*electronics*

MDPI

*Article*

# Enhancing Industrial IoT Network Security through Blockchain Integration

**Yash Bobde [1], Gokuleshwaran Narayanan [1], Manas Jati [1], Raja Soosaimarian Peter Raj [1,*], Ivan Cvitić [2,*] and Dragan Peraković [2]**

[1] School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, Tamil Nadu, India; yashsantosh.bobde2020@vitstudent.ac.in (Y.B.); gokuleshwaran.n2020@vitstudent.ac.in (G.N.)

[2] Department of Information and Communiation Traffic, Faculty of Transport and Traffic Sciences, University of Zagreb , Vukelićeva 4, 10000 Zagreb, Croatia; dragan.perakovic@fpz.unizg.hr

* Correspondence: raja.sp@vit.ac.in (R.S.P.R.); ivan.cvitic@fpz.unizg.hr (I.C.)

**Abstract:** In the rapidly evolving landscape of industrial ecosystems, Industrial IoT networks face increasing security challenges. Traditional security methods often struggle to protect these networks adequately, posing risks to data integrity, confidentiality, and access control. Our research introduces a methodology that leverages blockchain technology to enhance the security and trustworthiness of IoT networks. This approach starts with sensor nodes collecting and compressing data, followed by encryption using the ChaCha20-Poly1305 algorithm and transmission to local aggregators. A crucial element of our system is the private blockchain gateway, which processes and classifies data based on confidentiality levels, determining their storage in cloud servers or the Interplanetary File System for enhanced security. The system's integrity and authenticity are further reinforced through the proof of authority consensus mechanism. This system employs Zero Knowledge Proof challenges for device authorization, optimizing data retrieval while maintaining a delicate balance between security and accessibility. Our methodology contributes to mitigating vulnerabilities in Industrial IoT networks and is part of a broader effort to advance the security and operational efficiency of these systems. It reflects an understanding of the diverse and evolving challenges in IoT security, emphasizing the need for continuous innovation and adaptation in this dynamic field.

**Keywords:** Industrial IoT networks; blockchain technology; data security and integrity; ChaCha20-Poly1305 encryption; private blockchain gateway; Interplanetary File System; proof of authority consensus; Zero Knowledge Proof; data confidentiality; access control



**Citation:** Bobde, Y.; Narayanan, G.; Jati, M.; Raj, R.S.P.; Cvitić, I.; Peraković, D. Enhancing Industrial IoT Network Security through Blockchain Integration. *Electronics* **2024**, *13*, 687. https://doi.org/10.3390/electronics13040687

Academic Editors: Giovanni Crupi and Yung-Fa Huang

Received: 23 December 2023
Revised: 28 January 2024
Accepted: 5 February 2024
Published: 7 February 2024



## 1. Introduction

The Industrial Internet of Things (IoT) has ushered in a new era in the industrial sector, marked by the extensive integration of interconnected devices and systems. This revolution is redefining industry standards through real-time data collection, processing, and decision-making capabilities. However, the rapid expansion of IoT networks introduces significant challenges, particularly in the realms of data security, integrity, and privacy, which are crucial in industrial settings [1].

In this context, blockchain technology, renowned for its decentralized ledger system, emerges as a potent solution to these burgeoning challenges [2]. Its ability to ensure data integrity, transparency, and trustworthiness positions it as an ideal candidate to secure sensitive industrial data [3]. This research paper delves into the potential of blockchain in enhancing the security of IoT networks. We focus on employing private blockchain gateways to safeguard the data flow from sensor nodes to core processing units, integrating advanced cryptographic techniques like Zero Knowledge Proof (ZKP) to authenticate data and restrict access to authorized entities.

Before delving into our proposed solution, it is crucial to understand the disadvantages of existing IoT systems. Current IoT networks often suffer from centralized data management models, which pose significant risks in terms of single points of failure and potential data breaches. Additionally, these systems frequently struggle with scalability issues, as the number of interconnected devices grows exponentially. The lack of robust encryption and authentication mechanisms in many existing IoT frameworks further exacerbates the security vulnerabilities, making them susceptible to various cyber threats.

To contextualize our contribution, we overview the state of the art in this domain. The integration of blockchain in IoT is still in its early stages, with several studies and implementations exploring its potential. These efforts primarily focus on leveraging blockchain to ensure data integrity and facilitate secure, transparent transactions across IoT networks. However, there is a gap in effectively integrating blockchain with IoT to address both security concerns and operational efficiency comprehensively.

The primary contribution of this study lies in its comprehensive approach to addressing the security needs of IoT networks. We propose a novel system that employs advanced encryption techniques, priority-based data transmission, and consensus mechanisms to ensure the security, authenticity, and transparency of IoT data. This system is not only focused on enhancing security but also establishing a new standard in IoT network efficiency and privacy.

The rest of the article is organized as follows. Section 2 begins by introducing some preliminaries and related work, laying the groundwork for a deeper understanding of the current state of the art in blockchain and IoT integration. Section 3 discusses the key components of the proposed system, elucidating their functions and significance. The architecture of the proposed system is explored in Section 4, providing insights into its structural design. Section 5 delves into the features, limitations, practical implications, and results of the proposed system, offering a comprehensive analysis. Finally, the article concludes with Section 6, presenting a concise summary of the research and its contributions.

## 2. Related Work

In exploring the integration of IoT and blockchain, this section examines key studies to understand the current advancements and challenges in the field. These selected works provide a context and insights relevant to our research, highlighting the complexities and potential solutions in enhancing IoT security through blockchain technology. Tables 1 and 2 present a concise comparison of significant IoT and blockchain studies.

In [4], Christidis et al. argue for its potential to revolutionize the domain through decentralized, trustless interactions and automated processes via smart contracts. Despite this promise, they acknowledge significant challenges, such as scalability, privacy, and legal enforceability, that must be addressed. They suggest innovative solutions like "dual integration" for legal robustness and propose privacy-preserving techniques, although these come with trade-offs in performance and complexity. The study indicates that while blockchain can enable new business models and efficiencies in IoT, the deployment of such technology requires the careful consideration of its limitations and ongoing research to mitigate its drawbacks.

Alia Al Sadawi et al. [5] have presented a nuanced analysis of IoT and blockchain convergence, proposing a novel three-tier architecture that integrates dew and cloudlet computing to surmount existing challenges in scalability, efficiency, and latency. The architecture employs Practical Byzantine Fault Tolerance (PBFT) for consensus, enhancing the system performance and data integrity. Despite the strengths of their proposed system, the authors concede that PBFT's susceptibility to Sybil attacks remains a concern, with sharding offered as a potential but complex countermeasure. The authors' admission of these challenges underscores the necessity for continued exploration in fortifying the security framework of IoT–blockchain integration.

**Table 1.** Comparison of key literature on IoT and blockchain integration (Part 1).

| Authors | Title | Main Contributions | Challenges Identified | Proposed Solutions | Application Domain |
|---|---|---|---|---|---|
| Christidis et al. [4] | Blockchains and Smart Contracts for the Internet of Things | Discusses the potential of blockchain and smart contracts in revolutionizing IoT through decentralized interactions and automated processes. | Challenges like scalability, privacy, and legal enforceability. | Suggests solutions like dual integration for legal robustness and privacy-preserving techniques. | Internet of Things |
| Alia Al Sadawi et al. [5] | A Survey on the Integration of Blockchain With IoT to Enhance Performance and Eliminate Challenges | Provides a nuanced analysis of IoT and blockchain convergence, proposing a novel three-tier architecture integrating dew and cloudlet computing. | Addresses challenges in scalability, efficiency, and latency in IoT–blockchain systems. | Employs Practical Byzantine Fault Tolerance (PBFT) for consensus, enhancing system performance and data integrity. Recognizes PBFT's susceptibility to Sybil attacks and suggests sharding as a countermeasure. | IoT and Blockchain Integration |
| Ouaddah et al. [6] | Fair Access: a new Blockchain-based access control framework for the Internet of Things | Presents Fair Access, an innovative blockchain-based access control framework for IoT, demonstrated through a smart security camera system. | Challenges in real-time processing and blockchain scalability in IoT. | Proposes custom blockchain development and future extensions including secure storage layer and a billing model to incentivize data sharing. | IoT Security |
| Wang et al. [7] | RDIC: A blockchain-based remote data integrity checking scheme for IoT in 5G networks | Introduces a blockchain-based RDIC scheme to enhance IoT security within 5G networks, with rigorous proofs of correctness and unforgeability. | Need for trustworthy data and secure data integrity in autonomous vehicle systems and IoT within 5G networks. | Application of RDIC scheme to the Internet of Vehicles, addressing the vital need for trustworthy data in autonomous vehicle systems. | IoT Security in 5G Networks |
| Rane et al. [8] | Data-driven decision making with Blockchain-IoT integrated architecture: a project resource management agility perspective of industry 4.0 | Assesses the shortcomings of traditional project resource management (PRM) tools in the EPC industry, proposing an integrated blockchain and IoT architecture for enhanced decision making and operational agility. | Challenges in manual data entry and delayed updates in traditional PRM tools in the EPC industry. | Proposes the integration of blockchain and IoT for real-time data and autonomous resource coordination, aiming to improve decision making and agility in operations. | Project Resource Management in Industry 4.0 |

