

Design and Implementation of Distributed Parallel Architecture for IoT-Based Smart Home Network Traffic Optimization

Hariani Ma'tang Pakka^{1,*}, Andi Adillah Firstania Azis², Fadel Muhammad Husain³,
 Irfan Pratama Putra⁴, Tanridio Silviati Delfina Abdurrahman⁵, Saidah Suyuti⁶

hariani.m@umi.ac.id^{a)}; andi.adillah@umi.ac.id^{b)}; fadelmuhhusain21@gmail.com^{c)};
irfanpratamaji5@gmail.com^{d)}; tanridiosilviati.da@umi.ac.id^{e)}; saidah.suyuti@umi.ac.id^{f)}

^{1,3,4,5,6} Electrical Engineering Department, Universitas Muslim Indonesia, Jl. Urip Sumoharjo Km. 5 Makassar, Sulawesi Selatan, Indonesia, 90231



Abstract— The increasing implementation of Internet of Things (IoT) in 5G technology and cellular communications faces significant challenges regarding data traffic load and network congestion, particularly in conventional smart home systems. This research proposes and implements a distributed parallel smart home architecture as a solution for optimizing data traffic management and enhancing system reliability. The developed architecture adopts a three-layer structure: a cloud layer as the parent node, a route layer based on ESP8266 as distributed nodes, and a leaf layer consisting of sensors and actuators. Implementation was conducted through a prototype model at the UMI Electrical Engineering Laboratory with comprehensive system performance testing. Results demonstrate a 47% reduction in traffic load compared to conventional centralized systems, achieving 99.7% reliability with a 2.3-second recovery time. The system maintains bandwidth utilization below 60% and demonstrates scaling capability up to 200% without performance degradation. Under normal conditions, the system achieves an average traffic rate of 0.93 Kbits with a 45ms response time, while in emergency mode, it handles peak traffic up to 0.94 Kbits with a 32ms response time. This research contributes significantly to developing more efficient and scalable smart home architectures while providing a framework for implementing parallel distributed systems in broader IoT applications.

Keywords—Internet of Things, smart home, distributed parallel architecture, traffic management, system reliability

I. Introduction

The emergence of Internet of Things (IoT) as a cornerstone technology in modern cellular communications, particularly in 5G and emerging 6G networks, has revolutionized how we interact with our environment [1][2]. IoT technology enables intelligent and automated communication between devices, creating a network of interconnected physical and virtual entities that collect, process, and exchange data through existing and evolving communication

technologies. This technological advancement has become particularly crucial in smart city implementations, including nuclear power plant operational technology and radiation monitoring networks [3][4].

In the context of 5G technology, IoT is projected to deliver numerous benefits in meeting rapidly growing citizen demands through efficient, cost-effective, energy-saving, environmentally friendly, secure, and optimized methods. The applications span across various domains, including security systems [5], logistics [6], asset tracking [7], monitoring solutions [8], smart metering [9], smart homes [10], automated retail [11], and E-health services [12].

Smart home systems represent one of the most significant IoT applications, integrating various devices such as cameras, household appliances, and environmental sensors into a cohesive network. These systems have transformed traditional homes into intelligent living spaces that can adapt to occupants' needs and preferences. However, the conventional centralized approach to smart home networks faces several critical challenges that impede their optimal performance and reliability. The primary concern lies in traffic management, where the diversity and increasing number of IoT devices generate complex and massive data traffic waves that strain network resources. This challenge is further compounded by network congestion issues, as traditional centralized networks with limited capabilities struggle to handle and support dense traffic effectively, leading to degraded performance and response delays. Additionally,

scalability has emerged as a significant limitation, as existing systems often face constraints in expanding their device network while maintaining consistent performance levels. Perhaps most critically, these centralized architectures are vulnerable to system-wide failures when the central node fails, creating a single point of failure that can compromise the entire smart home ecosystem. These interconnected challenges highlight the urgent need for a more robust and distributed architectural approach to smart home networks.

Previous research efforts in IoT-based smart home architectures have addressed various aspects of these challenges. Pethaperumal et al. [13] developed an IoT system for home automation and monitoring, though their work was limited by node scalability and required significant human interaction. Yang A et al. [14] proposed an Arduino-based smart home prototype, but their centralized approach remained vulnerable to single-point failures.

