Innovations in Intelligent Systems and Advanced Engineering
Vol. 1, No. 2, 2025 (August)

Lightweight Blockchain Framework for Efficient Smart Home Device Communication

T. Buvaneswari
Department of Computer Science and Engineering, Annapoorana Engineering College (Autonomous), Salem, Tamil Nadu, India
buvanamuruga2008@gmail.com

Mageshkumar Naarayanasamy Varadarajan
Lead Software Engineer, Capital One, Glen Allen, Virginia, USA
mageshkumar.varadarajan@gmail.com

Mythily M
Division of Computer Science and Engineering, Karunya Institute of Technology and Sciences, Coimbatore, Tamil Nadu, India
mythily.m@gmail.com

Hemantha Kumar B N
Master of Computer Applications, ATME College of Engineering, Mysore, Karnataka, India
hemanthvviet2006@gmail.com

A Bharath
Department of Computer Science and Engineering, CVR College of Engineering, Hyderabad, Telangana, India
bharath.andugula@cvr.ac.in

Sangeetha A
Department of Computer Science and Engineering, R.M.K. College of Engineering and Technology, Chennai, India
asangeethacse@rmkcet.ac.in

P. Selvarani
Department of Computer Science and Engineering, Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai, Tamil Nadu, India
drselvarani@velhightech.com

J. Bennilo Fernandes
Department of Electronics and Communication Engineering, Kalasalingam Academy of Research and Education, Virudhunagar, Tamil Nadu, India
bennij05@gmail.com

Abstract: The swift expansion of the Internet of Things (IoT) has expedited the implementation of smart sensors, generating substantial volumes of time-series data that require safe, efficient, and dependable management. Current centralized systems have constraints in maintaining integrity, protecting communications, and deriving economic value from this data. A blockchain-based smart house gateway network is suggested to address security concerns in smart home environments. The framework has three layers: device, gateway, and cloud. Blockchain technology is integrated at the gateway layer to provide decentralized storage and safe data interchange, eliminating single points of failure inherent in centralized systems. This integration ensures authentication, high availability, and secure communication across devices and stakeholders. The system utilizes Ethereum blockchain technology and is assessed based on important parameters such as response speed and detection accuracy. Experimental study demonstrates that the framework much surpasses traditional methods, improving resilience and reliability in smart home IoT ecosystems. The suggested system offers a scalable approach for safe data management and dependable value exchange in dispersed settings.

Keywords: Internet of things, smart home security, blockchain, Ethereum, data integrity

I. INTRODUCTION

Smart home applications are always evolving due to improvements in Information and Communication Technology (ICT) and the Internet of Things (IoT) [1]. Gartner, a global research organization, anticipated that the quantity of smart home devices will exceed 25 billion by 2020, with the global smart home industry forecast to grow by over $7 billion by 2025. A "smart home" is characterized as a domestic setting where data is incessantly exchanged, facilitating automated and intelligent services via household products like televisions, lighting systems, and refrigerators. These gadgets provide a local communication network that connects several settings autonomously. Users may control and oversee these devices according to their preferences and organizational configurations. The Internet of Things and sophisticated network infrastructures are becoming essential facilitators of this shift. Communication in smart home networks is transitioning from wired to wireless due to embedded computers and IoT devices. Gateways now provide centralized management of several devices both within and beyond the house. The commercialization of 5G, consolidation among technology firms, and advancements in hardware enhance the evolution of dependable, efficient smart home systems.

Notwithstanding these developments, considerable security issues emerge. Centralized networks render smart gadgets susceptible to hackers. Televisions and refrigerators have been utilized to disseminate phishing information and spam, while a baby monitor in Texas was compromised to transmit obscene sounds. Likewise, inadequate passwords have facilitated extensive DDoS assaults on domestic devices [7]. With the rapid adoption of IoT, risks include data falsification, unauthorized device access, and manipulation of device functionalities through gateways or servers are on the rise [8]. Gateway flaws can enable attackers to manipulate data streams, highlighting the need for secure, economical designs that provide confidentiality, integrity, availability, low latency, and accessibility, while also ensuring scalability and flexibility.

