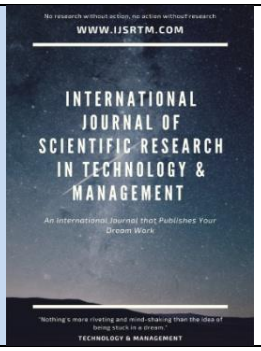
IJSRTM
https://www.ijsrtm.com
Vol. 6 Issue 1 January 2026: 15-21
Published online 09 Jan 2026
E-ISSN: 2583-7141

International Journal of Scientific Research in Technology & Management




# AI-Driven Zero-Trust Blockchain Framework for Secure and Scalable IoT Data Sharing

Niharika Sarathe
*Dept. of Computer Science and Engineering*
*Oriental Institute of Science and Technology*
Bhopal, Madhya Pradesh, India
saratheniharika98@gmail.com

Nikha Yadav
*Dept. of Computer Science and Engineering*
*Oriental Institute of Science and Technology*
Bhopal, Madhya Pradesh, India
nikhayadav820@gmail.com

Monu Kumar
*Dept. of Computer Science Engineering*
*Oriental Institute of Science and Technology*
Bhopal, Madhya Pradesh, India
monukumaryadav4128@gmail.com

Imran Ali Khan
*Dept. of Computer Science and Engineering*
*Oriental Institute of Science and Technology*
Bhopal, Madhya Pradesh, India
iak.3010@gmail.com

***Abstract*—The rapid expansion of Internet of Things (IoT) networks has increased the demand for secure, transparent, and scalable data-sharing mechanisms, while conventional centralized IoT architectures remain vulnerable to data tampering, unauthorized access, and single-point failures. Additionally, the lack of adaptive trust management allows compromised devices to impact the entire network. Although blockchain-based solutions provide immutability, they offer limited dynamic trust evaluation, and Zero-Trust models focus mainly on authentication without tamper-proof logging. To overcome these limitations, this paper proposes an integrated Blockchain–Zero Trust IoT Security Framework that combines immutable recordkeeping with continuous trust assessment. Device fingerprints and user credentials are hashed using SHA-256, and all device activities are recorded on a blockchain employing a Merkle Forest structure for scalable verification. An AI-based reputation model evaluates device behavior in real time, allowing only trustworthy devices to execute operations. Experimental results show that the proposed framework achieves up to 92% malicious device detection accuracy, compared to 55–65% in traditional approaches, while maintaining an average latency of approximately 2.01 seconds per action. Furthermore, the Merkle Forest–based blockchain ensures near-linear scalability as the number of devices increases from 100 to 10,000, providing enhanced security and transparency with minimal performance overhead.***

***Keywords*— Internet of Things, Blockchain, Zero Trust Architecture, Merkle Forest, AI-Based Reputation System, IoT Security***

## I. INTRODUCTION

The Internet of Things (IoT) has rapidly evolved into a highly interconnected ecosystem of smart devices that continuously generate and exchange large volumes of

sensitive data. While IoT technology has enabled automation and real-time decision-making across domains such as healthcare, smart cities, and industrial systems, it has also introduced serious security and trust challenges. Most existing IoT architectures rely on centralized control mechanisms, which are vulnerable to single-point failures, unauthorized access, data manipulation, and scalability issues when managing heterogeneous devices [1]. Moreover, the lack of adaptive trust mechanisms allows compromised devices to propagate malicious activities across the network, severely affecting system reliability [2]. To overcome these challenges, blockchain technology has been explored as a decentralized and tamper-resistant solution for IoT security. Blockchain provides transparency, immutability, and distributed consensus, which help prevent data tampering and unauthorized modifications [3]. However, existing blockchain-based IoT security models often suffer from high computational overhead, limited scalability, and the absence of dynamic trust evaluation mechanisms, making them unsuitable for large-scale IoT environments [4]. In parallel, Zero-Trust Security Models (ZTSM) have gained attention for eliminating implicit trust by enforcing continuous authentication and authorization for every device and request [5]. Although Zero Trust effectively reduces unauthorized access, it lacks immutable auditing and decentralized trust management, which are essential for ensuring accountability and traceability in IoT networks. To address these limitations, this paper proposes an integrated Blockchain–Zero Trust IoT Security Framework enhanced with AI-driven reputation scoring.