**Table 2.** Comparison of key literature on IoT and blockchain integration (Part 2).

| Authors | Title | Main Contributions | Challenges Identified | Proposed Solutions | Application Domain |
|---|---|---|---|---|---|
| Ma et al. [9] | Blockchain + IoT sensor network to measure, evaluate, and incentivize personal environmental accounting and efficient energy use in indoor spaces | Advances real-time carbon accounting and energy monitoring, integrating IoT sensors with blockchain for improved data acquisition and management in energy use evaluation. | Challenges like data lags and volatility in emissions factors. | Applies predictive modeling and machine learning algorithms to optimize energy consumption patterns, promoting sustainable energy behaviors. | Sustainable Energy Management |
| Farahani et al. [10] | The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions | Explores the synergistic integration of IoT with distributed ledger technologies (DLT), outlining opportunities and solutions for challenges in this convergence. | Identifies challenges in scalability, security, and privacy in the IoT-DLT ecosystem. | Suggests innovative approaches to address these challenges, underscoring the importance of further research and development in IoT and DLT integration. | IoT and Distributed Ledger Technologies |

**Table 2.** *Cont.*

| Authors | Title | Main Contributions | Challenges Identified | Proposed Solutions | Application Domain |
|---|---|---|---|---|---|
| Alrubei et al. [11] | A Secure Blockchain Platform for Supporting AI-Enabled IoT Applications at the Edge Layer | Develops a secure blockchain platform for AI-enabled IoT applications at the edge layer, enhancing security and decentralized operations. | Focuses on challenges related to security and integration of AI and IoT at the edge layer. | Proposes a blockchain solution to provide a secure and decentralized platform for public health surveillance and AI applications in IoT. | AI-Enabled IoT Applications |
| Sun et al. [12] | Blockchain-Based IoT Access Control System: Towards Security, Lightweight, and Cross-Domain | Proposes a blockchain-based IoT access control system, integrating Hyperledger Fabric for management of local ledgers and enhanced system resilience. | Addresses the need for secure, lightweight, and cross-domain access control in IoT. | Integrates the ABAC model with blockchain, introducing MSPs for trusted cross-domain interactions and emphasizing lightweight design for performance and resource efficiency. | IoT Access Control |
| Bataineh et al. [13] | Novel and Secure Blockchain Framework for Health Applications in IoT | Develops a novel and secure blockchain framework specifically tailored for health applications in IoT, focusing on enhancing data security and operational efficiency. | Challenges in data security and operational efficiency in healthcare IoT applications. | Proposes a private Ethereum network and smart contracts to create a secure, decentralized framework adhering to global EHR standards. | Healthcare IoT |

In [4], Christidis et al. argue for its potential to revolutionize the domain through decentralized, trustless interactions and automated processes via smart contracts. Despite this promise, they acknowledge significant challenges, such as scalability, privacy, and legal enforceability, that must be addressed. They suggest innovative solutions like "dual integration" for legal robustness and propose privacy-preserving techniques, although these come with trade-offs in performance and complexity. The study indicates that while blockchain can enable new business models and efficiencies in IoT, the deployment of such technology requires the careful consideration of its limitations and ongoing research to mitigate its drawbacks.

Alia Al Sadawi et al. [5] have presented a nuanced analysis of IoT and blockchain convergence, proposing a novel three-tier architecture that integrates dew and cloudlet computing to surmount existing challenges in scalability, efficiency, and latency. The architecture employs Practical Byzantine Fault Tolerance (PBFT) for consensus, enhancing the system performance and data integrity. Despite the strengths of their proposed system, the authors concede that PBFT's susceptibility to Sybil attacks remains a concern, with sharding offered as a potential but complex countermeasure. The authors' admission of these challenges underscores the necessity for continued exploration in fortifying the security framework of IoT–blockchain integration.

Ouaddah et al. [6] present an innovative access control framework for IoT, leveraging blockchain technology to address the growing need for robust security in the expanding IoT landscape. Their framework, Fair Access, is exemplified through a smart security camera system, demonstrating the practical application of identity-based and permissioned access control policies. Despite facing challenges such as real-time processing and blockchain scalability, the authors propose solutions like custom blockchain development and future extensions including a secure storage layer and a billing model to incentivize data sharing. This work not only provides a proof of concept for blockchain's application in IoT security but also opens avenues for further enhancements in access control mechanisms.

Wang et al. [7] have contributed to the enhancement of IoT security within 5G networks by introducing a blockchain-based RDIC scheme. Their research provides rigorous proofs of the scheme's correctness and unforgeability, which ensures a secure and efficient approach to data integrity. The application of their RDIC scheme to the Internet of Vehicles is of

particular importance, addressing the vital need for trustworthy data in autonomous vehicle systems. Wang et al.'s work progresses the understanding of RDIC mechanisms and lays the groundwork for future investigations into privacy-preserving and multi-owner RDIC frameworks, marking an important intersection of blockchain technology and IoT security.

Rane et al. [8] critically assess the shortcomings of traditional Project Resource Management (PRM) tools in the Engineering, Procurement, and Construction (EPC) industry, which are exacerbated by the rapid pace of Industry 4.0. They propose an integrated blockchain and IoT architecture to mitigate inefficiencies like manual data entry and delayed updates, highlighting the advantages of real-time data and autonomous resource coordination for improved decision making and agility in operations. Despite the promise of this integration in enhancing resource allocation and utilization, Rane et al. also recognize the implementation challenges, including the need for substantial infrastructural updates and the industry's adjustment to new practices, suggesting a cautious yet optimistic approach to adopting these technologies in PRM.

Ma et al. [9] have contributed significantly to the advancement of real-time carbon accounting and energy monitoring by highlighting the essential roles of carbon intensity (CI), overall carbon optimization (OCO), and marginal carbon optimization (MCO) in evaluating energy use and its environmental impact. Their integration of IoT sensors with blockchain technology has revolutionized data acquisition and management, improving the transparency and scalability of energy monitoring systems. The application of predictive modeling and machine learning algorithms in their study showcases the potential for the optimization of energy consumption patterns. Despite facing challenges like data lags and volatility in emissions factors, Ma et al.'s research offers a promising framework for the promotion of sustainable energy behaviours and the enhancement of demand response strategies, thereby making a notable contribution to sustainable energy management practices.

Farahani et al. [10] present a nuanced reference architecture for the healthcare sector that leverages the synergy between private and federated blockchains to ensure secure, compliant, and efficient data sharing among various healthcare stakeholders. The architecture emphasizes the empowerment of data owners through smart contracts, ensuring the control and privacy of data across their lifecycle. The integration of off-chain and on-chain data management is particularly notable for its adherence to GDPR and operational transparency. Through performance evaluations using the Hyperledger framework, Farahani et al. demonstrate the architecture's capability to handle high transaction loads, essential for the scalability of healthcare systems. This work by Farahani et al. is instrumental in illustrating the potential of blockchain technology to enhance data integrity, security, and privacy in healthcare, paving the way for innovative IoT eHealth solutions.

Alrubei et al. [11] explore the synergy of AI, IoT, and blockchain technologies to create a robust system for the monitoring of viral markers in sewage water, a method that could revolutionize the early detection of viruses like COVID-19. The system leverages the predictive power of AI, the sensory network of IoT, and the immutable ledger of blockchain to provide a secure and decentralized platform for public health surveillance. While the approach offers significant advantages, including real-time data collection and a minimal impact on device power, it is not without challenges. The complexity of integrating these technologies poses potential scalability issues, and the reliance on biosensors necessitates further research to assess their real-world efficacy and security implications. Alrubei et al.'s work underscores the need for comprehensive testing in diverse environments to ensure the system's reliability and effectiveness in public health applications.

Sun et al. [12] have made a significant contribution to the field of IoT access control by proposing a blockchain-based framework that leverages Hyperledger Fabric to manage local ledgers, thereby enhancing the system's resilience to centralized failures. Their approach integrates the ABAC model with blockchain to ensure immutable and traceable access control policies, reflecting the growing need for secure and fine-grained access control mechanisms. The introduction of MSPs by the authors enables trusted cross-domain

interactions, which is essential for the interoperability of contemporary IoT systems. The framework also demonstrates an ability to withstand DDoS attacks through the use of identity-based signatures at the edge device level, indicating a proactive approach to security. By prioritizing a lightweight design, Sun et al.'s system reduces the storage overhead and maintains efficient policy decision making, striking a balance between performance and limited resources. This research marks a substantial advancement in developing secure, decentralized, and efficient IoT access control systems and sets a new standard for subsequent research in the domain.

Bataineh et al. [13] explore the integration of IoT and blockchain technologies in healthcare, focusing on surgical management systems within hospitals. Utilizing a private Ethereum network and smart contracts, they develop a secure, decentralized framework that adheres to global EHR standards. The ERTCA architecture that they propose demonstrates the feasibility of merging IoT with blockchain to enhance CPU and network performance, compared to conventional systems. Their research offers a scalable approach to improve data security and operational efficiency in healthcare, suggesting significant potential for broader applications in the sector.

## 3. Key Components of the Proposed System

This section outlines the essential components of our proposed system, each playing a crucial role in enhancing the security, efficiency, and scalability of the Industrial IoT network integrated with blockchain technology.