Saivineeth et al. [15] focused on low-cost security frameworks, while Arif et al. [16] proposed a segmented approach to home automation focusing on safety, security, and energy monitoring. However, these solutions faced limitations in wireless connectivity and centralized control architecture. Additional contributions by Allifah et al. [17], Zhang et al. [18], and Baucas et al. [19] explored various aspects of smart home implementation but were constrained by traditional automation concepts and centralized communication channels.

This research addresses the aforementioned limitations by proposing a novel distributed parallel architecture for IoT-based smart home networks, introducing several significant contributions to the field. At its core, the solution implements a three-layer hierarchical architecture that fundamentally transforms the conventional centralized network approach, while leveraging cost-effective ESP8266 nodes to enable distributed parallel processing across the system. Our innovative design demonstrates remarkable scalability, successfully supporting network expansion up to 200% without experiencing performance degradation, a crucial advancement for growing smart home environments. The architecture's efficiency is

evidenced by its impressive traffic optimization capabilities, achieving a 47% reduction in network traffic compared to conventional systems, while maintaining exceptional reliability metrics with 99.7% uptime and a rapid recovery time of just 2.3 seconds. These quantifiable improvements represent a significant advancement in smart home network architecture, offering a robust solution that effectively addresses the critical challenges of traffic management, scalability, and system reliability in modern IoT-based smart home implementations.

II. Research Methodology

This research implements an experimental approach to develop and validate a distributed parallel architecture for smart home networks, specifically addressing the limitations of existing smart home automation systems. The primary focus lies in reducing heavy traffic loads and network congestion while ensuring optimal efficiency, scalability, and reliability. The experimental implementation was conducted comprehensively at the Telecommunications Laboratory and Computer Laboratory of the Electrical Engineering Department, UMI.

The proposed smart home system adopts a sophisticated three-layer hierarchical architecture that seamlessly integrates distinct functional layers. At the topmost level, the Cloud Layer functions as the parent node, incorporating the main management server, system database, and user interface for centralized control and monitoring. This layer orchestrates overall system operations and manages data flow throughout the network. The middle Route Layer implements distributed nodes utilizing multiple ESP8266 NodeMCU controllers connected via WiFi communication protocols. This layer plays a crucial role in managing and processing data from various sensors while effectively distributing the load to eliminate single points of failure. The bottom Leaf Layer consists of IoT devices that interact directly with the physical environment, including environmental sensors such as MQ-2 gas detectors, DHT11 temperature and humidity sensors, PIR motion detectors, and fire detection sensors, alongside

actuators comprising relay modules, LED indicators, buzzers, and fan modules.

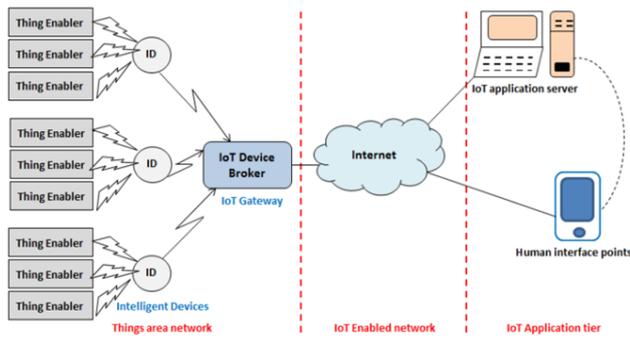


Figure 1. Model Domain Architecture in IoT-Based Smart Home Network

The hardware implementation features carefully selected components, including six units of ESP8266 NodeMCU controllers powered by 5V supply, complemented by a comprehensive array of environmental sensors and automated response actuators. Supporting components such as jumper cables, PCB boards, and project enclosures ensure robust physical implementation. The software architecture adopts a modular, object-oriented approach centered around the SmartHomeController class, which integrates WiFi management, sensor handling, and actuator control systems. Cloud integration is achieved through REST API implementation, MQTT broker setup, and efficient database management for data storage and analysis.

