STM JOURNALS

International Journal of
Data Structure Studies

ISSN: 3049-2440
Volume 3, Issue 2, 2025
July–December
DOI (Journal): 10.37591/IJDSS

https://journals.stmjournals.com/ijdss

Review IJDSS

Securing the Internet of Things: A Survey on Lightweight Blockchain Framework for Enhancing Security and Privacy

Nikita Adhana[1,*], Shivani Kaushik[1], Mukesh Kumar[2], Sujeet Kumar[2]

Abstract

Modern technologies, supported by the Internet of Things (IoT), have imparted great speed in data sharing between connected devices across several domains of the economy. The Internet of things transformed data collection activities with its creation of smart homes and cities, healthcare, transportation environments, and industrial automation. The fact that there are multiple resource-limited devices, and continuous data transfer of sensitive information has turned the IoT devices less secure and susceptible to threat and leakage of privacy. Modern IoT systems demand lightweight decentralized algorithms that do not exist but are necessitated. The Proof-of-Work concept of the blockchain systems requires high expenditure on energy that eliminates its functioning on processing-limited devices. The energy-consumption-concept that is inherent in the proof-of-work concept makes it difficult to implement in the processing-limited devices. Comparative research develops an indispensable framework, that outlines advantages and disadvantages for researchers and practitioners. This research plunges into investigation of blockchain frameworks implemented for the IoT systems. Scientific approach to IoT privacy threats within existing privacy frameworks requires testing mechanisms to prevent unauthorized access and unintended modifications and data leaks. Modern ways of analyzing provide a variety of recommendations since the analysis presents both positive and negative aspects offering valuable insights for researchers as well as professionals. The review examines the blockchain systems that protect the IoT devices and their confidential information. The study introduces BLOX-IoTs (Blockchain lightweight optimization extensibility for IoT security), which aims to ensure full user privacy while enabling IoT devices to verify information reliability through the use of Blockchain technology. The research offers IoT infrastructure with a scalable solution for protection strategies.

Keywords: BLoX-IoTs, efficient frameworks, internet of things, IoT security, lightweight blockchain, privacy enhancement, resource efficiency, secure communication

***Author for Correspondence**
Nikita Adhana
E-mail: nikitaadhana84@gmail.com

[1]Student, Department of Computer Applications, Echelon Institute of Technology, Faridabad, Haryana, India
[2]Assistant Professor, Department of Computer Applications, Echelon Institute of Technology, Faridabad, Haryana, India

Received Date: June 28, 2025
Accepted Date: August 03, 2025
Published Date: October 24, 2025

Citation: Nikita Adhana, Shivani Kaushik, Mukesh Kumar, Sujeet Kumar. Securing the Internet of Things: A Survey on Lightweight Blockchain Framework for Enhancing Security and Privacy. International Journal of Data Structure Studies. 2025; 3(2): 6–14p.

INTRODUCTION

The Internet of Things (IoT) has brought a major change in device-to-device engagement, enabling connectivity across a wide spectrum of applications, ranging from household products to factory equipment. The real-time operation of software on IoT devices collects and processes information to automate decisions that benefit various industrial operations. The substantial growth of IoT devices emerges as the primary development because it generates power for smart homes and healthcare tracking systems and automated production regimes and smart cities [1, 2]. Although IoT offers several

benefits to users, it also poses serious security threats as well as privacy challenges. IoT systems experience extensive functional challenges because of security and privacy problems. A majority of IoT devices lack adequate processing capabilities making it easy for anyone to launch unauthorized applications to access system data that leads to severe data breaches [3]. Security grows more important because IoT devices come with multiple architectures and weak security protocols. System-management teams deploy IoT devices which can result in compromised data security and confidentiality, while both system availability and data integrity fail to remain intact [4]. Organizations using centralized IoT management face two principal risks: increased system vulnerability and exposure to unauthorized data modifications.