### *3.1. Sensor Nodes*

Sensor nodes range from straightforward devices such as temperature monitors to complex systems like surveillance cameras, and they determine the nature and format of the data collected. These nodes are increasingly being equipped with edge computing capabilities, which allow for a degree of local data preprocessing [14]. Even less resource-intensive sensors can engage in basic edge computing tasks by employing streamlined algorithms and optimized firmware tailored to their processing abilities. This local preprocessing can include simple actions such as data filtering or threshold checks, which enable the sensors to send only relevant information, thereby reducing the volume of data transmitted.

This selective transmission is particularly beneficial for real-time applications, where it not only minimizes the latency due to less data needing to be sent through the network but also conserves bandwidth—a critical consideration in areas with limited connectivity. Additionally, for sensors incapable of complex computations, collaborative processing techniques can be utilized, where multiple sensors work in tandem or offload more demanding tasks to nearby edge devices or cloud services. Through these methods, even basic sensor nodes can contribute to the overall efficiency and responsiveness of the IoT ecosystem.

### *3.2. Blockchain*

Blockchain technology, fundamental to our proposed system, is a decentralized ledger system that records transactions across a network of computers. This decentralized nature is crucial in the IoT context, where it acts as a critical layer to ensure data integrity, security, and trust. Blockchain offers a tamper-proof record of data transactions between IoT devices, crucial for maintaining data integrity in networks where security and trust are paramount.

Its decentralized nature eliminates the need for a central authority, making the system inherently resistant to single points of failure and more secure than traditional centralized systems. Each transaction on the blockchain is verified by multiple nodes, ensuring transparency and trustworthiness in data exchanges [3].

However, blockchain operation is resource-intensive, involving complex cryptographic computations for transaction validation and ledger maintenance. To address these challenges, our proposed system leverages a private blockchain, a permissioned network where access is restricted to authorized nodes. This approach reduces the computational load and energy consumption, making it more suitable for IoT applications with resource con-

straints [15]. The private blockchain serves as the backbone for secure data transactions between IoT devices and the network, ensuring the secure, verified, and immutable recording of data. This integration aims to harness blockchain's security and reliability, while specifically addressing the resource limitations inherent in IoT devices.

### 3.3. Certificate Authority

Certificate authority (CA) plays a pivotal role in the proposed system, especially in the realm of data transmission. The process involves the strategic use of certificate caching, where, instead of repeatedly requesting new certificates, aggregators can store and reuse previously acquired ones. This approach, especially beneficial for consistent data structures or recurring data patterns, significantly reduces the latency and enhances the transmission speed. However, efficient cache management is paramount, encompassing considerations like certificate validity, cache storage limits, and replacement strategies such as Least Recently Used (LRU) or First In First Out (FIFO).

Furthermore, the integration of machine learning within the CA framework offers a novel dimension. It enables the CA to anticipate and swiftly validate recurrent certificate requests. This predictive capability stems from training the model on historical certificate requests and their respective outcomes. As the model assimilates more data, its predictive accuracy amplifies. However, while machine learning expedites the validation process, maintaining security remains paramount. Implementing regular audits, anomaly detection, and periodic manual checks ensures the sanctity of the validation process. Additionally, a feedback loop can be instituted, allowing the CA to perpetually refine its predictions based on real-time outcomes, ensuring sustained accuracy and relevance.

### 3.4. Interplanetary File System (IPFS)

The IPFS, or the Interplanetary File System, is a decentralized and distributed file system designed to make the web faster, safer, and more open. It replaces traditional file addressing with content addressing, meaning that files are retrieved based on their content hash rather than their location. This ensures data integrity, reduces the dependence on a single point of failure, and enables peer-to-peer data sharing, making the web more resilient and efficient [16].

### 3.5. Zero Knowledge Proof

Zero Knowledge Proof (ZKP) is a cryptographic technique that allows one party to prove to another that a statement is true, without revealing any specific information about the statement itself. In decentralized systems, ZKP caching can be implemented to store and reuse previously validated proofs, enhancing the efficiency. By caching ZKPs, systems can reduce the computational overhead of repeatedly generating or verifying the same proofs, leading to faster transaction times and optimized resource utilization while maintaining data privacy and security [17,18].

### 3.6. Proof of Authority (PoA)

PoA is a consensus mechanism in blockchain technology where a limited number of trusted entities, known as validators, are given the authority to create new blocks and validate transactions. Unlike proof of work (PoW) which relies on computational power, PoA is based on the reputation and identity of its validators. This approach offers faster transaction times and higher scalability. Additionally, PoA is energy-efficient as it does not require the intensive computational mining process. However, the centralized nature of validator selection can raise concerns about the system's decentralization and potential vulnerabilities [19].

### 3.7. Lightweight Compression

Lightweight compression is a technique designed to reduce the size of data using minimal computational resources. It is especially valuable in scenarios where devices have

limited processing power or bandwidth, such as with IoT sensors [20]. By condensing data efficiently, lightweight compression ensures faster transmission speeds and reduced storage needs. This approach not only conserves bandwidth but also extends the battery lives of devices by minimizing data processing and transmission times [21].

## 4. Proposed System

This section delineates the architecture of a novel multi-phase system designed to seamlessly integrate IoT devices with a private blockchain network, as depicted in Figure 1. The system is partitioned into four distinct phases, each addressing specific challenges and leveraging advanced cryptographic techniques to ensure data integrity, security, and efficient processing. The forthcoming subsections will elaborate on the operational intricacies of each phase.

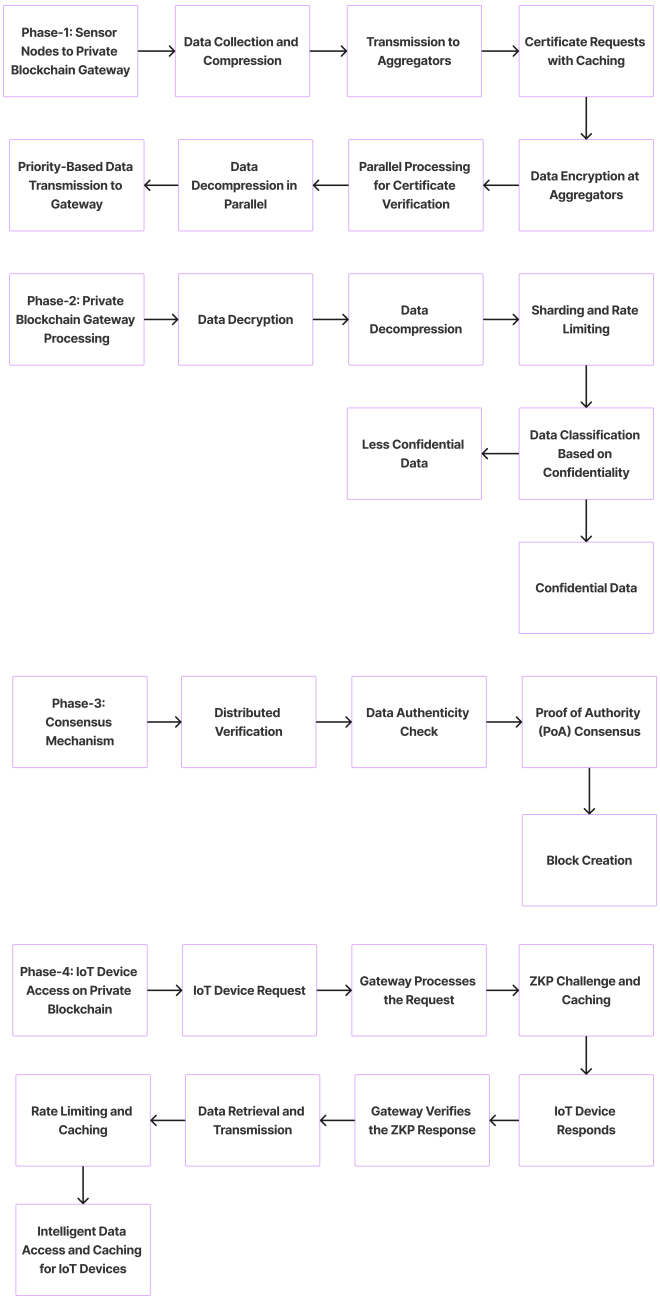


**Figure 1.** Architecture of the proposed system.

### *4.1. Phase-1: Sensor Nodes to Private Blockchain Gateway*

Phase-1 lays the groundwork for data acquisition and initial processing. It encompasses the collection of environmental data by sensor nodes, followed by a series of steps to prepare these data for secure and efficient transmission to the blockchain network. Algorithm 1 delineates the Phase-1 process, mapping the journey from data collection by sensor nodes to their transmission to the private blockchain gateway, encompassing key steps like compression, encryption, and prioritized transmission.

**Algorithm 1** Sensor Nodes to Private Blockchain Gateway

**Input:** Data from sensor nodes, local aggregator, CA certificate cache
**Output:** Encrypted and compressed data for gateway

**for** each sensor node **do**
  Collect data from environment
  Compress data using lightweight compression algorithm
  Transmit compressed data to local aggregator
**end for**
**for** each local aggregator **do**
  **if** certificate not in cache **then**
    Request batch certificate from CA
    Cache the received certificate
  **end if**
  Encrypt compressed data using ChaCha20-Poly1305 algorithm
  Send encrypted data to distributed nodes for verification
**end for**
**for** each distributed node **do**
  Verify batch certificate in parallel
  Decompress encrypted data in parallel
  Transmit decompressed data to gateway based on priority
**end for**

#### 4.1.1. Data Collection and Lightweight Compression

Sensor nodes, deployed in various environments, actively gather raw data. To optimize storage and transmission, these data undergo efficient lightweight compression. This process ensures that large volumes of data are compacted, readying them for secure and streamlined transmission to local aggregators.