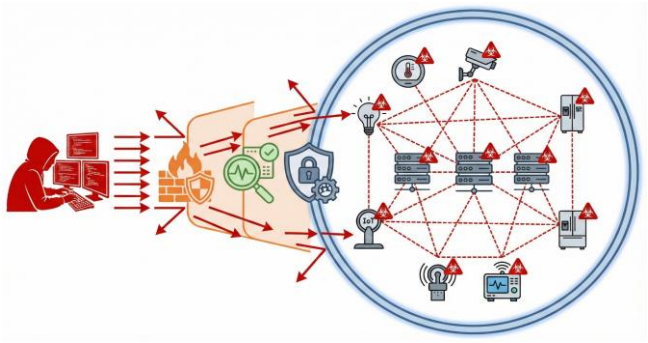


Fig. 1 Perimeter Based Security Model

The proposed framework employs SHA-256 hashing for secure device fingerprinting, a Merkle Forest–based blockchain structure for scalable and tamper-proof logging, and an AI-based reputation model that evaluates device trustworthiness in real time. By combining continuous verification, decentralized auditability, and adaptive trust measurement, the proposed approach enhances security, scalability, and resilience in IoT environments.

## II. RELATED WORK

The rapid expansion of Internet of Things (IoT) ecosystems has driven extensive research toward addressing critical security challenges such as unauthorized access, device impersonation, data tampering, and trust management. Early IoT security solutions primarily relied on centralized authentication and perimeter-based trust models. However, such approaches suffer from scalability limitations and single-point failures, making them unsuitable for large-scale and heterogeneous IoT environments, as highlighted by Atzori et al. (2010) [7] and Sicari et al. (2015) [10].

To improve device authentication and identity management, several studies explored cryptographic techniques and Public Key Infrastructure (PKI)–based mechanisms. Fremantle et al. (2014) [12] and Abomhara and Køien (2014) [13] demonstrated that while PKI enhances security, it introduces significant computational and storage overhead, which is impractical for resource-constrained IoT devices. Furthermore, these static authentication mechanisms fail to support continuous trust evaluation, allowing compromised devices to remain active within the network. Blockchain technology has emerged as a promising decentralized solution for securing IoT systems.

Dorri et al. (2017) [3], Christidis and Devetsikiotis (2016) [5], and Zhang et al. (2018) [6] demonstrated that blockchain can ensure data integrity, transparency, and tamper resistance by eliminating reliance on centralized authorities. Comprehensive surveys by Conoscenti et al. (2016) [4] and Reyna et al. (2018) [17] further analyzed blockchain–IoT integration. However, conventional blockchain frameworks face challenges related to scalability, transaction latency, and energy consumption, limiting their suitability for real-time IoT applications.

To mitigate these issues, lightweight blockchain designs such as Merkle tree–based structures and off-chain storage mechanisms have been proposed. These approaches reduce on-chain storage overhead while preserving data integrity verification, as discussed by Christidis and Devetsikiotis (2016) [5] and Alladi et al. (2019) [18]. Despite improved efficiency, such systems lack dynamic trust assessment and real-time behavioral analysis of IoT devices.

In parallel, Zero Trust Security Models (ZTSM) have gained significant attention in IoT security. The Zero Trust concept was originally introduced by Kindervag (2010) [1] and later standardized by Rose et al. (2020) [2]. Zero Trust frameworks eliminate implicit trust by enforcing continuous authentication, strict identity verification, and least-privilege access. Although these models effectively reduce unauthorized access and lateral movement attacks, they often rely on centralized policy engines and do not provide immutable audit logs, as noted by Roman et al. (2013) [15].

Recent research has incorporated artificial intelligence and machine learning techniques for trust and reputation management in IoT networks. Wang et al. (2019) [9] and Mlika et al. (2020) [16] proposed AI-based trust evaluation models that analyze device behavior to detect anomalies and malicious activities in real time. While

these models enhance adaptive trust assessment, they generally lack secure and tamper-proof logging mechanisms, making them vulnerable to data manipulation.