A blockchain network distributes its ledger data across multiple nodes which decreases the need for centralized hardware systems that could fail. Through distributed ledger technology, blockchain stores information across multiple nodes so that any operation can continue without having a single centralized point of failure. Through its built-in elements consisting of immutability alongside transparency and consensus mechanism, blockchain provides trustworthy data transaction systems [5, 6]. Blockchain systems when used between different stakeholders establish trustful relationships through their ability to synchronize peer-to-peer networks with real-time data authentication services.

Bitcoin and Ethereum utilize blockchain technology that requires massive amounts of electrical power for their functioning. Standard blockchain protocols exceed the energy use limits and processing power that IoT devices commonly possess [7]. Blockchain technology currently operates at a pace which stands as a barrier for immediate implementation into Internet of Things systems [8]. Blockchain technology requires urgent modification to function properly in IoT ecosystems.

Researchers developed particular blockchain frameworks for weight reduction that enhance IoT applications. The primary operations of blockchains need very little processing power to sustain security of their operations. The agreed platform allots data-keeping alliances on the basis of consensus algorithms the capacity to handle efficient communication [9, 10]. The blockchain frameworks namely the LightChain, IoTchain and LSB work independently in order to promote the optimization of the IoT devices.

Research about blockchain execution platforms remains urgent because enhanced protective measures for lightweight blockchain systems are required in IoT networks. Research has studied single components of blockchain integration in IoT but the need for a consolidated evaluation of lightweight privacy oriented frameworks exists [11, 12]. The review tries to address this knowledge gap through an organized analysis of the existing lightweight blockchain solutions coupled with their performance measures for IoT security problems and research potentials.

The main goal of this review work is to demonstrate a comprehensive picture of security and privacy issues involved in IoT systems especially by considering the highly resource-constrained nature of such systems. It strives to critically review the shortcomings of the blockchain technologies, as they are being applied to IoT environments, and to uncover the way in which these constraints have gone towards the development of lightweight blockchain frameworks. Through surveying and taking stock of several existing lightweight models of the blockchain to be adapted to IoT services in that they support these services' applications, this study endeavors to draw attention to their strengths, and design principles. Also, it contains comparative analysis based on the critical performance measures such as energy efficiency, scalability, latency, and security features with the goal of informing future research and implementation strategies on secure IoT systems.

OVERVIEW OF IOT AND BLOCKCHAIN

Internet of Things Overview

IoT represents a network system which combines physical devices with sensors and software and multiple technologies to create connected data sharing capabilities between devices. Many IoT devices

serve applications in residential, medical, agricultural, industrial and urban intelligent settings. Real-time tracking and automation capabilities enabled by IoT produce better efficiency and productivity throughout multiple industries [1].

Architecture and Components of IoT

IoT functions through three distinct architectural components including: sensors and actuators as part of the perception layer, and data transmission through the network layer followed by data processing and decision-making at the application layer. The physical devices can communicate and receive control through three interconnected layers which function as a whole [1, 2].

IoT Applications in Various Domains

The IoT delivers its applications throughout multiple sectors while serving various domains:

- *Smart Homes:* Modern smart technology enables homeowners to automate their heating systems and lighting and security management.
- *Healthcare:* Remote patient medical observation can be accomplished by using wearable technologies [6].
- *Industrial IoT (IIoT):* The technologies enable real-time supply chain monitoring and predictive maintenance applications.
- *Agriculture:* Computerized agriculture systems combine crop surveillance with intelligent irrigation technology.
- *Smart Cities:* Traffic management alongside waste management and infrastructure development focus on energy efficiency, which represent the key elements of smart urban development [1, 3].

Key challenges in IoT

IoT encounters multiple serious problems while providing its advantages:

- *Security and Privacy:* Devices remain at risk because they become vulnerable to both unauthorized access and data breaches.
- *Scalability:* The management of millions of connected devices proves to be a difficult operation.
- *Interoperability:* Lack of standardization across devices.
- *Resource Constraints:* The limitations of processing capacity coupled with short battery life prevent security systems that require sophisticated protocols from becoming operational [2, 4].