#### 4.1.2. Transmission of Data to Local Aggregators

Once the data are compressed, sensor nodes forward them to local aggregators. These aggregators act as intermediary collection points, amassing data from multiple sensor nodes. Their role streamlines the data flow, preparing it for further processing and eventual transmission to the blockchain gateway.

#### 4.1.3. Certificate Requests with Caching

Local aggregators request batch certificates from the CA to authenticate the data. To enhance the efficiency, these certificates are cached, ensuring that recurring data transmissions are expedited. This caching mechanism reduces the need for frequent CA validations, optimizing the data transmission process.

#### 4.1.4. Data Encryption at Aggregators

Local aggregators, after receiving and aggregating data from sensor nodes, employ the ChaCha20-Poly1305 encryption algorithm to secure the compressed data [22]. This encryption ensures that the data remain confidential and tamper-proof during their transmission to the distributed nodes and ultimately to the private blockchain gateway.

#### 4.1.5. Parallel Processing for Certificate Verification by Distributed Nodes

Distributed nodes across the network collaboratively engage in the verification of the batch certificates associated with the data. By leveraging parallel processing, these nodes efficiently authenticate the data's source and integrity, ensuring that only genuine and untampered data progress to the next stages of the system. This distributed approach enhances the system's scalability and responsiveness.

#### 4.1.6. Data Decompression in Parallel

Upon successful verification, the encrypted data batches received by the distributed nodes are decrypted. These nodes then employ parallel processing to decompress the data, reversing the initial lightweight compression. This parallel approach ensures the swift retrieval of the original sensor readings, preparing the data for subsequent transmission to the private blockchain gateway.

#### 4.1.7. Priority-Based Data Transmission to Gateway

After decompression, the data are prioritized based on predefined criteria, such as their importance, urgency, or source. The prioritized data are then transmitted to the private blockchain gateway. This structured approach ensures that critical data reach the gateway first, optimizing the overall data processing and ensuring timely responses to high-priority events or alerts.

### *4.2. Phase-2: Private Blockchain Gateway Processing*

In Phase-2, the private blockchain gateway acts as the central hub for data decryption, decompression, and intelligent distribution across the blockchain network. Algorithm 2 outlines the process that a private blockchain gateway follows when it receives encrypted and compressed data from distributed nodes. The gateway's role is to securely decrypt and decompress these data and then intelligently distribute them across the blockchain network. The final step is to update the blockchain with references to the data's new storage location.

**Algorithm 2** Private Blockchain Gateway Processing

**Input:** Encrypted and compressed data from distributed nodes
**Output:** Data stored in IPFS and blockchain updated with IPFS index and hash

1: Decrypt received data
2: Decompress data to retrieve original sensor readings
3: Allocate decompressed data to shards based on:
   - Dynamic sharding algorithms
   - Adaptive rate limits
4: **if** data are less confidential **then**
5: Store data in cloud server
6: Hash data using optimal hashing technique
7: Package data for IPFS and upload
8: Update blockchain with IPFS index and data hash
9: **else**
10: Package data for IPFS and upload directly
11: Update blockchain with only IPFS index
12: **end if**

#### 4.2.1. Data Decryption at the Private Blockchain Gateway

Upon receiving the transmitted data, the private blockchain gateway initiates the decryption process. Utilizing the corresponding decryption key, the gateway decrypts the data that were encrypted using the ChaCha20-Poly1305 algorithm at the aggregators. This

step ensures that the data remain secure during transmission and are only accessible to authorized entities within the network.

#### 4.2.2. Data Decompression

Upon receiving the compressed data, the private blockchain gateway initiates the decompression process. Utilizing specialized algorithms, the gateway reverses the lightweight compression applied earlier, restoring the data to their original form. These decompressed data retain all the original details and readings from the sensor nodes, making them ready for further processing or storage within the system.

#### 4.2.3. Intelligent Sharding and Adaptive Rate Limiting

The private blockchain gateway employs intelligent sharding techniques to efficiently allocate and distribute the decompressed data across various blockchain segments or shards. This dynamic allocation ensures optimal data storage and retrieval. Concurrently, adaptive rate limiting mechanisms are in place to monitor and control the data processing speed. By assessing the current network load and adjusting the data processing rate accordingly, the system ensures smooth operations without overburdening the network or the blockchain [23].

#### 4.2.4. Data Classification Based on Confidentiality

Upon receiving the decompressed data, the private blockchain gateway classifies the data based on their confidentiality level. Using predefined criteria, data are categorized as "less confidential" or "confidential". This classification determines the subsequent storage and handling procedures. "Less confidential" data might be stored in more accessible locations like cloud servers, while "confidential" data undergo stricter storage and access protocols, ensuring that sensitive information remains secure and protected.

#### 4.2.5. For Less Confidential Data

Data deemed "less confidential" undergo a specific handling process. Initially, they are stored in a cloud server, ensuring easy accessibility without compromising the blockchain's efficiency. An optimal hashing technique is then applied to these data, generating a unique digital signature or hash. These data are subsequently packaged in a format suitable for the IPFS and uploaded to it. The blockchain is then updated with both the IPFS index, which points to the data's location, and the generated hash, ensuring data integrity and quick retrieval when needed.

For access control, we employ Zero Knowledge Proof (ZKP), a method that allows the verification of access rights without revealing sensitive information, thereby maintaining data privacy and security. This approach is particularly effective in managing access to confidential data stored on the IPFS, ensuring that only authorized entities can access them.

Regarding data retention and deletion, our system adheres to predefined policies that align with regulatory requirements and organizational needs. These policies dictate the duration for which data are retained and the conditions under which they are deleted or archived. The blockchain component plays a crucial role here, offering a transparent and immutable record of all data transactions, access requests, and changes in data storage, thereby facilitating auditability and compliance with data governance standards.

#### 4.2.6. For Confidential Data

When data are classified as "confidential", they demand a heightened level of security and discretion. Such data are directly packaged in a format compatible with the IPFS and then uploaded to the IPFS, ensuring their decentralized and secure storage. Unlike less confidential data, only the IPFS index, which serves as a reference to the data's location in the IPFS, is updated on the blockchain. This approach ensures that the actual data remain off-chain, preserving their confidentiality while still allowing for their traceability and accessibility through the blockchain.

### *4.3. Phase-3: Consensus Mechanism*

Phase-3 is pivotal in the blockchain-based IoT system, focusing on the consensus mechanism to validate and authenticate data. This phase is crucial in ensuring the integrity and trustworthiness of the data recorded on the blockchain. Algorithm 3 outlines this process, detailing the steps from distributed verification by nodes to the creation of a new block on the blockchain. It encapsulates the collaborative effort of verification nodes in achieving consensus, the implementation of the proof of authority mechanism for reliable validation, and the final block creation, which solidifies the data's place in the blockchain ledger. This algorithm is a cornerstone in maintaining the system's security and reliability.

**Algorithm 3** Consensus Mechanism

**Input:** Data, metadata, verification nodes
**Output:** New block added to blockchain

1: **for** each verification node **do**
2: Participate in validating data authenticity
3: **end for**
4: Reach consensus among nodes on data authenticity using PoA
5: Create new block with:
- Data
- Associated metadata

6: Add new block to blockchain

#### 4.3.1. Distributed Verification by Verification Nodes

In this step, multiple verification nodes scattered across the network collaboratively participate in the process of validating the data's authenticity. These nodes, being distributed, bring in a decentralized approach to verification, enhancing the system's resilience against single points of failure or malicious attacks. Each node independently verifies the data and their associated metadata. Once the majority of these nodes reach a consensus on the data's authenticity, the data are deemed verified. This distributed verification ensures a robust and trustworthy validation process, reinforcing the system's overall security and integrity.

#### 4.3.2. Data Authenticity Check

This step involves a collective consensus mechanism where the verification nodes collaboratively determine the genuineness of the data. After individual verification by distributed nodes, they communicate their findings to reach a common agreement. If a majority consensus is achieved that the data are authentic and have not been tampered with, they are approved for further processing. This collective decision making ensures that the data's integrity is maintained, safeguarding the system from potential data breaches or malicious alterations.

#### 4.3.3. Proof of Authority (PoA) Consensus

In the PoA consensus mechanism, a set of trusted validators are chosen to create new blocks and validate transactions. Unlike proof of work (PoW) or proof of stake (PoS), PoA relies on the reputation of these validators, making it more energy-efficient and faster. Validators are pre-approved, and their authority comes from their identity and reputation. If they act maliciously, they stand to lose their validating rights and reputation. In this proposed system, PoA ensures that only legitimate and verified transactions (like data entries from IoT devices) are added to the blockchain, enhancing its security and trustworthiness [19].

Compared to public blockchains that use PoW or PoS, our private blockchain with PoA offers several advantages for IoT applications. Firstly, it significantly improves the energy efficiency, as the intensive computational mining process associated with PoW is

not required. This is particularly beneficial for IoT scenarios, where devices often have limited power resources.

In terms of transaction speeds, the private blockchain with PoA provides faster processing times due to the reduced number of nodes involved in the consensus process. This is crucial for IoT networks that require real-time data processing and rapid decision making.