Blockchain has lately surfaced as a feasible method to mitigate security problems in IoT and smart city applications [10]. Decentralized and trustless architecture facilitates information flow across distributed ledgers without dependence on central authority [11,12]. Blockchain facilitates secure peer-to-peer communications, guaranteeing transparency, immutability, and resilience. In smart homes, blockchain may be integrated into gateways to facilitate data interchange and storage through distributed architectures, therefore addressing the vulnerabilities of centralized systems [14]. This connection enhances secrecy, integrity, and authenticity by enabling decentralized and encrypted communication [15].

- ✓ This research proposes a blockchain-based smart home gateway network architecture to address security challenges in existing network designs and to mitigate potential risks in smart home environments.
- ✓ The study implements a decentralized architecture using Ethereum blockchain technology within the smart home gateway to fulfill key security requirements, including confidentiality, integrity, and authentication.
- ✓ The proposed approach is evaluated against conventional centralized security architectures through a comprehensive security analysis, demonstrating the effectiveness and robustness of the intended framework

Security vulnerabilities are examined inside the smart home network layer, and remedies are provided to fix them. Their approach leverages Internet Service Providers (ISPs) to monitor and verify approved devices, enabling control of smart home devices even when the internet connection is unavailable. However, due to the absence of adequate client data for evaluation, this methodology is limited in its ability to secure the internal web environment. Wireshark was used to analyze network traffic and evaluate device behavior, but the approach revealed a lack of confidential data protection for devices such as fire detectors, and its implementation was incompatible with tools other than Wireshark. A blockchain-based mechanism is proposed for managing firmware updates of embedded devices. This method validates updates using digital signatures and employs encryption with private keys. While effective for larger environments, this strategy does not offer a comprehensive security solution for smaller smart homes with only a limited number of devices. A software-defined networking (SDN)-based gateway architecture is introduced for integrated resource control and configuration. This architecture offers flexible and secure communication for the growing number of IoT devices. The hybrid method can generate weaknesses, especially weak-link concerns.

Other researchers have integrated artificial intelligence (AI) into security frameworks and proposed user-driven security strategies. While innovative, these methods are highly dependent on the availability of sufficient training data, which limits their effectiveness in real-world scenarios. Several studies also explore security threats in smart homes by classifying different types of attacks and providing a holistic view of vulnerabilities. For example, Poh proposed a framework for securing smart home data that supports authentication, secure storage, and query operations. This system learns and adapts communication patterns between the client, gateway, network, and device to strengthen confidentiality and data validation. Moreover, attacks on smart homes have been categorized into low, medium, and high levels of severity to guide appropriate countermeasures. Recent research trends further highlight the application of advanced technologies such as blockchain, software-defined networking, and deep learning to strengthen the resilience of IoT-enabled smart homes.

II. PROPOSED SYSTEM

Integrating blockchain into smart home gateways is essential for maintaining both data integrity and confidentiality during communication between devices and external entities. Conventional smart home networks generally rely on centralized architecture; however, incorporating blockchain within the cloud layer shifts the model toward a distributed framework. The proposed blockchain-enabled smart home gateway architecture is organized into three layers: device, gateway, and cloud.

Device Layer: This layer comprises diverse IoT devices and sensors responsible for collecting and monitoring data within the home environment. These devices continuously generate streams of information related to household activities and conditions.

Gateway Layer: Serving as the intermediary between devices and the cloud, the gateway layer stores data from the device layer and provides user access when required. It also facilitates secure communication and decentralized data management through blockchain integration.

Cloud Layer: Here, blockchain technology records each gateway's unique identifier along with its processed data. Because these records are distributed, users can securely access information anytime and anywhere, ensuring high availability and resilience.

Figure 1 presents the design overview, while Figure 2 illustrates the data flow from device collection to blockchain registration and user presentation.