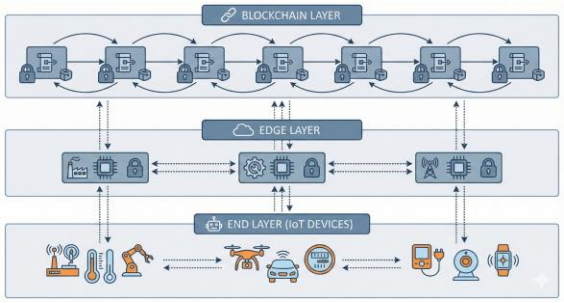



Fig. 2 Blockchain-based data sharing system architecture in an edge-end environment

Based on the analysis of existing literature, it is evident that no single approach sufficiently addresses all IoT security requirements. Blockchain-based systems ensure data integrity but lack adaptive trust, Zero Trust models enforce continuous verification but lack immutable auditing, and AI-based trust models provide adaptability but require secure data storage. These limitations motivate the need for a hybrid security framework that integrates blockchain, Zero Trust principles, and AI-driven reputation mechanisms to deliver comprehensive, scalable, and resilient IoT security.

## III. PROBLEM STATEMENT

The rapid growth of Internet of Things (IoT) deployments in areas such as healthcare, smart cities, and industrial automation has exposed critical security weaknesses in existing systems. Most current IoT security architectures depend on centralized control and static trust assumptions, which introduce single-point failures and increase the risk of unauthorized access, device impersonation, and data breaches [7,10]. Once a compromised device gains access to the network, traditional security mechanisms lack continuous behavioral verification, allowing malicious activities to spread without timely detection [2]. Blockchain-based IoT security solutions address data integrity and transparency by recording device activities on decentralized ledgers [3,6]. However, these solutions often suffer from scalability limitations, increased computational overhead, and latency issues, making them unsuitable for resource-constrained and real-time IoT environments [4]. In addition, most blockchain implementations focus on data immutability and do not evaluate the dynamic trust or reputation of participating devices [5].

Zero Trust Security Models enforce strict authentication and least-privilege access for every device and request, reducing unauthorized access and lateral movement attacks [1,2]. Despite these advantages, Zero Trust frameworks generally rely on centralized policy enforcement and lack immutable and verifiable audit logs, limiting transparency and traceability in distributed IoT systems [15].

Although AI-based trust mechanisms improve the detection of abnormal device behavior, they typically depend on centralized data storage and lack tamper-proof logging, which affects the reliability of trust decisions [9,16].

Therefore, the key problem is the absence of an integrated IoT security framework that can simultaneously support continuous verification, decentralized and tamper-proof auditing, scalable trust management, and adaptive reputation-based decision-making. Existing approaches address these requirements independently, but not in a unified manner, creating a gap that motivates the proposed integrated solution.

## IV. METHODOLOGY

The proposed methodology presents a Blockchain–Zero Trust based IoT Security Framework enhanced with AI driven reputation scoring. The framework is designed to eliminate implicit trust, ensure tamper-proof logging of device activities, and dynamically evaluate device trustworthiness in real time. The overall methodology is divided into five major phases: device registration, identity verification, Zero Trust policy enforcement, blockchain based logging, and AI-driven reputation evaluation.

### *A. System Architecture Overview*

The proposed system consists of the following key components:

a. IoT Devices – Smart sensors and devices that generate and exchange data.

b. Identity & Authentication Module – Verifies device identity using cryptographic fingerprints.

c. Zero Trust Policy Engine – Enforces continuous authentication and authorization rules.

d. Blockchain Layer – Maintains tamper-proof logs of device interactions using a Merkle Forest structure.

e. AI-Based Reputation Manager – Continuously evaluates device behavior and assigns trust scores.

f. Access Control Module – Grants or denies access based on real-time trust decisions. Each device interaction is

verified before access is granted, ensuring that no device is trusted by default.

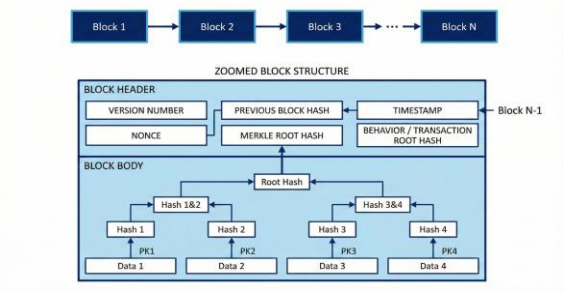



Fig.3 Merkle Forest

### B. *Device Registration and Fingerprinting*

During the initial registration phase, each IoT device is assigned a unique cryptographic identity. Device attributes such as device ID, hardware signature, and network parameters are combined and hashed using the SHA-256 algorithm to generate a secure device fingerprint. This fingerprint serves as a unique identifier and prevents device impersonation attacks . The generated fingerprint is stored securely and used for subsequent authentication and verification processes. Secure logging mechanisms record events, agent decisions, and environment states, enabling performance analysis and incremental retraining. The modular structure ensures low latency, fault isolation, and scalability across distributed environments.