Furthermore, the private nature of the blockchain ensures a higher level of security and control over the network. It reduces the risk of external attacks and allows for the better management of those who participate in the network. This controlled environment is ideal for IoT applications that often deal with sensitive data.

While PoS also offers improvements in energy efficiency, the combination of a private blockchain with PoA is chosen for its ability to provide faster transaction validations, lower latency, and enhanced security controls, aligning with the specific requirements of IoT networks.

#### 4.3.4. Block Creation

Once a consensus is achieved through the PoA mechanism, the next step is the formation of a new block. This block encapsulates the validated data or transactions, along with metadata like timestamps and references to previous blocks. After its creation, the block undergoes cryptographic hashing, producing a unique block hash. This hash, along with the block's content, ensures data integrity and immutability. The newly formed block is then appended to the blockchain, establishing a chronological and tamper-proof record of the data.

### *4.4. Phase-4: IoT Device Access on Private Blockchain*

Phase-4 is the culminating stage of the blockchain-based IoT system, focusing on the interaction between IoT devices and the blockchain. This phase is crucial in ensuring secure and efficient data access. Algorithm 4 provides a comprehensive overview of this phase, illustrating the sequence of events from an IoT device's data request to the final data retrieval and transmission. It encompasses the steps of request initiation, gateway processing, ZKP challenge generation and response, and the final data transmission, all underpinned by advanced security and efficiency measures. This algorithm is integral in detailing the secure and streamlined communication between IoT devices and the blockchain gateway, ensuring data integrity and accessibility.

**Algorithm 4** IoT Device Access on Private Blockchain

**Input:** Data request from IoT device, gateway, ZKP challenge
**Output:** Requested data transmitted to IoT device

```
IoT device sends data request to gateway
Gateway processes request and retrieves data
Gateway generates ZKP challenge
IoT device responds to ZKP challenge
if ZKP response is valid then
    Gateway retrieves requested data
    Transmit data to IoT device
    Apply rate limits and caching mechanisms
    Use intelligent algorithms for data access and caching
end if
```

#### 4.4.1. IoT Device Initiates Request to Gateway

IoT devices, equipped with sensors and connected to the network, have the capability to request specific data or information. When an IoT device needs data, it sends a structured request to the private blockchain gateway. This request typically contains details about the type of data needed, any specific timeframes or parameters, and authentication credentials

to verify the device's identity. The gateway, upon receiving this request, initiates processes to validate the device's authenticity and retrieve the requested data. Algorithm 4 shows the Phase-4 process.

#### 4.4.2. Gateway Processes the Request

Upon receiving a data request from an IoT device, the private blockchain gateway initiates a series of actions. First, it validates the authenticity of the requesting device using stored credentials or cryptographic methods. Once the device is authenticated, the gateway parses the request to understand the specific data or information required. Using this parsed information, the gateway then interacts with the underlying blockchain infrastructure or other integrated systems to retrieve the relevant data. Throughout this process, the gateway ensures that the data access policies are adhered to, ensuring that only authorized devices receive the appropriate data.

#### 4.4.3. ZKP Challenge Generation and Caching

In this step, the private blockchain gateway employs the ZKP cryptographic technique to bolster the security measures, as illustrated in Figure 2. This method allows the gateway, acting as the verifier, to ascertain that the requesting IoT device, the prover, possesses specific credentials without demanding the direct disclosure of said credentials. By sending a ZKP challenge to the IoT device, the gateway ensures that only those devices with the correct knowledge can respond accurately. This meticulous challenge response mechanism effectively bars unauthorized entities from accessing the data. Additionally, to enhance the efficiency, successful ZKP challenges and their corresponding responses are cached for future verifications [17].

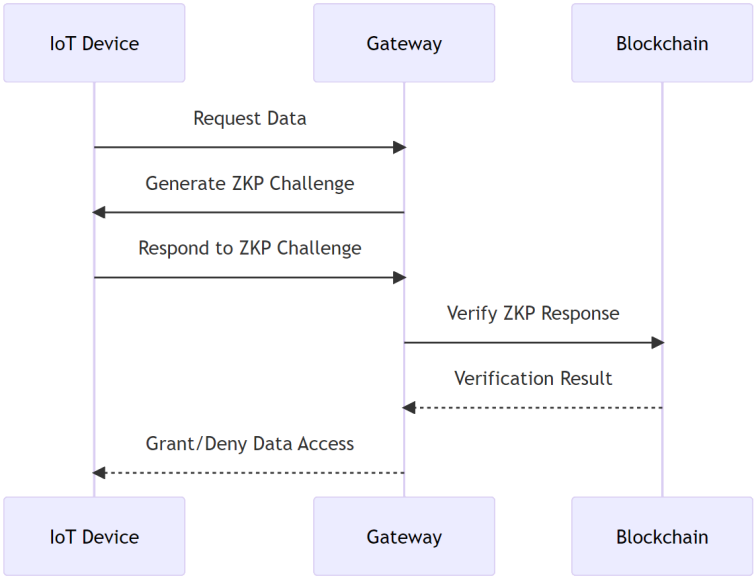


**Figure 2.** ZKP challenge generation and caching process.

#### 4.4.4. IoT Device Responds to the Challenge

Upon receiving the ZKP challenge from the private blockchain gateway, the IoT device, acting as the prover, formulates a response based on its credentials and the knowledge that it possesses. This response is constructed in such a manner that it demonstrates the device's authenticity and right to access the requested data without revealing any sensitive or private information. The formulated response is then transmitted back to the gateway for verification. This interaction ensures that only legitimate and authorized devices can proceed further in the data retrieval process.

#### 4.4.5. Gateway Verifies the ZKP Response

Once the private blockchain gateway receives the response to the ZKP challenge from the IoT device, it proceeds to verify the validity of the response. Utilizing the properties of ZKP, the gateway, acting as the verifier, determines whether the IoT device possesses the correct credentials and knowledge without gaining insights into the actual data or content held by the device. If the response is verified successfully, it confirms the device's authenticity and authorization to access the requested data. On the other hand, if the verification fails, the device's request is denied, ensuring that only authenticated devices gain access to the data.

#### 4.4.6. Data Retrieval and Transmission

Upon successful verification of the IoT device's authenticity through the ZKP response, the private blockchain gateway initiates the data retrieval process. It searches the blockchain for the specific data or transaction records requested by the IoT device. Once located, the data are extracted and prepared for transmission. The gateway ensures that the data are packaged appropriately, maintaining their integrity and security. Subsequently, the packaged data are transmitted to the requesting IoT device, allowing it to access the information that it seeks. Throughout this process, the gateway ensures efficient and secure data transfer, prioritizing the confidentiality and accuracy of the transmitted data.

#### 4.4.7. Rate Limiting and Caching

To manage the flow of data and prevent potential system overloads, the private blockchain gateway employs a rate-limiting mechanism. This ensures that data requests from IoT devices are processed at a controlled pace, preventing any single device or group of devices from overwhelming the system with excessive requests in a short timeframe. Concurrently, the gateway utilizes caching techniques to store frequently accessed data. By keeping a temporary storage or "cache" of these data, the gateway can swiftly respond to recurring requests without repeatedly querying the blockchain. This not only speeds up the data retrieval process but also reduces the computational load on the blockchain, enhancing the overall system efficiency and responsiveness [24].

#### 4.4.8. Intelligent Data Access and Caching for IoT Devices

The private blockchain gateway incorporates advanced algorithms designed to optimize data access for IoT devices. Recognizing the patterns and frequency of data requests from specific devices, the gateway intelligently determines which data sets to cache and which to fetch in real time. By predicting the data needs of IoT devices based on historical access patterns, the gateway can pre-emptively cache data that are likely to be requested soon. This proactive approach ensures that IoT devices receive the data that they need with minimal latency. Furthermore, by reducing unnecessary data fetches from the blockchain, the system conserves computational resources, ensuring a smoother and more efficient operation.

### *4.5. Underlying Mathematical Principles*

This section outlines the key mathematical principles underpinning our proposed system, elucidating how these concepts are integral to ensuring the security, efficiency, and scalability of the blockchain-integrated IoT network.

#### 4.5.1. Hash Function

The hash function $H$ is fundamental to the blockchain's data integrity, converting variable-sized input data $x$ into a fixed-size hash $y$. In our system, hash functions validate the immutability of records by hashing each transaction or data block to produce a unique fingerprint $H(x) = y$. This mechanism is critical for data integrity verification during consensus and for linking blocks in the blockchain through their hashes.

#### 4.5.2. Elliptic Curve Cryptography (ECC)

Elliptic curve cryptography (ECC) provides a secure framework for communication within our blockchain network. The elliptic curve equation $y^2 = x^3 + ax + b$ is used to generate public–private key pairs, crucial for data encryption and decryption. ECC is employed for transaction signing, enabling authentication and non-repudiation through a signature verifiable by the corresponding public key.

