IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, July 2025
Impact Factor: 7.67

Security Challenges in Connected Device Networks: A Blockchain-Based Approach

Vasigala Priyanka[1] and Pinniboina Prasanna Kumar[2]
Lecturer, Computer Science[1]
B.Sc. Computer Science[2]
Sir. C. R. Reddy College of Engineering, Eluru

Abstract: *The rapid expansion of the Internet of Things (IoT) has revolutionized how devices collect, exchange, and process data across a wide range of applications. However, the highly distributed and resource-constrained nature of IoT systems presents significant security challenges, particularly in data integrity, device authentication, and network resilience. Traditional centralized security models, while effective in controlled IT environments, often fail to scale securely in IoT ecosystems due to single points of failure and insufficient auditability. This study explores the integration of blockchain technology into IoT networks as a decentralized solution to address these security vulnerabilities. Through a mixed-methods research design involving both simulation-based experiments and statistical analysis, the paper evaluates blockchain's impact on unauthorized access prevention, tamper resistance, energy efficiency, and latency. A private Ethereum test network was implemented, with smart contracts deployed to automate authentication and access control. Results demonstrate that blockchain significantly reduces unauthorized access attempts and prevents data tampering, with a slight trade-off in latency and energy consumption. A Chi-Square test confirmed the statistical significance of reduced breaches in the blockchain model ($\chi^2(1) = 5.26$, $p = 0.021$). While performance overhead was observed, it remained within acceptable limits for non-critical applications. The findings affirm blockchain's potential as a transformative security layer for IoT environments, especially when data integrity, traceability, and decentralized trust are required. Future research is suggested to enhance scalability, reduce resource demands, and integrate AI for intelligent threat detection in blockchain-enabled IoT systems.*

Keywords: Internet of Things (IoT), Blockchain, IoT Security, Decentralized Networks, Ethereum, Secure IoT Architecture, IoT Authentication

I. INTRODUCTION

Importance of Security in IoT Ecosystems

The Internet of Things (IoT) represents a paradigm shift in computing, where billions of devices—including sensors, actuators, embedded systems, and wearables—are interconnected to collect, process, and exchange data. According to a report by Statista (2023), the number of connected IoT devices is expected to exceed 29 billion by 2030. As this ecosystem grows, so does its attack surface, making it an increasingly attractive target for cybercriminals. Security in IoT ecosystems is critical for several reasons. First, many IoT devices handle sensitive user data, such as health records, location information, and real-time behaviour tracking. If compromised, this data can be misused for identity theft, surveillance, or other malicious purposes (Roman et al., 2013). Second, IoT systems often control critical infrastructure—such as water systems, energy grids, and medical devices—where a breach can lead not just to financial loss but also to life-threatening situations (Conti et al., 2018). Third, IoT devices are frequently deployed in unmonitored or physically exposed environments, making them more vulnerable to physical tampering and unauthorized access. Many of these devices operate autonomously and require minimal human intervention, which complicates manual monitoring or intervention when threats arise (Sicari et al., 2015). Moreover, the sheer diversity and heterogeneity of IoT devices—from lightweight sensors to high-end edge servers—make the implementation of uniform security standards extremely difficult. Devices often come from different manufacturers, operate on different

DOI: 10.48175/IJARSCT-28539

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, July 2025
Impact Factor: 7.67

firmware, and use various protocols, making interoperable and scalable security solutions a significant challenge (Weber, 2010). Thus, the integrity, confidentiality, and availability of data in IoT networks are of paramount importance, not only for user privacy but for the operational stability of the systems they support.

Limitations of Traditional IoT Security Models

Traditional security models, which rely heavily on **centralized architectures**, are increasingly proving insufficient for protecting modern IoT ecosystems. These models typically depend on centralized servers or cloud systems for functions such as device authentication, data encryption, and access control. While effective in controlled IT environments, they fall short in the context of highly distributed and resource-constrained IoT deployments.One major limitation is the **single point of failure** inherent in centralized systems. If the central server is compromised—either by hacking, Denial-of-Service (DoS) attack, or insider threat—the entire network can become vulnerable (Zhou et al., 2019). This is particularly dangerous in mission-critical environments like healthcare or smart manufacturing, where downtime or data breaches can lead to severe consequences.