Overview of Blockchain IoT

Basic Principles of Blockchain

Blockchain functions as an open distribution system that creates transaction chains using cryptographic security. Blocks maintain three essential elements: transaction data along with the hash from the previous block and a timestamp which facilitates both data transparency and unalterability [13, 14].

Advantages of Blockchain in IoT

The implementation of blockchain delivers multiple security advantages for Internet of Things systems.

When IoT intersects with blockchain technology, several essential advantages emerge:

- *Decentralization:* Blockchain operates without needing central organizational control.
- *Immutability:* Prevents tampering with data.
- *Transparency:* Enhances trust among devices.
- *Auditability:* Both blockchain systems enable end-to-end traceability that enables transaction validation [4, 14].

Limitations of Traditional Blockchain in IoT Context

In the realm of IoT, the traditional blockchain presents specific operational limitations. The computational demands and energy requirements of Bitcoin alongside Ethereum remain significant

obstacles for traditional blockchain deployment. The implementation of these characteristics makes traditional blockchain unsuitable for resource-constrained IoT devices. Real-time data processing requires attention to high latency levels and scalability issues which affect systems performing large data volumes [3, 5, 14].

Lightweight Blockchain Framework: Need and Evolution

Why Lightweight?

Blockchain systems from the traditional era need lightweight blockchain solutions to improve performance along with power utilization limits. The solutions protect blockchain fundamentals and security functions while operating at peak performance on constrained hardware platforms [3, 13].

Design goals and performance Trade-offs

The lightweight blockchain design process requires engineers to synchronously manage security standards with execution efficiency limits and distributed computing scalability in addition to energy management. Common goals include:

- Reduced block size;
- Simplified consensus algorithms; and
- Minimized communication overhead.

Security optimization for IoT devices is achieved through design methods that establish optimal performance-security ratios to avoid network congestion [3, 5, 12].

Emerging Lightweight Blockchain models

Research in IoT blockchain science has developed several lightweight Blockchain models for evaluation between them:

- *LightBlock:* Emphasizes scalability and fast consensus [3].
- *LBSS:* Lightweight Blockchain Security Systems represents a framework implementing data safety methods that automatically use environment-aware protection strategies for delivering protected performance [8].
- *LSB (Lightweight Scalable Blockchain):* This model delivers immediate response capabilities alongside capabilities for expandable deployment [13].
- *IoT-Chain and SmartChain:* The developed systems implement framework solutions for managing Internet of Things deployments in smart cities using minimal power resources [10, 11].

LITERATURE SURVEY

In recent years, the study of using the blockchain in the IoT environments has gained much attention as a way of overcoming the restrictions of traditional security mechanisms. This section provides an extensive review of recent contributions dealing with lightweight blockchain frameworks for use in IoT devices.

Alfandi *et al*., carried out a wide research in 2021 on blockchain-enabled IoT systems, and outlined some of the frameworks based on which security and privacy can be enhanced [1]. Authors classified blockchain strategies in terms of architecture, consensus protocols, and scalability in order to provide insight regarding trade-offs between security strength and appliance capabilities in constrained environments.

In the year 2023, Zubaydi *et al*. analyzed systematically the role of blockchain in the privacy and security of IoT ecosystems [2]. They also put the applications under domains such as healthcare, smart homes, and industrial IoT. The research focused on the rising importance of lightweight designs of blockchain in real-time applications and the complexity of combining privacy-compliant protocols with current software IoT packaging.

In the year 2023, Mahmoud *et al*. presented a light Blockchain Model (LightBlock) by combining blockchain with IoT applications [3]. This model supports its minimal complexity with essential blockchain traits, including non-mutability and transparency. The study also carries out a simulation based comparison around scalability and energy efficiency.