#### 4.5.3. Zero Knowledge Proof (ZKP)

Zero Knowledge Proof enables transactions or data validation without revealing the content, thus maintaining privacy and security [17,18]. Our system utilizes ZKP where a prover $P$ can demonstrate the knowledge of a secret $x$ corresponding to a statement $S$ without disclosing $x$. This is particularly advantageous for IoT devices that need to authenticate themselves to access services without compromising sensitive information. The interaction can be represented as

$$P(x) \rightarrow V : \text{“I know x such that S(x) is true”}$$

$$V \rightarrow P : \text{“Prove it without revealing x”}$$

#### 4.5.4. Consensus Mechanism—Proof of Authority (PoA)

PoA is a consensus mechanism that relies on a limited number of trusted validators $V$ to maintain the network's integrity and security. Each validator $v$ is assigned a trust score, which reflects their reliability and reputation within the network. The probability $P(v)$ that a validator will be chosen to create a new block is directly proportional to their trust score, ensuring that the most reputable validators have a higher chance of being selected. This system is designed to be efficient and less resource-intensive compared to proof of work, making it well suited for private blockchain networks where validators are known and trusted entities [19,25].

The selection probability for a validator $v$ in PoA can be mathematically represented as

$$P(v) = \frac{\text{Trust Score of } v}{\sum_{i=1}^{n} \text{Trust Score of } V_i}$$

where $n$ is the total number of validators in the network. This formula ensures that the selection process is fair and weighted according to the trustworthiness of each validator.

#### 4.5.5. Sharding

Sharding is a database partitioning technique in blockchain technology that enhances the network scalability. By dividing the blockchain into smaller segments, known as shards, each is capable of processing transactions independently. This division allows for parallel transaction processing, which significantly increases the network's capacity to handle a larger volume of transactions and improves the overall system performance. The number of nodes per shard, on average, is determined by the ratio of the total number of nodes $N$ to the number of shards $s$, expressed as $\frac{N}{s}$. This distribution of nodes across shards is instrumental in facilitating a more efficient validation process by leveraging parallel computing within the blockchain [23].

#### 4.5.6. Lightweight Compression

Lightweight compression algorithms are crucial in efficiently managing the large volumes of data from IoT devices. The compression ratio $R$, defined as $R = D_o/D_c$, measures the reduction from the original data size $D_o$ to the compressed size $D_c$, facilitating the handling of data on bandwidth-constrained networks.

#### 4.5.7. Rate Limiting

Rate limiting is a critical control mechanism that ensures the stability and responsiveness of the network by preventing congestion. It achieves this by setting a maximum allowable rate of data transmission, denoted as $R_{\text{max}}$, which serves as a threshold. The actual rate of data transmission, $R_{\text{actual}}$, is continuously monitored and compared against this threshold. The lower of the two values is then used to regulate the data flow, thereby maintaining optimal network performance even under high demands. This strategy is vital in preserving the quality of service across the system.

The rate limiting mechanism is mathematically expressed as follows:

$$\text{Data Transmission} = \min(R_{\text{max}}, R_{\text{actual}})$$

where $R_{\text{max}}$ is the predefined maximum rate of data transmission that the network can handle, and $R_{\text{actual}}$ is the current rate at which data are being transmitted. This ensures that the network operates within its capacity limits, thus preventing overload and ensuring fair resource allocation among users.

## 5. Discussion

This section delves into the various aspects of our proposed system, examining its unique features, addressing its limitations, and exploring its practical implications and potential use cases. We also present the results of our performance evaluation, providing insights into the system's efficiency and scalability.

### *5.1. Features of the Proposed System*

The proposed system, designed to fortify Industrial IoT networks using blockchain technology, boasts a range of distinctive features. These include real-time data collection and processing, where sensor nodes are equipped to collect data in real time, and, with the integration of lightweight compression algorithms, the data are efficiently processed for transmission. It ensures efficient data transmission by employing priority-based data transmission, ensuring that critical data are transmitted to the private blockchain gateway promptly. The system also leverages certificate caching, so that local aggregators can cache previously received certificates, reducing the need for constant communication with the CA. Furthermore, it uses advanced encryption, encrypting data with the ChaCha20-Poly1305 algorithm to ensure confidentiality during transmission [22]. An added layer of security is provided through ZKP integration, ensuring that only authorized IoT devices can access the data. Depending on the data's confidentiality, they are either stored in a cloud server or uploaded directly to the IPFS, ensuring decentralized and secure data storage. The system also employs intelligent sharding and adaptive rate limiting, using dynamic sharding algorithms and adaptive rate limits to efficiently allocate and process the incoming data [23]. Lastly, for IoT devices accessing data, the system employs smart algorithms to determine which data to cache and which to retrieve in real time, ensuring optimized data retrieval [15].

Table 3 serves as a comparative analysis between the proposed methodology and existing systems across various criteria crucial to Industrial IoT networks integrated with blockchain technology. It succinctly outlines the advancements of the proposed system, emphasizing its superiority in aspects like data collection, compression, and security. The proposed methodology showcases significant improvements in efficiency and security through advanced features like edge computing, sophisticated data compression algorithms, and enhanced encryption methods like ChaCha20-Poly1305. It also introduces innovative approaches in certificate handling and data verification, employing machine learning and distributed node verification for better scalability and security. Furthermore, the integration of the IPFS for data storage and the adoption of the proof of authority consensus mechanism highlight the system's focus on decentralized, energy-efficient operations. Finally, the use of Zero Knowledge Proof for IoT device access underscores a

strong commitment to data privacy and security. Overall, the table effectively contrasts the proposed system's cutting-edge features with the limitations of existing systems, underscoring the comprehensive enhancements that it brings to the realm of IoT and blockchain integration.

**Table 3.** Comparison between proposed methodology and existing systems.

| Criteria | Proposed Methodology | Existing System | Remarks |
| --- | --- | --- | --- |
| Data Collection | Utilizes sensor nodes with edge computing capabilities.<br>Achieves efficient data collection with reduced latency. | Relies on centralized data collection, leading to potential bottlenecks [26].<br>Exhibits higher latency and inefficiency due to centralized processing. | Edge computing enhances efficiency by distributing processing. |
| Data Compression | Employs advanced algorithms for optimal data size reduction.<br>Facilitates faster and more efficient data transmission. | Uses basic compression methods with limited effectiveness [27].<br>Results in slower data transmission due to basic compression. | Advanced algorithms improve transmission efficiency. |
| Certificate Handling | Implements certificate caching to minimize validation times.<br>Uses machine learning for efficient CA validation. | Requires frequent CA validations due to lack of caching [28].<br>Depends on slower traditional CA validation processes. | Caching and ML for CA validation enhance security and efficiency. |
| Encryption | Adopts ChaCha20-Poly1305 for high-security encryption.<br>Ensures strong security and data integrity during transmission. | Employs standard encryption methods with potential vulnerabilities [29].<br>Faces challenges in maintaining data integrity and security. | ChaCha20-Poly1305 ensures enhanced security. |
| Verification | Enables parallel verification through distributed nodes.<br>Offers a secure and scalable verification process. | Centralized verification creates scalability and security issues [30].<br>Suffers from security and scalability limitations. | Parallel verification enhances security and scalability. |
| Data Storage | Integrates IPFS for decentralized storage with blockchain indexing.<br>Differentiates data storage based on confidentiality. | Utilizes centralized cloud storage, posing risks of single points of failure [31].<br>Does not differentiate, leading to potential security risks. | IPFS provides secure and decentralized storage. |
| Consensus Mechanism | Employs proof of authority for efficient consensus.<br>Ensures rapid validation with less energy use. | Uses proof of work, known for high energy consumption.<br>Consumes more energy and has slower validation times. | PoA is more energy-efficient than PoW. |
| IoT Device Access | Utilizes Zero Knowledge Proof for secure data access.<br>Enhances privacy and security for data access. | Lacks ZKP implementation, leading to security concerns [32].<br>Exposes data access to security vulnerabilities. | ZKP significantly improves data privacy and security. |

### *5.2. Limitations*

The integration of blockchain technology with IoT systems offers numerous advantages but also presents several challenges that must be addressed. One of the primary concerns is scalability; as the number of IoT devices within a network grows, the blockchain's size and the volume of transactions can increase exponentially. This surge has the potential to impact the transaction verification times adversely, leading to scalability issues that could hinder the system's ability to expand efficiently.

To address the scalability challenges in blockchain–IoT integration, several strategies can be considered. Implementing efficient blockchain algorithms and data structures, such as proof of stake (PoS) or delegated proof of stake (DPoS), can alow the system to handle larger transaction volumes more effectively than traditional proof of work (PoW) systems. Off-chain solutions like state channels or sidechains can also alleviate the load on the main blockchain by processing transactions externally. Additionally, integrating blockchain with edge computing can decentralize data processing, reducing the data transmission needs and enhancing the scalability.

Furthermore, the proof of authority (PoA) consensus mechanism, utilized in our proposed system, offers a viable solution. PoA, by relying on a limited number of trusted validators, streamlines the validation process, making it more efficient and less resource-intensive. This approach is particularly suitable for private blockchain networks where scalability and speed are critical. These strategies, while not exhaustive, provide a foundation for the overcoming of scalability challenges in the dynamic field of blockchain and IoT.

Another significant challenge is latency [33]. The blockchain verification process, despite being optimized with strategies such as data compression and priority-based transmission, still introduces an inherent delay. This latency can be at odds with the real-time operational requirements that are often essential in IoT applications, where immediate data processing and action are critical.

The complexity of implementing a blockchain–IoT integrated system cannot be understated. It requires a combination of expertise in both blockchain technology and IoT infrastructure, which can be a formidable barrier for organizations that lack the necessary technical resources. This complexity can slow down or even deter the adoption of blockchain in IoT applications.

