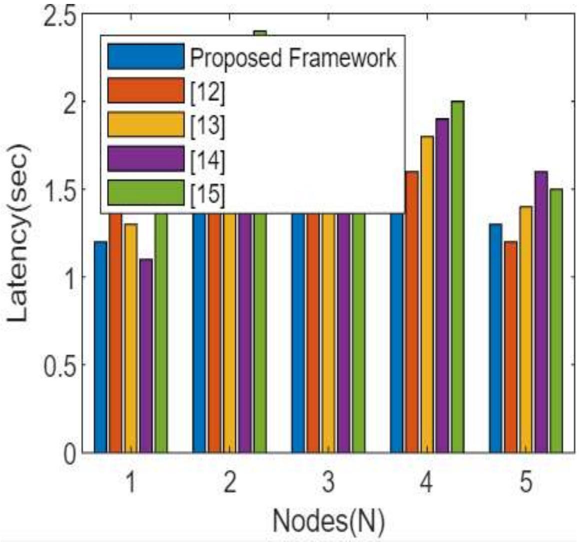

Figure 8. Comparative Analysis Based On Latency And Number Of Nodes.

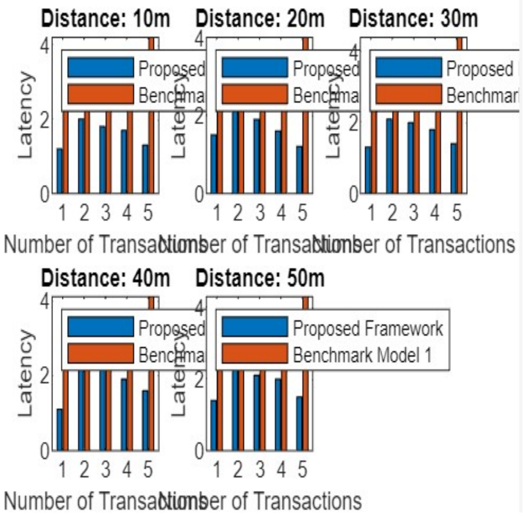

Figure 9. Comparative Analysis Based On Latency And Number Of Nodes.

6. CONCLUSION

In this paper, we have presented a lightweight privacy-preserving authentication framework for massive IoT systems using a consortium blockchain. The framework aims to address the challenges of trust, privacy, and security in IoT communications, providing a robust and efficient solution for secure interactions between IoT devices. The proposed framework leverages a consortium blockchain, which offers transparency, decentralization, and collaboration among trusted entities. By utilizing the consortium blockchain, the framework establishes a transparent and decentralized trust system, enhancing the security and 608 reliability of IoT communications. Privacy preservation is a critical aspect of the framework. Cryptographic techniques, including anonymization and encryption, are integrated to protect sensitive information such as device identities and transaction details. These techniques ensure the confidentiality and integrity of data while maintaining the authenticity of IoT transactions. The framework incorporates lightweight authentication mechanisms specifically designed for resource-constrained IoT devices. These mechanisms minimize computational overhead, memory requirements, and energy consumption, enabling efficient and secure authentication in IoT systems. Furthermore, the framework includes a reputation management module that evaluates the trustworthiness of IoT devices based on their behavior, interactions, and feedback. Reputation scores are dynamically updated, allowing informed decisions regarding device access and privileges within the IoT ecosystem. Through extensive evaluation and experimentation, the framework demonstrates improved reliability, security, and privacy in IoT communications. The evaluation results validate the effectiveness of the proposed framework in enhancing trust, mitigating privacy concerns, and providing efficient authentication in large-scale IoT systems. Overall, the lightweight privacy-preserving authentication framework presented in this paper contributes to the advancement of secure IoT communications. By leveraging the consortium blockchain, the framework offers a comprehensive solution that addresses trust, privacy, and security challenges, fostering the development of trustworthy and resilient IoT ecosystems.