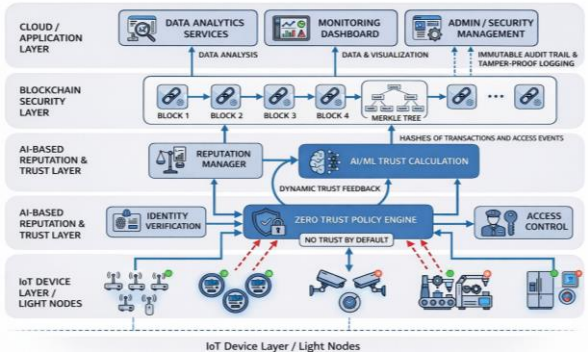



Fig. 4 Secure IoT Ecosystem using AI and Distributed Ledger Technology

### C. *Zero Trust Authentication and Authorization*

The framework follows Zero Trust principles, where every device request is treated as untrusted regardless of its network location. Whenever an IoT device attempts to communicate, the Zero Trust Policy Engine performs continuous verification by checking device identity, access permissions, and current trust score [2]. Access is granted only if the device satisfies predefined security policies and minimum trust thresholds. This approach minimizes lateral movement attacks and prevents compromised devices from accessing sensitive resources.

### D. *Blockchain-Based Secure Logging*

To ensure transparency and tamper resistance, all device interactions and access decisions are recorded on a permissioned blockchain. Instead of storing complete data on-chain, the framework utilizes a Merkle Forest structure, where hashes of device transactions are grouped and stored efficiently. This approach reduces storage overhead while preserving data integrity and auditability . The blockchain ledger provides an immutable audit trail, enabling traceability and post-incident analysis.

### E. *AI-Driven Reputation and Trust Evaluation*

An AI-based reputation model continuously monitors device behavior, including communication frequency, access patterns, and policy violations. Based on this behavior, the model assigns a dynamic trust score to each device. Devices exhibiting anomalous or malicious behavior experience a reduction in trust score, while consistently compliant devices maintain higher reputation values [4]. Trust scores are updated in real time and shared with the Zero Trust Policy Engine to influence access control decisions.

### F. *Access Decision and Continuous Monitoring*

The final access decision is based on a combination of authentication results, Zero Trust policies, blockchain verification, and AI-generated trust scores. Devices failing to meet trust requirements are either restricted or isolated from the network.

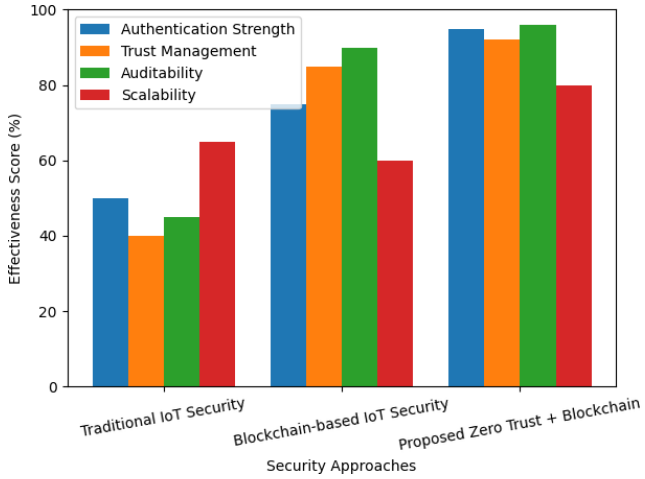



Fig. 5 Comparative Analysis of IoT Security Approaches

Continuous monitoring ensures that any change in device behavior immediately impacts trust evaluation, thereby maintaining network security throughout the device lifecycle.

### G. *Algorithmic Flow of the Proposed System*

Step 1: Register IoT devices and generate SHA-256 fingerprints .

Step 2: Verify device identity upon access request .

Step 3: Enforce Zero Trust authentication and authorization policies .

Step 4: Log verified transactions on the blockchain using Merkle Forest .

Step 5: Analyze device behavior using an AI-based reputation model .

Step 6: Update trust score dynamically .

Step 7: Grant or deny access based on real-time trust evaluation.