Second, many IoT devices are resource-limited in terms of CPU, memory, and battery life. Implementing heavy cryptographic algorithms or real-time intrusion detection systems becomes impractical on such devices (Alrawais et al., 2017). Consequently, developers often resort to minimal or outdated security mechanisms, exposing devices to threats like data sniffing, spoofing, or firmware manipulation.Third, traditional IoT security protocols often lack real-time responsiveness and scalability. As IoT networks grow in size, centralized servers can become bottlenecks, resulting in higher latency and delayed threat detection. Additionally, these models struggle with auditing and traceability. If a data breach occurs, it can be difficult to determine who accessed what and when, particularly when logs are stored in vulnerable or compromised locations (Yang et al., 2017).Finally, many centralized systems lack interoperability. Devices from different vendors may not follow a standardized approach to data encryption or access control, leading to fragmented security practices that are hard to manage or enforce consistently (Fernandes et al., 2016).These limitations emphasize the need for a decentralized, lightweight, and transparent security framework—a gap that emerging technologies like blockchain are well-positioned to address.

II. LITERATURE REVIEW

The convergence of the Internet of Things (IoT) and blockchain technologies has gained significant scholarly attention, especially in the context of network security. This literature review synthesizes key studies that investigate the vulnerabilities in IoT architectures, existing mitigation techniques, and the emerging role of blockchain as a security enabler in decentralized environments.

IoT networks are inherently heterogeneous and layered, typically divided into four distinct levels: **perception layer**, **network layer**, **middleware layer**, and **application layer** (Sicari et al., 2015). Each of these layers is subject to specific security threats:

- **Perception Layer**: Includes physical devices like sensors and actuators. Security concerns here revolve around device tampering, data injection, and signal interference (Weber, 2010).
- **Network Layer**: Responsible for transmitting data between devices and central servers. This layer is vulnerable to eavesdropping, DoS (Denial of Service) attacks, and routing-based exploits (Roman et al., 2013).
- **Middleware Layer**: Focuses on service management and processing logic. Here, threats include software vulnerabilities, poor authentication, and unauthorized access to data streams (Conti et al., 2018).
- **Application Layer**: Where user interaction and decision-making happen. This layer faces privacy breaches, insecure APIs, and weak data validation routines (Yang et al., 2017).

Existing Security Solutions and Their Shortcomings

Several traditional security measures have been proposed to mitigate the risks in IoT systems. These include:

- **Public Key Infrastructure (PKI)**: Used for authentication and encryption.
- **Symmetric Key Cryptography**: Lightweight and energy-efficient, but suffers from key distribution challenges.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, July 2025
Impact Factor: 7.67

- **Intrusion Detection Systems (IDS)**: Monitor network anomalies but often demand high computational resources.

While these mechanisms work well in conventional IT environments, their effectiveness diminishes in IoT due to the **resource-constrained** nature of devices (Alrawais et al., 2017). For instance, implementing full-scale encryption on a microcontroller-based device often leads to performance bottlenecks and reduced battery life.Another concern is the reliance on **centralized cloud infrastructures**, which create a **single point of failure**. If an attacker gains access to the cloud platform, the entire IoT ecosystem can be compromised (Zhou et al., 2019). Moreover, centralized systems often fail to offer adequate **auditability**, making it difficult to track unauthorized activities or data manipulations post-incident (Fernandes et al., 2016). Furthermore, traditional systems struggle with **interoperability** and **scalability**. Devices from different vendors may use proprietary communication protocols or incompatible firmware, leading to siloed security implementations that are hard to integrate or update uniformly (Weber, 2010).

Role of Blockchain in Decentralized Security

Blockchain technology, first popularized by Bitcoin, is fundamentally a **decentralized, immutable, and transparent ledger**. It eliminates the need for a centralized authority by enabling trust through consensus algorithms such as Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT) (Narayanan et al., 2016).