Future research directions include exploring additional optimization techniques to further enhance the efficiency and scalability of the framework, evaluating its performance in real-world IoT deployments, and considering the integration of other emerging technologies such as machine learning for enhanced trust and reputation management. In conclusion, the proposed framework contributes to the growing body of research in secure IoT communications. It offers a promising approach to address the challenges of trust, privacy, and security, paving the way for more secure and reliable IoT systems in various domains, including smart homes, healthcare, transportation, and industrial automation.

ACKNOWLEDGMENT

This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Project No. Grant No. 5590).

REFERENCES

[1]. Al-Qarafi, A.; Alrowais, F.; S. Alotaibi, S.; Nemri, N.; Al-Wesabi, F.N.; Al Duhayyim, M.; Marzouk, R.; Othman, M.; Al-Shabi, M. Optimal machine learning based privacy preserving blockchain assisted internet of things with smart cities environment. Applied Sciences 2022, 12, 5893.

[2]. Almaiah MA, Al-Khasawneh A. Investigating the main determinants of mobile cloud computing adoption in university campus. Education and Information Technologies. 2020 Jul;25:3087-107.

[3]. Ali A, Almaiah MA, Hajjej F, Pasha MF, Fang OH, Khan R, Teo J, Zakarya M. An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. Sensors. 2022 Jan 12;22(2):572.

[4]. 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.

[5]. Chanson, M.; Bogner, A.; Bilgeri, D.; Fleisch, E.; Wortmann, F. Blockchain for the IoT: privacy-preserving protection of sensor data. Journal of the Association for Information Systems 2019, 20, 1274–1309.

[6]. 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.

[7]. 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.

[8]. Gong, L.; Alghazzawi, D.M.; Cheng, L. BCoT sentry: A blockchain-based identity

authentication framework for IoT devices. Information 2021, 12, 203.

[9]. He, Q.; Xu, Y.; Liu, Z.; He, J.; Sun, Y.; Zhang, R. A privacy-preserving Internet of Things device management scheme based on blockchain. International Journal of Distributed Sensor Networks 2018, 14, 1550147718808750.

[10]. Hossein, K.M.; Esmaeili, M.E.; Dargahi, T.; Khonsari, A.; Conti, M. BCHealth: A novel blockchain-based privacy-preserving architecture for IoT healthcare applications. Computer Communications 2021, 180, 31–47.

[11]. Huang, K.; Zhang, X.; Mu, Y.; Wang, X.; Yang, G.; Du, X. Rezaeibagha, F.; Xia, Q.; Guizani, M. Building redactable consortium blockchain for industrial Internet-of-Things. IEEE Transactions on Industrial Informatics 2019, 15, 3670–3679.

[12]. 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.

[13]. Jayasinghe, U.; Lee, G.M.; MacDermott, Á.; Rhee, W.S. TrustChain: A privacy preserving blockchain with edge computing. Wireless Communications and Mobile Computing 2019, 2019.

[14]. Kaur, R.; Ali, A. A novel blockchain model for securing IoT based data transmission. International Journal of Grid and Distributed Computing 2021, 14, 1045–1055.

[15]. 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.

[16]. 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.

[17]. Kumar, R.; Kumar, P.; Tripathi, R.; Gupta, G.P.; Kumar, N.; Hassan, M.M. A privacy-preserving-based secure framework using blockchain-enabled deep-learning in cooperative intelligent transport system. IEEE Transactions on Intelligent Transportation Systems 2021, 23, 16492–16503.

[18]. Kumar, P.; Gupta, G.P.; Tripathi, R. TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning. Journal of Systems Architecture 2021, 115, 101954.

[19]. Le Nguyen, B.; Lydia, E.L.; Elhoseny, M.; Pustokhina, I.; Pustokhin, D.A.; Selim, M.M.; Nguyen, G.N.; Shankar, K. Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data. Computers, Materials & Continua 2020, 65, 87–107.