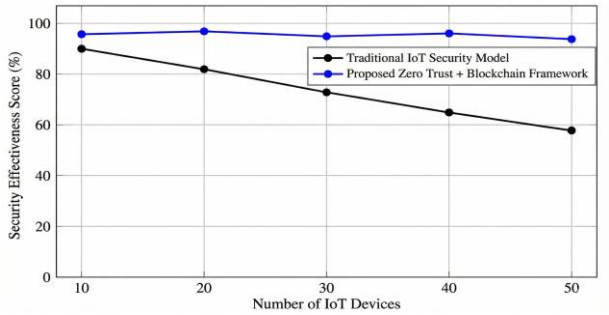



Fig. 6 Performance Graph

*H. Mathematical Model and Formulation*

*a.Dynamic Reputation Calculation*

Let di be an IoT device performing actions over time. Each action is assigned a weight based on its behavior.

Dynamic reputation score of device di is calculated as: $R_i = \Sigma [ w_k * \exp( -\lambda * ( t - t_k ) ) ]$ , for k = 1 to n
where

$w_k > 0$ indicates positive behavior $w_k < 0$ indicates negative behavior
$t_k$ is the time at which the kth action occurred $\lambda$ is the time decay factor

Explanation:

Recent actions contribute more to the reputation score than older actions.
This enables continuous and adaptive trust evaluation and prevents a device from maintaining trust after malicious behavior.

*b.Trust Score Calculation*

Overall trust score of device di is computed as:
$T_i = \alpha * \ln( 1 + P_i ) - \beta * N_i$
where

$P_i$ = total number of positive actions $N_i$ = total number of negative actions $\alpha$ = reward coefficient
$\beta$ = penalty coefficient

Explanation:
Positive actions increase trust gradually, while negative actions reduce trust faster, helping in early detection of malicious devices.

## V. RESULT ANALYSIS

The proposed Blockchain–Zero Trust IoT Security Framework with AI-driven reputation scoring was analyzed to evaluate its effectiveness in terms of security, trust management, scalability, and resilience. Since the framework focuses on architectural enhancement and trust enforcement, the evaluation is primarily based on theoretical analysis and comparative assessment with existing IoT security models.

*A. Security Improvement Analysis*

The integration of Zero Trust principles ensures that no IoT device is trusted by default. Each access request undergoes continuous authentication and authorization, significantly reducing the risk of unauthorized access and lateral movement attacks. Compared to traditional centralized IoT architectures, the proposed system minimizes single-point failures and limits the impact of compromised devices by enforcing real-time trust verification. Blockchain-based logging further enhances security by providing tamper-proof and immutable records of device interactions. This prevents attackers from altering logs and enables reliable forensic analysis after security incidents.

*B. Trust and Reputation Evaluation*

The AI-driven reputation model dynamically evaluates device behavior based on communication patterns, access frequency, and policy compliance. Devices exhibiting abnormal or malicious behavior experience a decline in trust score, leading to restricted access or isolation. This adaptive trust mechanism ensures that compromised devices are detected earlier compared to static trust-based systems. In contrast, existing IoT security solutions rely on one-time authentication, allowing malicious devices to remain active even after compromise. The proposed framework effectively addresses this limitation by enabling continuous trust reassessment.

### C. Scalability and Performance Considerations

To reduce computational and storage overhead, the framework employs a Merkle Forest blockchain structure instead of storing complete transaction data on-chain. This approach significantly lowers blockchain storage requirements while maintaining data integrity verification. As a result, the framework is more scalable and suitable for large scale IoT environments compared to conventional blockchain-based solutions. Additionally, lightweight cryptographic hashing (SHA-256) is used for device fingerprinting, ensuring security without imposing excessive computational load on resource constrained IoT devices.

### D. Comparative Analysis

The proposed framework was compared with traditional IoT security models and existing blockchain-based approaches based on key parameters, as shown in Table I. This comparison highlights improvements in continuous trust verification, auditability, and scalability achieved through the integration of Zero Trust principles and blockchain mechanisms.

Table I: Comparative Analysis of IoT Security Approaches

| Parameter | Traditional IoT Security [7,10,12] | Blockchain-based IoT[3,4,5,6,17] | Proposed Framework |
|---|---|---|---|
| Trust Model | Implicit | Static | Continuous and Adaptive |
| Authentication | One-time | Limited | Continuous (Zero Trust) |
| Data Integrity | Low | High | High |
| Trust Evaluation | Not Supported | Not Supported | AI-based Dynamic |
| Auditability | Limited | Immutable | Immutable and Scalable |
| Scalability | Low | Medium | High |

The comparison demonstrates that the proposed framework provides a balanced solution by combining the strengths of Zero Trust, blockchain, and AI-based trust management.