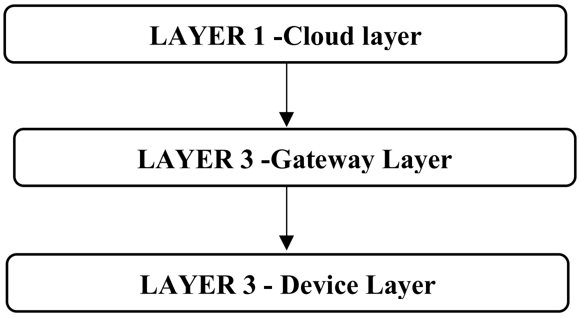


Figure 1: Proposed Design Overview

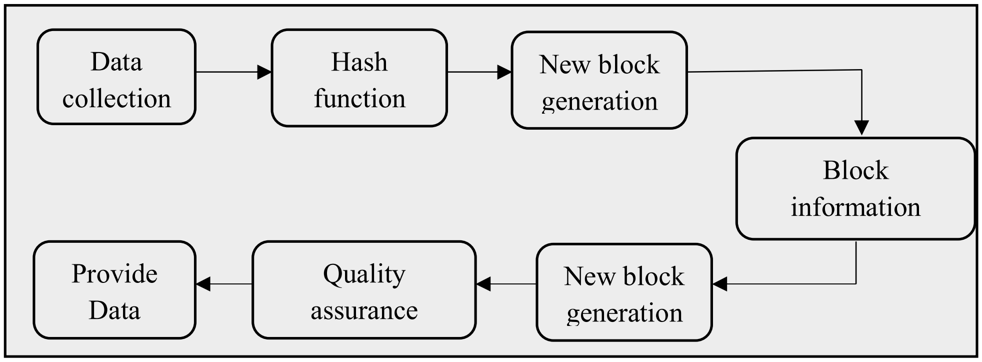


Figure 2: Methodological Flow of Proposed Framework

After hashing computation and formatting, data is wrapped into blocks. These blocks are then validated at regular intervals to ensure data integrity, even in the event of attempted falsification. Furthermore, continuous data analysis and quality management are incorporated to maintain the reliability of the system. This guarantees that consumers receive correct, verified, and relevant information, improving smart home gateway security and usability. Figure 3 depicts the proposed blockchain-based architecture.