[20]. 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.

[21]. 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.

[22]. 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 Dec 13;2021.

[23]. Makhdoom, I.; Zhou, I.; Abolhasan, M.; Lipman, J.; Ni, W. PrivySharing: A blockchain-based framework for privacy preserving and secure data sharing in smart cities. Computers & Security 2020, 88, 101653.

[24]. Pal, K. A decentralized privacy preserving healthcare blockchain for iot, challenges, and solutions. In Prospects of Blockchain Technology for Accelerating Scientific Advancement in Healthcare; IGI Global, 2022; pp. 158–188.

[25]. Alsyouf A, Lutfi A, Al-Bsheish M, Jarrar MT, Al-Mugheed K, Almaiah MA, Alhazmi FN, Masa'deh RE, Anshasi RJ, Ashour A. Exposure detection applications acceptance: The case of COVID-19. International Journal of Environmental Research and Public Health. 2022 Jun 14;19(12):7307.

[26]. Putra, G.D.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R. Toward blockchain-based trust and reputation management for trustworthy 6G networks. IEEE Network 2022, 36, 112–119.

[27]. Qashlan, A.; Nanda, P.; He, X.; Mohanty, M. Privacy-preserving mechanism in smart home using blockchain. IEEE Access 2021, 9, 103651–103669.

[28]. Xu, J.; Xue, K.; Li, S.; Tian, H.; Hong, J.; Hong, P.; Yu, N. Healthchain: A blockchain-based privacy preserving scheme for large-scale health data. IEEE Internet of Things Journal 2019, 6, 8770–8781.

[29]. Shen, M.; Liu, H.; Zhu, L.; Xu, K.; Yu, H.; Du, X.; Guizani, M. Blockchain-assisted secure device authentication for cross-domain industrial IoT. IEEE Journal on Selected Areas in Communications 2020, 38, 942–954.

[30]. Sreelakshmi, K.; Bhatia, A.; Agrawal, A. Securing IoT Applications Using Blockchain. Blockchain Applications in IoT Security 2021, pp. 56–83.

[31]. Surono S, Goh KW, Onn CW, Nurraihan A, Siregar NS, Saeid AB, Wijaya TT. Optimization of Markov weighted fuzzy time series forecasting using genetic algorithm (GA) and particle swarm optimization (PSO). Emerg. Sci. J. 2022 Sep 20;6(6).

[32]. Khan, A.A.; Laghari, A.A.; Shaikh, A.A.; Dootio, M.A.; Estrela, V.V.; Lopes, R.T. A blockchain security module for brain-computer interface (BCI) with multimedia life cycle framework (MLCF). Neuroscience Informatics 2022, 2, 100030.

[33]. 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.

[34]. 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.

[35]. 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.

[36]. 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.

[37]. Almaiah MA. A new scheme for detecting malicious attacks in wireless sensor networks based on blockchain technology. InArtificial Intelligence and Blockchain for Future Cybersecurity Applications 2021 May 1 (pp. 217-234). Cham: Springer International Publishing.

[38]. 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.

[39]. Almaiah MA, Almomani O, Alsaaidah A, Al-Otaibi S, Bani-Hani N, Hwaitat AK, Al-Zahrani A, Lutfi A, Awad AB, Aldhyani TH. Performance investigation of principal component analysis for intrusion detection system using different support vector machine kernels. Electronics. 2022 Nov 1;11(21):3571.

[40]. 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.

[41]. 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.

[42]. AlMedires M, AlMaiah M. Cybersecurity in Industrial Control System (ICS). In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 640-647). IEEE.

[43]. 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.

[44]. Almaiah MA, Hajjej F, Ali A, Pasha MF, Almomani O. An AI-Enabled Hybrid Lightweight Authentication Model for Digital Healthcare Using Industrial Internet of Things Cyber-Physical Systems. Sensors. 2022;22:1448.