In the context of IoT security, blockchain offers several unique advantages:

1. **Decentralization**: No central server means no single point of failure, making networks more resilient to targeted attacks (Christidis & Devetsikiotis, 2016).
2. **Immutability**: Once recorded, transactions cannot be altered, which ensures the integrity of data logs and audit trails (Atzori, 2017).
3. **Transparency**: All participants in the network can verify the authenticity and history of data, fostering accountability.
4. **Smart Contracts**: Enable automated policy enforcement and device-level authorization without human intervention (Zhang & Wen, 2016).

Projects such as **IOTA**, **Ethereum-based DApps**, and **Hyperledger Sawtooth** have introduced blockchain-enabled platforms specifically designed to cater to low-power devices and real-time environments. IOTA, for instance, utilizes a Directed Acyclic Graph (DAG) structure, known as the Tangle, which eliminates the need for miners and reduces transaction fees, making it ideal for microtransactions in IoT systems (Popov, 2018). Despite these strengths, the integration of blockchain into IoT is not without its challenges. Scalability remains a concern; most public blockchains suffer from limited transaction throughput and high latency. The **energy consumption** associated with mining and maintaining the ledger is also a significant barrier, especially for battery-operated IoT devices (Li et al., 2018). Moreover, **real-time responsiveness** is difficult to achieve in blockchain systems due to the consensus verification time. As a result, blockchain is often unsuitable for critical control systems requiring millisecond-level latency. Nonetheless, researchers agree that the **combination of blockchain with edge computing and lightweight consensus protocols** could present a scalable, secure, and efficient model for future IoT ecosystems (Reyna et al., 2018). The reviewed literature highlights the **inadequacy of conventional security models** in handling the evolving threat landscape of IoT and emphasizes the **potential of blockchain** to fill these gaps. While the promise is substantial, real-world application still requires further refinement in terms of energy efficiency, latency management, and scalability. The need for interdisciplinary research that combines cryptography, distributed systems, and embedded device engineering is more urgent than ever.

Objectives of the Study

Primary Objectives

1. To investigate the security vulnerabilities, present in traditional IoT network architectures.
2. To evaluate the applicability of blockchain in addressing these vulnerabilities.
3. To propose a blockchain-based model tailored for securing data transmission and device integrity in IoT systems.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, July 2025
Impact Factor: 7.67

Secondary Objectives

1. To compare the performance of a blockchain-integrated IoT network against traditional systems.
2. To assess the feasibility of deploying smart contracts for automating access control and device communication.
3. To identify scalability and energy efficiency challenges of blockchain in low-powered IoT environments.

IV. HYPOTHESES

Main Hypothesis Statement

The integration of blockchain technology significantly enhances the security, transparency, and reliability of IoT networks compared to traditional centralized security architectures.

Sub-Hypotheses Derived

- H1: Blockchain-enabled IoT systems demonstrate reduced vulnerability to data tampering and unauthorized access.
- H2: Smart contracts can automate and enforce secure device communication policies without the need for central oversight.
- H3: The performance trade-offs of using blockchain in IoT environments (latency, processing overhead) are within acceptable operational limits for non-critical real-time applications

V. RESEARCH DESIGN

5.1 Justification for Mixed-Methods Approach

A purely quantitative method would be inadequate because it could overlook the architectural and behavioral implications of blockchain in IoT environments. Similarly, relying solely on qualitative techniques would limit the ability to empirically measure performance metrics such as latency, throughput, energy consumption, and attack resistance.

Thus, a mixed-methods design is ideal for this study as it allows:

- Quantitative benchmarking of network performance (latency, throughput).
- Qualitative assessment of system behavior, scalability, and design complexity.
- Triangulation of results to enhance the reliability and validity of findings.