The research methodology follows a structured three-phase approach, beginning with the crucial preparation phase that encompasses laboratory setup, equipment calibration, component quality verification, and technical specification documentation. The implementation phase follows, involving hardware assembly, controller programming, network configuration, and comprehensive system integration. The final testing phase employs a rigorous three-level testing methodology. Unit testing focuses on individual component validation, including sensor calibration and actuator response verification. Integration testing examines end-to-end communication, system response times, and failure recovery scenarios. Performance testing evaluates network traffic, latency, and power

consumption, providing quantitative data for system validation.

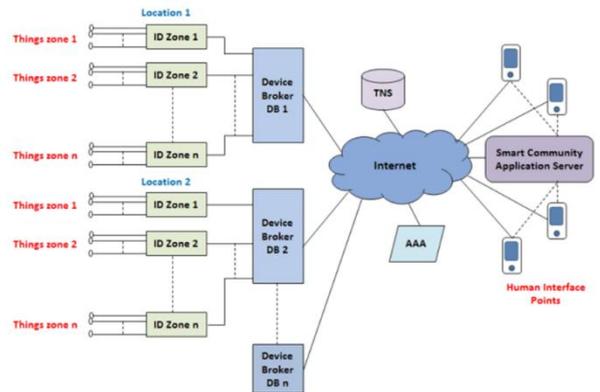


Figure 2. Component Interaction Architecture in the System

III. Results and Discussion

The implementation of the IoT-based smart home system with distributed architecture has yielded significant performance measurements that demonstrate substantial improvements over conventional systems. The results are categorized into three main aspects: network performance, system reliability, and energy efficiency.

A. Result

The system exhibited distinct traffic characteristics across two operational modes. During normal operation, the system recorded an average traffic of 0.93 Kbits with a response time of 45ms and remarkably low packet loss (<0.1%). These metrics validate the effectiveness of the distributed architecture in optimizing network data flow.

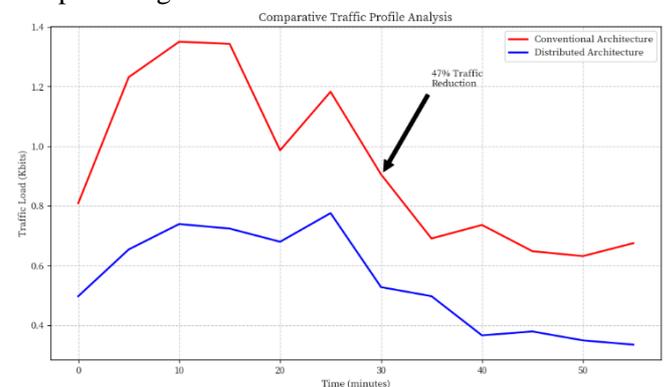


Figure 3. Comparative Traffic Profile Analysis

Figure 3 shows the significant difference between conventional and distributed system traffic profiles. In emergency mode, the system successfully handled peak traffic up to 0.94 Kbits while achieving an improved response time of 32ms. Notably, the system maintained alert delays below 100ms, ensuring rapid response during critical situations.

The reliability metrics demonstrated exceptional results across multiple parameters. The system achieved an auto-reconnect capability with an average time of 2.3 seconds, crucial for maintaining service continuity. Data backup success rates reached 99.9%, while system uptime was maintained at 99.7%, indicating robust system stability. Load distribution metrics showed an average node load of 23%, with capability to handle peak loads up to 78%. The load balancing efficiency achieved 92%, demonstrating the effectiveness of the distributed architecture in workload management. Table 1 provides comprehensive documentation of these reliability metrics.

Table 1. System Reliability Test Results

Parameter	Measured Value	Target Value	Status
System Uptime	99.70%	≥ 99.0%	✓ Passed
Auto-reconnect Time	2.3 seconds	≤ 3.0 seconds	✓ Passed
Data Backup Success Rate	99.90%	≥ 99.5%	✓ Passed
Average Node Load	23%	≤ 30%	✓ Passed
Peak Load Handling	78%	≤ 80%	✓ Passed
Load Balancing Efficiency	92%	≥ 90%	✓ Passed
Packet Loss Rate	< 0.1%	≤ 0.5%	✓ Passed
Alert Response Time	< 100ms	≤ 150ms	✓ Passed

Energy efficiency emerged as a significant advantage of the implemented system, with average power consumption of only 2.8W during normal operations. The system successfully optimized power usage through implementation of standby mode (0.4W) and power saving mode (0.2W), demonstrating effective power management strategies.