Interoperability also poses a substantial challenge. The current landscape lacks standardized protocols, making it difficult to ensure that a blockchain–IoT system can seamlessly integrate with a wide array of IoT infrastructures and other blockchain solutions. This lack of standardization can lead to fragmented systems that are unable to communicate and work together effectively [34].

To enhance the interoperability in blockchain–IoT systems, a focused approach towards developing and adopting standardized protocols is essential. This involves collaborative efforts among industry stakeholders to establish universal standards that enable seamless integration across diverse blockchain platforms and IoT infrastructures. Such standardization would facilitate effective communication and interoperability, preventing fragmentation and ensuring cohesive functionality. Additionally, exploring adaptable middleware solutions that can act as intermediaries between different systems could provide a practical way to achieve interoperability in the absence of universal standards. These efforts are crucial in creating a harmonized blockchain–IoT ecosystem capable of supporting a wide range of applications and technologies.

Lastly, the increased computational demand of the proposed blockchain enhancements for IoT applications is a critical issue. These enhancements may require more computational power than what existing IoT devices can provide, making them impractical for deployment on current systems. This limitation is particularly concerning as it directly affects the feasibility of implementing such a system in real-world scenarios. It is an aspect that not only needs to be acknowledged in the conclusions of any discussion on the topic but also requires careful consideration and planning for the practical application of blockchain technology in the IoT domain [5,34].

Future research in the realm of blockchain–IoT integration should focus on several key areas. Enhancing scalability is paramount, possibly through the development of more efficient blockchain algorithms and data structures to handle large transaction volumes. Reducing the latency to meet real-time IoT requirements is another critical area, potentially involving the optimization of blockchain verification processes or the exploration of faster consensus mechanisms. Additionally, inspired by [35], integrating hardware-based

security measures such as secure elements and Trusted Execution Environments (TEEs) can significantly bolster the security of IoT devices within the blockchain network. These hardware solutions provide a robust platform for cryptographic operations and secure storage, addressing the physical and logical vulnerabilities in IoT devices. A deeper understanding of the security provided by TEEs, as elaborated in [36], underscores their potential in safeguarding sensitive operations and data against various threats, while also acknowledging the need to address their inherent vulnerabilities and attack vectors. The insights from [37] into the vulnerabilities of wireless communication protocols in IoT devices underline the importance of securing not only the blockchain layer but also the communication channels, emphasizing a holistic approach to IoT security. Simplifying the complexity of blockchain–IoT system implementation is also essential, calling for user-friendly integration solutions that cater to varying technical expertise levels. Addressing interoperability challenges through standardized protocols and interfaces will be crucial for seamless integration across diverse IoT infrastructures and blockchain systems. The computational demands of blockchain enhancements in IoT applications necessitate the development of IoT devices capable of handling lightweight processes such as data compression and basic cryptographic functions. This advancement would enable more efficient, low-power IoT devices with enhanced processing capabilities, facilitating smoother blockchain integration. Lastly, exploring the synergy of emerging technologies like edge computing and artificial intelligence with blockchain and IoT could lead to innovative and practical applications, further enhancing the efficiency, security, and scalability of IoT networks [38].

### *5.3. Practical Implications and Use Cases*

The proposed system offers several practical implications. It promises enhanced data security by integrating blockchain with IoT, ensuring that data remain tamper-proof, crucial for industries like healthcare or aviation. Its decentralized nature means that it offers scalability, handling increased data flows as IoT devices grow in a network, without a direct increase in costs or complexity. Operational efficiency is also highlighted with features like lightweight compression and priority-based transmission, leading to faster data processing and transmission for quicker real-time decision making. Moreover, the system can result in cost savings by reducing the need for centralized data storage and processing centers and optimizing data transmission. An additional layer of privacy is introduced through the use of ZKP, ensuring that data can be verified without revealing their contents [17,18].

Beyond these implications, the proposed system finds relevance in various real-world scenarios or use cases. In smart factories, machinery and equipment are interconnected, allowing the system to monitor machine health, predict maintenance needs, and even halt operations when a potential fault is detected. It is applicable in precision agriculture, where farmers deploy sensors across fields to monitor conditions, securely transmitting and processing data to inform timely decisions on irrigation, fertilization, and harvesting. The healthcare sector can benefit, especially in hospitals where IoT devices monitor patient health in real time, ensuring data security and patient privacy. The system proves beneficial for supply chain management, tracking products in real time through the supply chain, guaranteeing data accuracy and integrity, and enhancing trust among suppliers, distributors, and consumers. Lastly, as cities advance towards interconnectivity, the system can cater to smart cities, managing data from various sources like traffic lights, public transport, and utilities, ensuring smooth city operations and prompt responses in emergencies.

### *5.4. Results*

The testing environment for this study was primarily set up on Google Colab, a cloud-based Python programming environment that offers a versatile platform for the simulation of an IoT-based blockchain network. The simulation involved Python (Version 3.10.6, Python Software Foundation, Wilmington, DE, USA) scripts designed to mimic the behavior of sensor nodes, local aggregators, distributed nodes, and a private blockchain gateway. The network

topology and the event-driven simulation of the IoT environment were facilitated using Python libraries such as networkx and simpy. This setup allowed for a realistic representation of the data flow and processing within the proposed system.

In assessing our system's performance, we focused on key metrics such as the data size, compression efficiency, transmission times, and processing latency, as detailed in Table 4. These metrics are instrumental in understanding how our system responds to varying data loads, highlighting its scalability and efficiency. Notably, as the data size increased from 10 KB to 100 KB, we observed a corresponding rise in the transmission times and processing latencies. However, our system's design, which integrates parallel processing and intelligent data management, effectively managed these increases.

**Table 4.** Performance evaluation of the proposed system.

| Data Size | Size After Compression | Transmission Time to Local Aggregator (ms) | Data Processing Latency at Aggregators (ms) | Transmission Time to Distributed Nodes (ms) | Data Processing Latency at Distributed Nodes (ms) | Transmission Time to Gateway (ms) |
|---|---|---|---|---|---|---|
| 10 KB | 2.5 KB | 5.102 | 8.256 | 15.314 | 20.478 | 18.589 |
| 20 KB | 5 KB | 7.189 | 10.342 | 18.467 | 25.531 | 22.674 |
| 50 KB | 12.5 KB | 10.478 | 13.589 | 22.643 | 30.756 | 28.812 |
| 100 KB | 25 KB | 15.867 | 18.932 | 30.987 | 35.104 | 35.219 |

This demonstrates the system's capability to efficiently handle larger data volumes, a critical aspect for real-world IoT applications.

The effectiveness of our lightweight compression algorithm was evident in the significant reduction in the data size, which in turn reduced the transmission time to the local aggregator. Additionally, the processing latencies at both the aggregators and distributed nodes were efficiently managed, showcasing the system's adeptness in data verification, decryption, and decompression.

Overall, this comprehensive evaluation in a controlled testing environment offers valuable insights into the system's performance, underscoring its potential for practical application in IoT scenarios, where managing large volumes of data with speed and efficiency is paramount.

## 6. Conclusions

This research contributes to the evolving field of integrating IoT with blockchain technology, addressing key challenges in security, integrity, and privacy for extensive interconnected systems. Our methodology enhances the data flow from sensor nodes to a private blockchain gateway, incorporating cryptographic safeguards and consensus mechanisms aimed at improving security.

The implementation of Zero Knowledge Proof (ZKP) and decentralized federated learning in our framework represents an effort to enhance security, with a focus on limiting data access to authorized entities. While our blockchain-centric approach shows promise, it is part of a broader, ongoing exploration to meet the comprehensive security needs of IoT networks.

In terms of performance, our system shows promising results that suggest potential improvements over existing models in data handling and security. The performance metrics, as outlined in Table 4, indicate an improvement in efficiency for data transmission and processing. This observed efficiency may be attributed to the implementation of optimized data compression and parallel processing techniques. These features are particularly relevant in managing large data volumes in real-world IoT applications, although further comparative studies would be beneficial to confirm these initial findings.

Looking ahead, future research will delve into integrating hardware-based solutions alongside our software-based security measures, aiming to forge a more robust and resilient system. Acknowledging the increased computational demands of our proposed enhancements, our focus will shift towards optimizing the computational efficiency of

cryptographic techniques and exploring the adaptability of existing IoT devices to these enhancements. Moreover, as IoT technology continues to evolve, it is conceivable that future IoT devices will inherently meet the computational needs required for such advanced security measures. This research represents a step in an ongoing journey towards developing more secure, efficient, and reliable IoT networks, underscoring the necessity for continuous innovation and adaptation in this dynamic field.