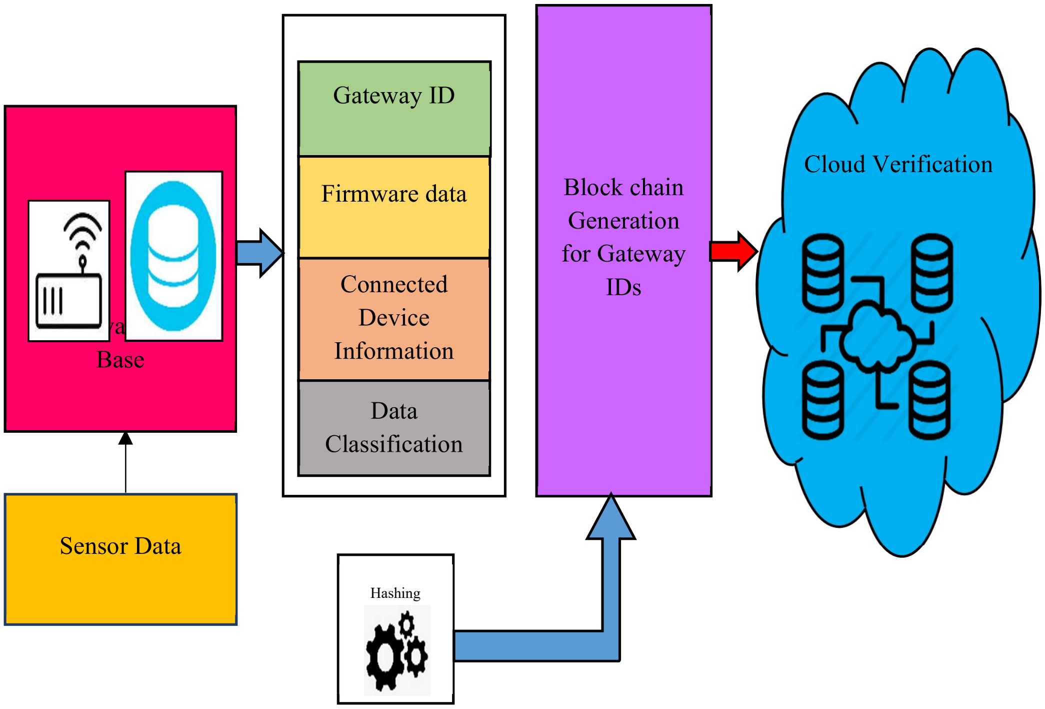


Figure 3: Proposed Block Chain Architecture

The framework, composed of interconnected blockchain nodes, ensures the integrity of both data transfer and recordkeeping. To safeguard data generated by end nodes, the SHA-3 hash algorithm is employed, allowing information to be securely stored either within the blockchain network or in associated databases, depending on the context. On the cloud-based blockchain platform, blocks are compared in real time, enabling the identification of any forged entries. The proposed architecture operates in three main stages:

1. Data Collection and Storage: Data are collected through gateways distributed across the smart home network. These gateways request additional information from devices when needed and aggregate raw data into storage systems. The data are initially stored at the gateway level to ensure availability and minimize latency.

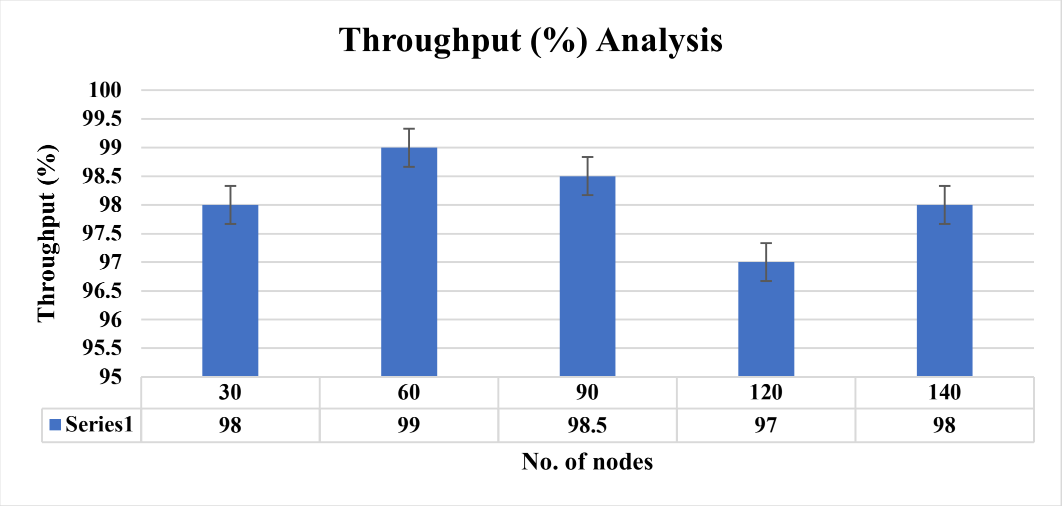
2. Data Pre-processing and Standardization: Before blockchain integration, the collected raw data undergoes pre-processing within the gateway to filter relevant information and reduce computational complexity. The pre-processed data are then standardized and classified, ensuring consistency for subsequent processing.

3. Blockchain Generation and Verification: The refined data, along with associated gateway IDs, are encapsulated into blockchain blocks. These blocks are transmitted to the cloud layer, where they undergo end-to-end encryption and verification against known gateway IDs. This process strengthens trust and security, ensuring that only validated and tamper-resistant data are recorded within the blockchain.