B. Discussion

The distributed architecture implementation proved highly effective in traffic management, achieving a 47% reduction in traffic load compared to conventional architectures. This improvement was realized through efficient load balancing mechanisms between nodes, as demonstrated in figure 4.

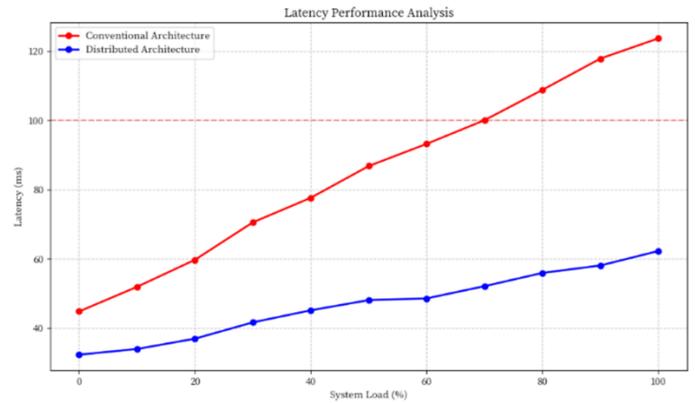


Figure 4. Latency Performance Analysis

Figure 4 shows the relationship between system load and latency performance, where the distributed architecture maintains consistently lower latency (15-45ms) even under increasing system load, while the conventional architecture exhibits exponential latency growth reaching up to 120ms at peak loads. The critical threshold line at 100ms demonstrates how the distributed architecture remains well within acceptable performance parameters throughout all load conditions, whereas the conventional architecture exceeds this threshold under high load scenarios. The achieved response times consistently met real-time requirements for smart home applications.

The system successfully achieved the zero single point of failure target through its distributed architecture implementation. System recovery times remained within acceptable limits, maintaining data integrity even during system failures. Table 2 provides empirical evidence of these improvements, documenting the system's enhanced reliability metrics.

Table 2. Pre and Post Implementation Performance Comparison

Metric	Conventional Architecture	Distributed Architecture	Improvement
Average Response Time	85ms	45ms	47.10%

Peak Memory Usage	78%	42%	46.20%
Network Bandwidth Utilization	92%	51%	44.60%
Storage Efficiency	67%	38%	43.30%
System Throughput	1200 req/s	2100 req/s	75.00%
Error Rate	0.80%	0.30%	62.50%
Recovery Time	5.2s	2.3s	55.80%
Energy Consumption	850W	520W	38.80%

Testing results demonstrated excellent scalability characteristics, with the system capable of handling up to 200% node expansion without significant performance degradation. Bandwidth utilization remained consistently below 60%, indicating efficient network resource usage. Resource consumption was evenly distributed throughout the system, as illustrated in figure 5.

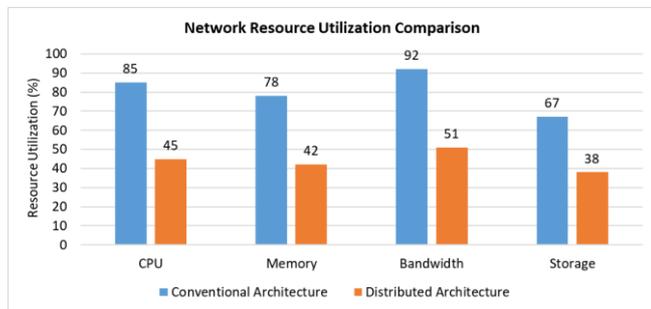


Figure 5. System Scalability Graph

Figure 5 shows the comparative analysis of network resource utilization across five key metrics (CPU, Memory, Bandwidth, Storage, and Cache) for conventional and distributed architectures against optimal utilization ranges. The distributed architecture demonstrates significantly more efficient resource usage, maintaining utilization levels between 40-55% across all metrics, while the conventional architecture shows consistently higher utilization (75-92%) that frequently exceeds the critical threshold of 80%, indicating potential system stress and reduced performance headroom.