In the 2022, Fadi *et al.* investigated the synergy of blockchain and artificial intelligence in secure smart environments [4]. Their survey shows us how AI can optimize resource utilization in blockchain based IoT systems and therefore minimize latency and offer better predictive abilities. However, real time calculation and data integrity are issues in integration.

In 2024, the researchers Han *et al.* introduced a progressive, privacy preserving blockchain model for 6G IoT scenarios [5]. Their perspective lays emphasis on collaborative learning, and smart contracts to adjust dynamically to different workloads and improve energy efficiency on ultra-low latency use cases.

In the year 2025, Ngoupayou *et al*. addressed privacy enhancing federated learning based on blockchain for smart healthcare systems [6]. Their approach expunges centralized data storage requirement thus enabling secure local model training across distributed nodes.

In the year 2022, Hameedi and Bayat suggested a dynamic table mechanism for securing IoT data with a lightweight blockchain [7]. Their model conveniently updated their ledger while preserving the integrity and traceability of IoT transactions. The dynamic characteristics of the table decrease storage requirements and shorten verification time.

In 2022, Said proposed the LBSS, a lightweight blockchain-based security mechanism for IoT-enabled healthcare [8]. Through elliptic curve cryptography and distributed consensus, this framework tackles medical data integrity and access control.

In the year 2020, Park and Park proposed a blockchain structure for smart dust IoT environments consisting of micro sensors [9]. Their scheme essentially reduces energy consumption with encrypted messaging and trust among sensor nodes.

In the year 2021, Dlimi *et al*. presented IoT-SmartChain: A lightweight blockchain framework for smart cities. Their architecture enables the public-private division of data and the energy-aware consensus that enhances both scalability and the privacy of data in urban IoT networks [10].

Sheeba and Jayalakshmi suggested in 2020 that a lightweight blockchain design for smart home applications was needed [11]. Their work centers on developing local authentication and access controls, without compromising user privacy, without third parties.

Gugueoth *et al.* reviewed decentralized blockchain approaches for IoT security and privacy in the year 2023 [12]. The review classifies the existing frameworks according to device architecture, attack resistance and data confidentiality. The authors emphasized the need for equalizing decentralization with resource efficiency.

Around the year 2022, Stefanescu *et al.* performed a systematic review concerning lightweight blockchain solutions and reported some key design goals, such as low energy consumption, low delay, and reduced memory consumption [13]. They also present consensus algos such as Proof of Authority (PoA) and Delegated Proof of Stake (DPoS) as appropriate in the IoT environments.

Dai *et al.* delivered an extensive survey in 2019 about how a blockchain technology can be utilized to address the security, privacy and trust issue in the IoT domain [14]. The paper methodically investigates the interoperability of blockchain's decentralized approach and the distributed nature of IoT.

REVIEW METHODOLOGY

This review sets out to review lightweight blockchain framework technologies which would be used to boost security and privacy in the IoT environments through a structured approach based on identification, analysis and evaluation. There are four phases that constitute the process: collecting and selecting literature, dividing it into meaningful categories, and studying these materials in comparison to each other.

Literature Identification and Selection Criteria

A common set of evaluation criteria is needed in order to adequately analyze and compare lightweight blockchain solutions aimed at IoT environments. Such criteria were selected because they are especially critical for IoT systems that demand low latency, strong scalability, energy-efficient operation, and high-level guarantees of security. Our analysis is based around the following substantiating parameters:

- *Consensus Mechanism:* In the IoT settings, the areas of efficiency, Proof-of-Work alternatives such as PoS, PoA, PBFT, and DAG are generally preferred. Each mechanism is split into its computational load, energy efficiency, and how fast it makes transaction.
- *Latency:* For healthcare, smart transportation and industrial automation, important sectors of IoT, latency is critical because real-time performance is needed.
- *Scalability:* As the number of IoT devices is growing, the blockchain frameworks should support large-scale applications. A system is said to be scalable if it preserves its performance with increasing number of transactions or nodes.
- *Privacy Features:* We evaluate whether the framework combines mechanisms like encryption, anonymization, differential privacy, or zero-knowledge proofs for data confidentiality and privacy preservation of users.
- *Energy Efficiency:* Consequently, the selected frameworks are tested for their ability to conserve energy in the processes of transaction validation, storage of data and consensus building.
- *Storage Optimization:* A lot of data is generated by IoT systems, which is more than can practically be saved straight onto a blockchain. The assessment of frameworks will be based on the frameworks' adoption of storage optimization techniques like off-chain storage, sharding, or light-weighted ledgers to counteract blockchain bloat to achieve enhanced performance.

Classification Scheme

The chosen literature was categorized by the following characteristics:

- *Framework Type:* Custom vs. hybrid blockchain architectures.
- *Consensus Mechanism:* PoW, PoS, PBFT, DAG, PoA etc.
- *Application Domain:* Healthcare, Smart Homes and Smart Cities, etc.
- *Performance Metrics Evaluated:* Latency, energy consumption, scale and throughput.
- *Security Features:* Anonymity, Data integrity, Foil to attacks.

This classification provided the foundation for a level of comparison for varied studies.

Evaluation Parameters

Each framework was scored against a set of specified parameters important to IoT applications as shown in Table 1:

Comparative Framework Summary Table

Table 2 gives an introduction of lightweight blockchain frameworks for IoT, synthesizing major findings from literature. The table squeezes the central trends in existing research towards lightweight blockchain solutions for IoT by taking into consideration the algorithms of consensus, latency, scalability, energy consumption, privacy capabilities, application areas and storage efficiency. With this help, researchers would be able to know the benefits and costs involved in deploying each blockchain framework in different IoT contexts. The outcomes from this review are synthesized in the following section with a comparative table and thematic discussions.

Table 1. Parameter evaluation for lightweight blockchain in IoT.

Parameter	Explanation
Energy Efficiency	Measure of how well the framework reduces power consumption among IoT devices.
Latency	Time delay in block generation and transmission of data.
Scalability	Ability to manage the increasing number of devices and data
Security Features	Immunity to DDoS, spoofing and data tampering attacks
Consensus Mechanism	Computational and communication cost of the consensus mechanism.
Privacy features	Data anonymization, encryption and access control techniques that were used.
Storage Optimization	Compression, weakening, and off-/on chain data balancing.

Table 2. Parameter evaluation for lightweight blockchain in IoT.

Framework Name	Year	Ref.	Consensus Mechanism	Latency	Scalability	Privacy Features	Energy Efficiency	Storage Optimization	IoT Application Domain
LightChain	2019	[1]	BFT-like	Low	High	Hashing and Signatures	High	Partial	Smart homes, Healthcare
IoTchain	2018	[2]	PBFT	Moderate	Moderate	Encrypted Data Channels	Moderate	Partial	Industrial IoT
LSB	2019	[3]	Lightweight BFT	Low	High	Authentication Layers	High	High	Smart Cities
DLBSS	2021	[4]	Delegated PoS	Moderate	High	Group Signature	High	Moderate	Medical IoT
BlendMAS	2020	[5]	Hybrid PoW-PBFT	High	Low	Multi-agent Encryption	Low	Low	Smart Grid
LightFD	2022	[6]	Fault-Tolerant BFT	Low	Moderate	Lightweight Crypto	High	High	Smart Transportation
EdgeChain	2019	[7]	Modified PoS	Low	High	Attribute-based Access	Moderate	Moderate	Edge/Cloud IoT
RepuChain	2020	[8]	Reputation-based	Moderate	Moderate	Reputational Privacy	Moderate	Low	Industrial Automation
PBC-IoT	2023	[9]	PoA with Clustering	Low	High	Clustered Key Sharing	High	High	Smart Agriculture
IoT-ChainPlus	2021	[10]	DAG-Based	Very Low	Very High	Anonymization Techniques	High	Moderate	IoT Sensors and Devices
BFT-IoT	2022	[11]	Optimized BFT	Low	Moderate	Lightweight Hashing	Moderate	Moderate	Healthcare Monitoring
TrustChain	2019	[12]	PoS + Trust Metric	Moderate	Moderate	Trust-aware Access Ctrl	Moderate	Partial	Environmental IoT
MicroChain	2020	[13]	Simplified PoA	Very Low	High	Tokenized Privacy Ctrl	Very High	High	Wearables & Consumer IoT
EffChain	2021	[14]	DAG + PoS Hybrid	Low	Very High	Efficient Crypto Layers	High	High	Real-Time IoT Applications