Through this layered approach, the architecture enhances confidentiality, integrity, and authenticity, thereby mitigating common security vulnerabilities in conventional centralized smart home networks.

III. RESULTS AND DISCUSSIONS

To demonstrate the effectiveness of the proposed system, throughput and latency parameters are incorporated into the performance evaluation. These metrics are critical for assessing the efficiency and responsiveness of the smart home gateway network. Figure 4 presents the throughput analysis, illustrating the system's ability to handle increasing volumes of data while maintaining stable performance. Figure 5 provides the latency analysis, highlighting the time delay associated with data transmission, processing, and blockchain validation within the proposed framework. The combined evaluation confirms that the proposed blockchain-based architecture achieves high throughput with minimal latency, thereby ensuring both scalability and responsiveness in smart home environments.



	30	60	90	120	140
■ Series1	98	99	98.5	97	98

Figure 4: Throughput Analysis for Proposed Block Chain Architecture

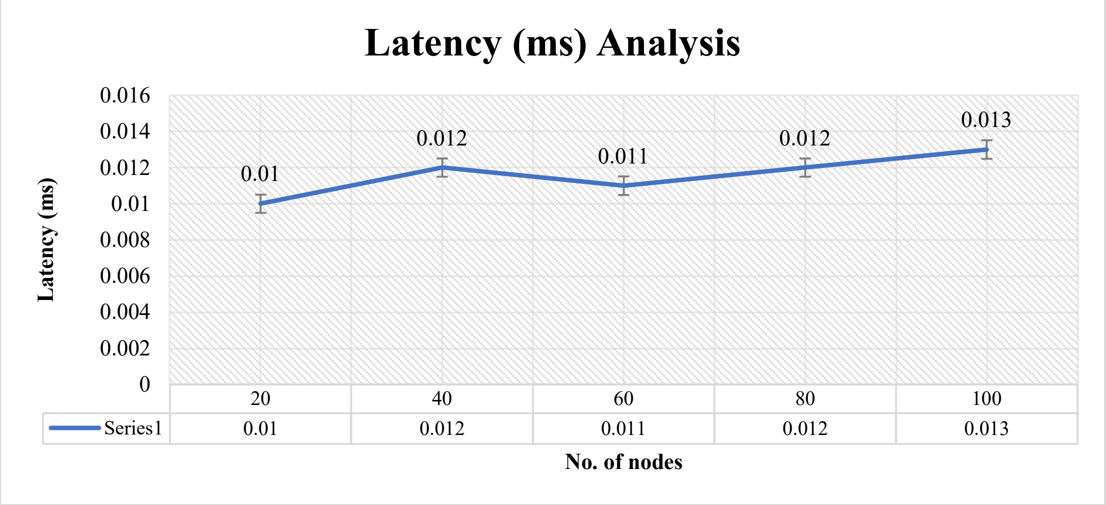


Figure 5: Latency Analysis for the Proposed Block Chain Architecture

Figure 4 illustrates the throughput performance of the proposed blockchain-based architecture. The results demonstrate that the framework consistently achieves stable throughput, ranging between 97% and 99%, even under varying conditions. As shown in Figure 5, the system maintains minimal latency, even with an increasing number of nodes. Across the analysis, latency values remained within the range of 0.01 ms to 0.013 ms, confirming the framework's efficiency in data processing and block validation. Based on these results, it can be concluded that the proposed blockchain architecture is highly suitable for smart home applications. Its ability to deliver high throughput with negligible latency, alongside strong privacy and security mechanisms, makes it an effective and scalable solution for next-generation IoT-enabled smart environments.