5.2 Methodological Framework

The research was conducted in two phases:

1. Simulated Experimental Setup:
    - Developed two IoT environments: one using traditional centralized security and the other integrating blockchain with smart contracts.
    - Devices used included Raspberry Pi 4 (for sensors), NodeMCU ESP8266 (for actuation), and a private Ethereum blockchain node (using Ganache).
    - Smart contracts were deployed using Solidity via the Truffle Suite.
    - Network communication was established through MQTT protocol for IoT message transfer.
2. Analytical & Observational Study:
    - Collected data on unauthorized access attempts, successful authentications, transaction latency, and energy usage.
    - Observed how smart contracts autonomously handled access control and data validation.

5.3 Data Collection Techniques

- System Log Analysis: Captured transaction data, smart contract events, and authentication failures.
- Network Monitoring: Used Wireshark and Grafana dashboards to monitor packet flow, latency, and network load.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, July 2025
Impact Factor: 7.67

- Power Usage: Measured via USB power meters to understand the overhead introduced by blockchain operations.
- Interviews: Conducted semi-structured interviews with 5 IoT engineers and 3 blockchain developers to gain insights into real-world implementation feasibility.
- Comparative Benchmarking: Traditional vs. blockchain-based models were tested under identical environmental variables for comparative analysis.

5.4 Tools and Technologies Used

- Blockchain Platform: Ethereum (private testnet using Ganache CLI)
- Smart Contract Language: Solidity
- IoT Boards: Raspberry Pi 4, NodeMCU (ESP8266)
- Protocols: MQTT for messaging, HTTP/Web3 for blockchain communication
- Monitoring Tools: Wireshark, Python (data parsing), Grafana (visualization)

5.5 Validity and Reliability

To ensure validity, real-time data was used to simulate realistic scenarios, including network attacks and device misbehaviour. To ensure reliability, multiple test runs were performed under controlled conditions, and results were averaged to account for anomalies or environmental noise. Peer review of system architecture by external experts also contributed to the credibility of the experimental setup.

VI. SAMPLE AND SAMPLING TECHNIQUE

In this research, the term “sample” pertains not to human participants but to the hardware, software environments, and configurations used to simulate and assess the performance of blockchain-enabled security in IoT networks. The sample was selected using purposive sampling, which is ideal for technical experimentation where specific functionality, compatibility, and reproducibility are required. The objective was to simulate a scalable, realistic micro-environment reflective of common IoT use cases such as smart homes or small industrial automation setups. The hardware components included three Raspberry Pi 4 units functioning as IoT sensor nodes (measuring temperature, humidity, and motion), and two NodeMCU ESP8266 boards acting as actuators (such as smart switches). These devices were chosen for their processing capability, compatibility with MQTT protocols, and ability to interface with blockchain libraries. A local area network was created using a standard Wi-Fi router to connect these devices. Additionally, a centralized IoT system was simulated using a basic Apache server stack hosted on a laptop, serving as a control model for comparison. To replicate blockchain integration, the study deployed a private Ethereum test network using Ganache. Smart contracts were developed in Solidity and deployed using the Truffle Suite. These smart contracts handled core security functionalities including device authentication, sensor data logging, and threshold-based actuator triggers. Blockchain transactions were initiated through Web3.js and executed on the Ethereum Virtual Machine (EVM) locally. The software ecosystem comprised multiple tools tailored for monitoring and analysis. Wireshark was used for packet inspection, while Grafana dashboards visualized real-time network and energy metrics. Python scripts parsed log files, identified failed transactions, and extracted timestamps for latency analysis. The devices were powered through USB meters that measured voltage and current to calculate energy consumption during blockchain operations. Sampling criteria were based on realistic constraints faced by actual IoT deployments. All chosen devices were low-powered, operated under memory constraints, and were programmed using lightweight firmware. This ensured that the findings reflected practical deployment conditions. The selected sample was also modular and allowed for stress testing through increased transaction frequency, which helped evaluate system performance under simulated high-load conditions. Despite being compact and controlled, the sample exhibited limitations. First, the local network environment lacked wide geographic distribution, which may not fully account for internet latency or long-distance synchronization challenges. Second, the experiment involved homogeneous firmware, while real-world deployments often involve diverse software ecosystems. Lastly, the blockchain simulation was conducted on a private network, which doesn’t

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, July 2025
Impact Factor: 7.67

replicate the resource intensiveness or consensus delays of public blockchain environments. Nevertheless, the sample provided a reliable and reproducible testbed to examine blockchain's role in securing IoT data flow, authentication, and network resilience. The insights gained are applicable to broader deployments, especially in settings that prioritize data integrity, transparency, and decentralized control.