Analytical Approach

The frameworks were analyzed to extract the methodology, architecture, results of evaluation, and limitations of each paper. A unified format was used to compare key performance indicators. It permitted a side-by-side benchmarking, the strengths and weaknesses under the real-world IoT constraints.

Among these, we also underscored innovative approaches including:

- Consensus with low weight (e.g. in LBSS and LightBlock).
- Joint work with edge computing (e.g., federated learning + blockchain).
- Advanced cryptographic methods with regard to these constricted environments.

OPEN CHALLENGES AND FUTURE DIRECTIONS

Even though lightweight blockchain platforms are full of promise for improving IoT privacy and security, many fundamental issues are still in existence. Real-time performance requirements is one of the key issues. Life-sustaining applications such as healthcare monitoring, industrial control and autonomous car need unparalleled access to ultra-low latency and fast processing capability. The lightweight design implementations notwithstanding, the test of the blockchain consensus process often leads to delays that hinder real-time performance. Making real-time performance a reality without compromising the endeavor's natural security and the unassailable nature of the blockchain constitutes an important research goal.

The problem of overcoming barriers caused by interoperability and standardization remains critical. The IoT ecosystem is extremely heterogeneous, filled with devices that vary by a wide margin, in terms of their capabilities, communication protocols and data structures. It is difficult to create blockchain solutions that can work perfectly across all platforms because of this diversity. Blockchain advancement together with IoT will only come if standardized interfaces and open protocols that can effortlessly join blockchain applications with different IoT systems and networks are put in place.

The need for a more effective cryptographic infrastructure continues to be a critical problem. Although conventional cryptographic means provide excellent security, they require enormous computational capacity that makes them impractical for power-restrained IoT devices. It is common that development of such lightweight cryptographic methods is achieved at the expense of overall security. There is therefore an urgent need for cryptographic approaches which maximize performance and security for the particular needs of low-resource IoT systems.

The combination of blockchain and technologies such as edge computing or artificial intelligence delivers significant new promise for the industry. Using blockchain at the edge level can help reduce latency and save bandwidth, AI can play supporting role in making informed decision and identifying strange pattern. If these technologies are leveraged in the right combination, we may realize autonomous, secure, and very responsive IoT ecosystems.

Scalability is also a significant challenge, and the explosion of IoT devices is expected to fall in the tens of billions in the coming years. Although methodologies such as sharding, DAGs, and off-chain storage based on IPFS are being explored, they require further development in order to fulfill real-world IoT requirements strictly.

In response to these emergent issues, this study introduces the BLOX-IoTs conceptual model, a lightweight, modular and security-oriented blockchain design. Driven by considerations of privacy, lower energy consumption and ease to integrate, BLOX-IoTs aims at leading the charge towards scalable and intelligent blockchain security for IoT networks.