IV. CONCLUSION

This study introduces a blockchain-based secure gateway architecture designed for smart home settings and IoT applications, highlighting the significance of privacy, integrity, and authentication. The proposed system guarantees tamper-resistant data management and reliable communication by combining blockchain with diverse IoT devices and gateways. The integration of the SHA-2 encryption technique fulfils classification and validation criteria, while systematic pre-processing and transformation improve the consistency of stored and transferred data. The assessment of three distinct scenarios validated the architecture's practicality and showcased its superiority over traditional methods regarding security and dependability. Nevertheless, the paper acknowledges that blockchain activities may bring computational complexity, possibly affecting performance in resource-limited environments. To address this difficulty, future strategies involve the implementation of edge computing-based offloading methods to enhance resource efficiency. The suggested system offers a scalable and robust approach to safeguarding next-generation smart home IoT infrastructures.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

REFERENCES

[1]. R. Sun, J. Xi, C. Yin, J. Wang, G.J. Kim, "Location privacy protection research based on querying anonymous region construction for smart campus," Mobile Information Systems, vol. 2018, no. 1, pp. 1-11, 2018.

[2]. R.J. Robles, T. H. Kim, D. Cook, S. Das, "A review on security in smart home development," International Journal of Advanced Science and Technology, vol.15, pp. 1-10, 2010.

[3]. J.H. Park, M.M.Salim, J.H. Jo, J.C.S.Sicato, S. Rathore, J.H. Park, "CIoT-Net: a scalable cognitive IoT based smart city network architecture," Human-centric Computing and Information Sciences, vol. 9, no. 1, pp. 1–29, 2019.

[4]. J. Wang, Y. Gao, W. Liu, A.K. Sangaiah, H.J. Kim "Energy efficient routing algorithm with mobile sink support for wireless sensor networks," Sensors, vol. 19, no. 7, pp. 1468–1494, 2019.

[5]. Y. Mittal, P. Toshniwal, S. Sharma, D. Singhal, R. Gupta, V.K. Mitta, "A voice-controlled multi-functional smart home automation system," In: 2015 Annual IEEE India conference, pp.1-6, 2015.

[6]. M. Schiefer "Smart home definition and security threats," Ninth International Conference on IT security incident management & IT forensics, pp. 114-118, 2015.

[7]. B. Xiong, K. Yang, J. Zhao, K. Li, "Robust dynamic network traffic partitioning against malicious attacks," Journal of Network and Computer Applications, vol. 87, pp. 20–31, 2017.

[8]. P. Pongle, and G. Chavan, "A survey: attacks on RPL and 6LoWPAN in IoT," International Conference on Pervasive Computing, pp. 1-6, 2015.

[9]. K. Gu, L. Yang, and B. Yin, "Location data record privacy protection based on differential privacy mechanism," *Information Technology and Control,* vol. 47, no. 4, pp. 639–654, 2018

[10]. P.K. Sharma, S. Rathore, J.H. Park, "DistArch-SCNet: blockchain-based distributed architecture with li-fi communication for a scalable smart city network," IEEE Consumer Electronics Magazine, vol. 7, no. 4, pp. 55–64, 2018.

[11]. P.R Wire (2016) Gartner: blockchain and connected home are almost at the peak of the hype cycle. https ://prwir e.com.au/pr/62010 /gartn er-block chain -andco nnect ed-home-are-almos t-at-the-peak-of-the-hype-cycle. Accessed 28 Dec 2019.

[12]. P.K. Sharma, S.Y. Moon, J.H. Park, "Block-VN: a distributed blockchain-based vehicular network architecture in smart city," Journal of Information Processing Systems, vol. 13, no. 1, pp. 184–195, 2017.

[13]. I. Sanchez, R. Satta, I.N. Fovino, G. Baldini, G. Steri, D. Shaw, A. Ciardulli, "Privacy leakages in smart home wireless technologies. In: 2014 international carnahan conference on security technology, 2014.

[14]. T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, B. Amaba, "Blockchain technology innovations," IEEE technology &architecture management conference (TEMSCON), 2017

[15]. S. Rathore, Y. Pan, J.H. Park, "Block DeepNet: a Blockchain-based secure deep learning for IoT network," Sustainability, vol. 11, no. 14, pp. 3960–3974, 2019.