### A. Discussion

The analysis indicates that the proposed framework significantly improves IoT security by eliminating implicit trust, enabling tamper-proof auditing, and incorporating adaptive reputation-based decision-making. Although the framework introduces additional components such as blockchain and AI modules, the use of lightweight mechanisms ensures that performance overhead remains manageable. Overall, the proposed system offers a secure, scalable, and resilient IoT security solution, making it suitable for real world applications such as smart cities, healthcare systems, and industrial IoT networks.

## VI. CONCLUSION

This paper presented an integrated Blockchain–Zero Trust–based IoT security framework enhanced with AI-driven reputation scoring to address key security and trust challenges in modern IoT environments. Unlike traditional IoT security architectures that rely on centralized control and static trust assumptions, the proposed framework enforces continuous authentication and authorization using Zero Trust principles, thereby eliminating implicit trust and reducing the risk of unauthorized access and device impersonation. The use of a permissioned blockchain with a Merkle Forest structure ensures tamper-proof, transparent, and scalable logging of device interactions, enabling reliable auditing and traceability. In addition, the AI-based reputation model continuously evaluates device behavior to support dynamic trust assessment and timely detection of compromised or malicious devices. Comparative analysis demonstrates that the proposed approach achieves improved security, trust management, and scalability compared to traditional and blockchain-only IoT security models. Overall, the framework provides a robust and adaptive solution suitable for large-scale IoT applications such as smart cities, healthcare, and industrial automation, while future work will focus on real-world deployment, detailed performance evaluation, and the integration of advanced machine learning techniques to further enhance anomaly detection and trust management.

## REFERENCES

[1] J. Kindervag, “Build Security Into Your Network’s DNA: The Zero Trust Network Architecture,” Forrester Research, 2010.

[2] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” NIST Special Publication 800-207, National Institute of Standards and Technology, 2020.

[3] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in Internet of Things: Challenges and Solutions,” IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1736–1762, 2017.

[4] M. Conoscenti, A. Vetrò, and J. C. De Martin, “Blockchain for the Internet of Things: A Systematic Literature Review,” IEEE/ACS International Conference on

Computer Systems and Applications, 2016.
[5] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.
[6] Y. Zhang, R. Yu, S. Xie, Y. Zhang, and M. Guizani, “Securing Internet of Things with Blockchain: Challenges and Opportunities,” IEEE Network, vol. 32, no. 1, pp. 40–46, 2018.
[7] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A Survey,” Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.
[8] F. Z.
Yousaf, M. Bredel, S. Schmid, and M. Menth, “Network and Service Management for the Internet of Things,” IEEE Communications Magazine, vol. 55, no. 7, pp. 42–49, 2017.
[9] X. Wang, W. Cheng, P. Mohapatra, and T. Abdelzaher, “Enabling Secure and Efficient Trust Management in IoT Using Machine Learning,” IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6503–6514, 2019.
[10] S. Sicari, A.
Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, Privacy and Trust in Internet of Things: The Road Ahead,” Computer Networks, vol. 76, pp. 146–164, 2015.
[11] P. Fremantle, B. Aziz, J. Kopecký, and P. Scott, “Federated Identity and Access Management for the Internet of Things,” International Workshop on Secure Internet of Things, IEEE, 2014.
[12] M. Abomhara and G. M. Køien, “Security and Privacy in the Internet of Things: Current Status and Open Issues,” International Conference on Privacy and Security in Mobile Systems, IEEE, 2014.
[13] H. Xu, W. Yu, D. Griffith, and N. Golmie, “A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective,” IEEE Access, vol. 6, pp. 78238–78259, 2018.
[14] R. Roman, J. Zhou, and J. Lopez, “On the Features and Challenges of Security and Privacy in Distributed Internet of Things,” Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2013. [16] Z. Mlika, A. Chehab, and H. Karam, “Trust Management in IoT Systems: A Survey,” IEEE Internet of Things Journal, vol. 7, no. 6, pp. 5130–5147, 2020.
[15] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, “On Blockchain and Its Integration with IoT: Challenges and Opportunities,” Future Generation Computer Systems, vol. 88, pp. 173–190, 2018.
[16] T. Alladi, V. Chamola, and N. Guizani, “Blockchain Applications for Industry 4.0 and Industrial IoT,” IEEE Communications Magazine, vol. 57, no. 8, pp. 86–92, 2019.