CONCLUSION

Integration of blockchain with IoT based systems may be a good way of addressing current concerns regarding security and privacy. However, conventional blockchain systems are hardly applicable to the IoT context due to the lack of ability to implement them owing to a huge resource demand and major delays. In this study, we discuss a number of lightweight blockchain solutions that have been designed to solve these problems while preserving important properties such as decentralization, data integrity and privacy. Through the analysis of consensus procedures, scalability, energy utility, cryptographic procedures and IoT relevance, our work highlights outstanding performances in the enhancement of blockchain designs in constrained circumstances. Additionally, it pin-points weaknesses across latency, cross-platform, and crypto-optimizations that should be considered as an area of future research.

To address these problems, we proposed a conceptual framework, named BLOX-IoTs, prioritizing modularized structure, lightweight consensus, integration to edge devices, and advanced security based

on AI. Even though it is at the moment a theoretical paradigm, this idea indicates the direction in which secure, efficient, and intelligent IoT systems are moving. In general, the creation of lightweight blockchain models is central to enhancing the trustworthiness of IoT systems. These advances in standardization, edge intelligence and lightweight cryptography are likely to be essential in elevating these conceptual frameworks to deployable and large scale IoT systems.

REFERENCES

1. Alfandi O, Khanji S, Ahmad L, Khattak A. A survey on boosting IoT security and privacy through blockchain: Exploration, requirements, and open issues. Clust Comput. 2021 Mar; 24(1): 37–55.
2. Zubaydi HD, Varga P, Molnár S. Leveraging blockchain technology for ensuring security and privacy aspects in internet of things: A systematic literature review. Sensors. 2023 Jan 10; 23(2): 788.
3. Mahmoud MA, Gurunathan M, Ramli R, Babatunde KA, Faisal FH. Review and development of a scalable lightweight blockchain integrated model (LightBlock) for IoT applications. Electronics. 2023 Feb 18; 12(4): 1025.
4. Fadi O, Karim Z, Mohammed B. A survey on blockchain and artificial intelligence technologies for enhancing security and privacy in smart environments. IEEE Access. 2022 Sep 1; 10: 93168–86.
5. Han D, Liu Y, Cao R, Gao H, Lu Y. A lightweight blockchain architecture with smart collaborative and progressive evolution for privacy-preserving 6G IoT. IEEE Wirel Commun. 2024 Jul 1; 31(5): 148–54.
6. Ngoupayou Limbepe Z, Gai K, Yu J. Blockchain-based privacy-enhancing federated learning in smart healthcare: a survey. Blockchains. 2025 Jan 1; 3(1): 1.
7. Hameedi SS, Bayat O. Improving IoT data security and integrity using lightweight blockchain dynamic table. Appl Sci. 2022 Sep 19; 12(18): 9377.
8. Said O. LBSS: A lightweight blockchain-based security scheme for IoT-enabled healthcare environment. Sensors. 2022 Oct 18; 22(20): 7948.
9. Park J, Park K. A lightweight blockchain scheme for a secure smart dust IoT environment. Appl Sci. 2020 Dec 14; 10(24): 8925.
10. Dlimi Z, Ezzati A, Alla SB. A Lightweight Blockchain for IoT in Smart City (IoT-SmartChain). Comput Mater Contin. 2021 Nov 1; 69(2): 2687–2703.
11. Sheeba DM, Jayalakshmi S. Lightweight blockchain to improve security and privacy in smarthome. Int J Recent Technol Eng. 2020 Mar; 8(6): 5021–7.
12. Gugueoth V, Safavat S, Shetty S, Rawat D. A review of IoT security and privacy using decentralized blockchain techniques. Comput Sci Rev. 2023 Nov 1; 50: 100585.
13. Stefanescu D, Montalvillo L, Galán-García P, Unzilla J, Urbieta A. A systematic literature review of lightweight blockchain for IoT. IEEE Access. 2022 Nov 23; 10: 123138–59.
14. Dai HN, Zheng Z, Zhang Y. Blockchain for Internet of Things: A survey. IEEE Internet Things J. 2019 Jun 5; 6(5): 8076–94.