VII. DATA ANALYSIS

The data collected from both the blockchain-integrated and traditional IoT networks was analyzed to compare their performance across key security and operational metrics. This analysis involved both descriptive and inferential statistics to evaluate the significance of observed differences. The primary performance indicators included:

- Latency (ms)
- Energy Consumption (mAh)
- Unauthorized Access Attempts
- Successful Tampering Incidents
- Transaction Success Rate (%)

7.1 Descriptive Statistics

The following table summarizes the mean values recorded during the simulation phase for both security models:

Metric	Blockchain System	Traditional System
Average Latency (ms)	340 ms	170 ms
Power Consumption (mAh/hour)	410 mAh	335 mAh
Unauthorized Access Attempts	0	5
Successful Tampering Incidents	0	3
Transaction Success Rate (%)	96.8%	93.2%

Data was gathered over a 2-hour period under identical environmental conditions with 100 simulated transactions per setup. Latency was measured using Python timestamp logs, while energy consumption was recorded using USB power meters attached to each device.

7.2 Inferential Statistics

To determine whether the differences in performance between the two systems were statistically significant, the following inferential tests were conducted:

A. Independent Samples T-Test: Latency

- Null Hypothesis (H_0): There is no significant difference in latency between blockchain and traditional systems.
- Alternative Hypothesis (H_1): There is a significant difference in latency.

Using SPSS and a sample size of 100 transactions per model:

- Mean Latency (Blockchain) = 340 ms
- Mean Latency (Traditional) = 170 ms
- Standard Deviation: ~45 ms for both
- $t(198) = 19.01$, $p < 0.001$

Interpretation: The p-value is less than 0.05, indicating a statistically significant increase in latency in the blockchain model. The result supports the assertion that smart contract validation introduces computational overhead.

B. Chi-Square Test: Unauthorized Access Attempts

- H_0: Unauthorized access occurrences are equally likely across both systems.
- H_1: Unauthorized access attempts vary significantly between systems.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, July 2025
Impact Factor: 7.67

	Unauthorized Access	No Unauthorized Access	Total
Blockchain	0	100	100
Traditional	5	95	100

- $\chi^2(1) = 5.26$, $p = 0.021$

Interpretation: Since the p-value is below 0.05, we reject the null hypothesis. There is a statistically significant reduction in unauthorized access in the blockchain system.

C. Mann-Whitney U Test: Transaction Success Rate

Given that the transaction success rates were not normally distributed (confirmed via Shapiro-Wilk test), a non-parametric test was used:

- $U = 3{,}920$, $p = 0.034$

Interpretation: Blockchain systems showed a slightly higher transaction success rate than traditional systems, and the difference is statistically significant.

7.3 Correlation Analysis

A Pearson correlation was conducted to examine the relationship between energy consumption and security performance (i.e., fewer tampering incidents):

- $r = -0.72$, $p < 0.01$

Interpretation: There is a strong negative correlation between increased energy consumption and the likelihood of successful tampering. This supports the idea that added computational resources in blockchain systems contribute to stronger security enforcement.

7.4 Data Visualization

The following insights were visualized for clearer understanding:

- Latency trends: Line graphs showed consistent delays in blockchain-based systems.
- Energy curves: Bar charts reflected higher energy usage per hour under blockchain transactions.
- Security events: Heatmaps indicated unauthorized attempts were isolated only in traditional systems.

VIII. RESULTS AND DISCUSSION

The results of this study show a clear distinction in security performance between traditional IoT networks and those enhanced by blockchain technology. A critical finding was derived from the Chi-Square test applied to assess the relationship between the security model used (blockchain vs. traditional) and the occurrence of unauthorized access attempts.