**Author Contributions:** Conceptualization, Y.B. and G.N.; methodology, G.N., I.C. and M.J.; software, G.N.; validation, G.N., M.J., D.P. and I.C.; formal analysis, G.N.; investigation, Y.B. and M.J.; resources, G.N.; data curation, G.N., R.S.P.R. and I.C.; writing—original draft preparation, G.N. and Y.B.; writing—review and editing, G.N., Y.B., M.J., D.P. and I.C.; supervision, R.S.P.R., I.C. and D.P.; project administration, R.S.P.R. and I.C.; funding acquisition, I.C. and D.P. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** Data are conteined within the article.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Idrees, S.; Nowostawski, M.; Jameel, R.; Mourya, A. Security Aspects of Blockchain Technology Intended for Industrial Applications. *Electronics* **2021**, *10*, 951. [CrossRef]
2. Saxena, S.; Bhushan, B.; Ahad, M. Blockchain based solutions to secure IoT: Background, integration trends and a way forward. *J. Netw. Comput. Appl.* **2021**, *181*, 103050. [CrossRef]
3. Bhutta, M.N.M.; Khwaja, A.A.; Nadeem, A.; Ahmad, H.F.; Khan, M.K.; Hanif, M.A.; Song, H.; Alshamari, M.; Cao, Y. A Survey on Blockchain Technology: Evolution, Architecture and Security. *IEEE Access* **2021**, *9*, 61048–61073. [CrossRef]
4. Christidis, K.; Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
5. Sadawi, A.A.; Hassan, M.S.; Ndiaye, M. A Survey on the Integration of Blockchain with IoT to Enhance Performance and Eliminate Challenges. *IEEE Access* **2021**, *9*, 54478–54497. [CrossRef]
6. Ouaddah, A.; Elkalam, A.; Ouahman, A. FairAccess: A new Blockchain-based access control framework for the Internet of Things: FairAccess: A new access control framework for IoT. *Secur. Commun. Netw.* **2017**, *9*, 5943–5964. [CrossRef]
7. Wang, H.; He, D.; Yu, J.; Xiong, N.N.; Wu, B. RDIC: A blockchain-based remote data integrity checking scheme for IoT in 5G networks. *J. Parallel Distrib. Comput.* **2021**, *152*, 1–10. [CrossRef]
8. Rane, S.B.; Narvel, Y.A.M. Data-driven decision making with Blockchain-IoT integrated architecture: A project resource management agility perspective of industry 4.0. *Int. J. Syst. Assur. Eng. Manag.* **2022**, *13*, 1005–1023. [CrossRef]
9. Ma, N.; Waegel, A.; Hakkarainen, M.; Braham, W.W.; Glass, L.; Aviv, D. Blockchain + IoT sensor network to measure, evaluate and incentivize personal environmental accounting and efficient energy use in indoor spaces. *Appl. Energy* **2023**, *332*, 120443. [CrossRef]
10. Farahani, F.; Firouzi, F.; Luecking, M. The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. *J. Netw. Comput. Appl.* **2021**, *177*, 102936. [CrossRef]
11. Alrubei, S.M.; Ball, E.; Rigelsford, J.M. A Secure Blockchain Platform for Supporting AI-Enabled IoT Applications at the Edge Layer. *IEEE Access* **2022**, *10*, 18583–18595. [CrossRef]
12. Sun, S.; Du, R.; Chen, S.; Li, W. Blockchain-Based IoT Access Control System: Towards Security, Lightweight, and Cross-Domain. *IEEE Access* **2021**, *9*, 36868–36878. [CrossRef]
13. Bataineh, M.R.; Mardini, W.; Khamayseh, Y.M.; Yassein, M.M.B. Novel and Secure Blockchain Framework for Health Applications in IoT. *IEEE Access* **2022**, *10*, 14914–14926. [CrossRef]
14. Chatamoni, A.; Bhukya, R. Lightweight Compressive Sensing for Joint Compression and Encryption of Sensor Data. *Int. J. Eng. Technol. Innov.* **2022**, *12*, 167–181. [CrossRef]
15. Mathur, S.; Kalla, A.; Gür, G.; Bohra, M.; Liyanage, M. A Survey on Role of Blockchain for IoT: Applications and Technical Aspects. *Comput. Netw.* **2023**, *227*, 109726. [CrossRef]
16. Daniel, E.; Tschorsch, F. IPFS and Friends: A Qualitative Comparison of Next Generation Peer-to-Peer Data Networks. *IEEE Commun. Surv. Tutorials* **2022**, *24*, 31–52. [CrossRef]
17. Chi, P.-W.; Lu, Y.-H.; Guan, A. A Privacy-Preserving Zero-Knowledge Proof for Blockchain. *IEEE Access* **2023**, *11*, 85108–85117. [CrossRef]
18. Sun, X.; Yu, F.R.; Zhang, P.; Sun, Z.; Xie, W.; Peng, X. A Survey on Zero-Knowledge Proof in Blockchain. *IEEE Netw.* **2021**, *35*, 198–205. [CrossRef]
19. Lashkari, B.; Musilek, P. A Comprehensive Review of Blockchain Consensus Mechanisms. *IEEE Access* **2021**, *9*, 43620–43652. [CrossRef]

20. Kadhim, A.; Manaa, M. Improving IoT data Security Using Compression and Lightweight Encryption Technique. In Proceedings of the 2022 5th International Conference on Engineering Technology and Its Applications (IICETA), Al-Najaf, Iraq, 31 May–1 June 2022; pp. 187–192. [CrossRef]
21. Philip, M.A.; Vaithiyanathan. A survey on lightweight ciphers for IoT devices. In Proceedings of the 2017 International Conference on Technological Advancements in Power and Energy (TAP Energy), Kollam, India, 21–23 December 2017; pp. 1–4.
22. Serrano, R.; Duran, C.; Sarmiento, M.; Pham, C.-K.; Hoang, T.-T. ChaCha20–Poly1305 Authenticated Encryption with Additional Data for Transport Layer Security 1.3. *Cryptography* **2022**, *6*, 30. [CrossRef]
23. Yu, G.; Wang, X.; Yu, K.; Ni, W.; Zhang, J.A.; Liu, R.P. Survey: Sharding in Blockchains. *IEEE Access* **2020**, *8*, 14155–14181. [CrossRef]
24. Fu, S.; Zhao, L.; Ling, X.; Zhang, H. Maximizing the System Energy Efficiency in the Blockchain Based Internet of Things. In Proceedings of the ICC 2019—2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6. [CrossRef]
25. Guru, A.; Mohanta, B.K.; Mohapatra, H.; Al-Turjman, F.; Altrjman, C.; Yadav, A. A Survey on Consensus Protocols and Attacks on Blockchain Technology. *Appl. Sci.* **2023**, *13*, 2604. [CrossRef]
26. Goyat, R.; Kumar, G.; Alazab, M.; Conti, M.; Rai, M.; Thomas, R.; Saha, R.; Kim, T. Blockchain-Based Data Storage with Privacy and Authentication in Internet of Things. *IEEE Internet Things J.* **2022**, *9*, 14203–14215. [CrossRef]
27. Kim, T.; Noh, J.; Cho, S. SCC: Storage Compression Consensus for Blockchain in Lightweight IoT Network. In Proceedings of the 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 11–13 January 2019; pp. 1–4. [CrossRef]
28. Xu, S.; Li, Y.; Deng, R.; Zhang, Y.; Luo, X.; Liu, X. Lightweight and Expressive Fine-Grained Access Control for Healthcare Internet-of-Things. *IEEE Trans. Cloud Comput.* **2022**, *10*, 474–490. [CrossRef]
29. Karthikeyan, S.; Poongodi, T. Secured Data Compression and Data Authentication in Internet of Thing Networks Using LZW Compression Based X.509 Certification. In Proceedings of the 2022 IEEE International Conference on Data Science and Information System (ICDSIS), Hassan, India, 29–30 July 2022; pp. 1–5. [CrossRef]
30. Zhang, Y.; He, D.; Choo, K. BaDS: Blockchain-Based Architecture for Data Sharing with ABS and CP-ABE in IoT. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 2783658:1–2783658:9. [CrossRef]
31. Hameed, S.; Shah, S.; Saeed, Q.; Siddiqui, S.; Ali, I.; Vedeshin, A.; Draheim, D. A Scalable Key and Trust Management Solution for IoT Sensors Using SDN and Blockchain Technology. *IEEE Sens. J.* **2021**, *21*, 8716–8733. [CrossRef]
32. Gupta, R.; Garg, R. Mobile Applications Modelling and Security Handling in Cloud-Centric Internet of Things. In Proceedings of the 2015 Second International Conference on Advances in Computing and Communication Engineering, Dehradun, India, 1–2 May 2015; pp. 285–290. [CrossRef]
33. Alfa, A.; Alhassan, J.; Olaniyi, O.; Olalere, M. Blockchain technology in IoT systems: Current trends, methodology, problems, applications, and future directions. *J. Reliab. Intell. Environ.* **2020**, *7*, 115–143. [CrossRef]
34. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. A survey on the adoption of blockchain in IoT: Challenges and solutions. *Blockchain Res. Appl.* **2021**, *2*, 100006. [CrossRef]
35. Muñoz, A.; Farao, A.; Correia, J.R.C.; Xenakis, C. P2ISE: Preserving Project Integrity in CI/CD Based on Secure Elements. *Information* **2021**, *12*, 357. [CrossRef]
36. Muñoz, A.; Rios, R.; Roman, R.; Lopez, J. A survey on the (in)security of Trusted Execution Environments. *Comput. Secur.* **2023**, *129*, 103180. [CrossRef]
37. Muñoz, A.; Fernandez Gago, C.; López-Villa, R. A Test Environment for Wireless Hacking in Domestic IoT Scenarios. *Mob. Netw. Appl.* **2022**, *1*, 1–10. [CrossRef]
38. Prabadevi, B.; Deepa, N.; Pham, Q.; Nguyen, D.; Maddikunta, P.; Reddy, G.; Pathirana, P.; Dobre, O. Toward Blockchain for Edge-of-Things: A New Paradigm, Opportunities, and Future Directions. *IEEE Internet Things Mag.* **2021**, *4*, 102–108. [CrossRef]