Chi-Square Analysis: Unauthorized Access

To determine whether the use of blockchain significantly impacts the prevention of unauthorized access, a Chi-Square test of independence was conducted. The frequency table used is presented below:

	Unauthorized Access	**No Unauthorized Access**	**Total**
Blockchain System	0	100	100
Traditional System	5	95	100

The result of the Chi-Square test was: **$\chi^2(1) = 5.26$, $p = 0.021$**

Since the p-value is less than 0.05, we reject the **null hypothesis**, which stated that there is no difference in the occurrence of unauthorized access between the two systems. The result suggests a **statistically significant association** between the type of security system used and the frequency of unauthorized access attempts.This finding supports the argument that **blockchain-integrated IoT networks provide superior resistance to unauthorized device access**. In the traditional system, token-based or password-based authentication mechanisms were vulnerable to credential

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, July 2025
Impact Factor: 7.67

spoofing, which led to five successful access breaches during testing. These breaches occurred when malicious nodes mimicked legitimate devices and gained access to central server functions.In contrast, the blockchain model used **smart contracts to verify each transaction and authenticate devices based on predefined rules**. Unauthorized devices, lacking a verified digital identity on the blockchain, were automatically denied interaction, making breaches virtually impossible under test conditions.The effectiveness of this mechanism is attributed to the decentralized nature of blockchain, which **eliminates the single point of failure** inherent in centralized systems. Moreover, the **immutability** of the blockchain ensured that even if a malicious actor attempted to manipulate previously stored data, any such changes would be instantly visible and unverifiable, thus automatically invalidated by the consensus logic.From a practical standpoint, this outcome demonstrates the potential of blockchain to not only **reduce real-time threats** but also enhance **network trust, transparency, and accountability**. While these results are promising, it is also important to note the limitations, such as the increased resource demand and latency introduced by blockchain validation, which were addressed in other performance metrics.

In conclusion, the Chi-Square test provides strong statistical evidence that **unauthorized access is significantly less likely in blockchain-secured IoT systems**, underscoring the value of adopting decentralized security frameworks in future deployments.

REFERENCES

[1]. Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the Internet of Things: Security and privacy issues. IEEE Internet Computing, 21(2), 34–42. https://doi.org/10.1109/MIC.2017.37

[2]. Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? Journal of Governance and Regulation, 6(1), 45–62. https://doi.org/10.22495/jgr_v6_i1_p5

[3]. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

[4]. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78, 544–546. https://doi.org/10.1016/j.future.2017.07.060

[5]. Fernandes, E., Jung, J., & Prakash, A. (2016). Security analysis of emerging smart home applications. In IEEE Symposium on Security and Privacy (pp. 636–654). https://doi.org/10.1109/SP.2016.44

[6]. Kumar, P., & Mallick, P. K. (2018). Blockchain technology for security issues and challenges in IoT. Procedia Computer Science, 132, 1815–1823. https://doi.org/10.1016/j.procs.2018.05.140

[7]. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2018). A survey on the security of blockchain systems. Future Generation Computer Systems, 107, 841–853. https://doi.org/10.1016/j.future.2017.08.020

[8]. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: A comprehensive introduction. Princeton University Press.

[9]. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT: Challenges and opportunities. Future Generation Computer Systems, 88, 173–190. https://doi.org/10.1016/j.future.2018.05.046

[10]. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. Computer Networks, 57(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018

[11]. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

[12]. Weber, R. H. (2010). Internet of Things – New security and privacy challenges. Computer Law & Security Review, 26(1), 23–30. https://doi.org/10.1016/j.clsr.2009.11.008

[13]. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. IEEE Internet of Things Journal, 4(5), 1250–1258. https://doi.org/10.1109/JIOT.2017.2694844

[14]. Zhang, Y., & Wen, J. (2016). The IoT electric business model: Using blockchain technology for the internet of things. Peer-to-Peer Networking and Applications, 10(4), 983–994. https://doi.org/10.1007/s12083-016-0456-1