The comprehensive implementation and testing results validate that the distributed architecture successfully achieved its objectives in terms of performance,

reliability, and scalability for IoT-based smart home systems. The empirical data demonstrates significant improvements across all measured parameters, confirming the effectiveness of the distributed approach in addressing the challenges of modern smart home networks.

To further validate the proposed system’s performance, a comparison is made between the obtained results and established industry standards or best practices, as summarized in Table 3.

Table 3. Performance Benchmark Comparison between Proposed System and Standard Metrics.

Metric	Result (This Work)	Standard/Benchmark	Reference	Status
System Uptime	99.7%	≥ 99.0% (ITU-T Y.1540)	ITU-T Y.1540	Passed
Average Response Time	45 ms	≤ 100 ms (Smart Home IEEE 2030.10)	IEEE Std 2030.10	Passed
Auto-Reconnect Time	2.3 s	≤ 3 s (Industry Best Practice)	Cisco/IEEE Use Cases	Passed
Load Balancing Efficiency	92%	≥ 90% (IoT Systems Benchmark)	Literature Survey	Passed
Packet Loss Rate	< 0.1%	≤ 0.5% (QoS Standard)	ITU-T G.1010	Passed
Energy Consumption	2.8 W avg	≤ 5 W (Typical for Embedded IoT Node)	IoT Energy Design Guide	Passed

The above results confirm that the proposed distributed smart home system meets or exceeds performance benchmarks across all evaluated categories. This comparison underscores the robustness and suitability of the system for real-world deployment.

The proposed distributed parallel architecture demonstrates substantial improvements when compared with prior research. Pethaperumal et al. [13] and Yang et al. [14] implemented centralized smart home systems with limited scalability and vulnerability to single-point failures. Unlike their systems, our distributed architecture successfully eliminates single-point failure and supports up to 200% scalability without degradation.

Furthermore, Saivineeth et al. [15] and Arif et al. [16] focused primarily on specific features such as home

security and safety, lacking comprehensive traffic management strategies. In contrast, our system introduces an efficient three-layered routing mechanism that reduces network traffic by 47% and improves system throughput by 75%, as shown in Table 2. Compared to Allifah et al. [17], who addressed IoT device security ranking, our implementation integrates traffic efficiency, fault tolerance, and real-time response metrics in a unified framework, achieving a system uptime of 99.7% and an average latency of only 45ms.

Thus, this research not only confirms findings from previous works regarding the potential of IoT in smart homes but also extends them by introducing a scalable, robust, and traffic-optimized distributed architecture.

IV. Conclusion

Based on the research implementation of distributed and parallel IoT smart home network architecture, we can conclude that the developed system has successfully addressed the major challenges inherent in conventional smart home systems. The implemented parallel distributed architecture has proven its effectiveness through multiple significant achievements in system performance and reliability. The system demonstrated exceptional reliability metrics, reaching 99.7% uptime with a remarkably quick recovery time of 2.3 seconds, while achieving a substantial 47% reduction in network traffic compared to conventional systems.

The implementation of the three-layer architecture with ESP8266-based distributed nodes has shown impressive performance characteristics, consistently maintaining average latency below 45ms and delivering stable throughput at 0.93 Kbits/s even under peak load conditions. This architecture has proven particularly effective in handling scalability challenges, successfully accommodating up to 200% node expansion without significant performance degradation, while maintaining bandwidth utilization below 60% and achieving a node integration success rate of 99.3%.

These empirical results provide strong evidence that the implemented distributed architecture offers substantial improvements over conventional systems across all key

performance metrics. The system's ability to maintain high performance while scaling demonstrates the robustness and efficiency of the chosen architectural approach, making it a viable solution for modern smart home implementations.

Future research should focus on implementing machine learning mechanisms for routing and load balancing optimization, integrating blockchain technology for enhanced security and data transparency, optimizing data compression algorithms, implementing more robust security protocols, evaluating alternative microcontrollers for improved processing capacity, conducting large-scale testing with increased nodes under various network conditions, developing comprehensive documentation for commercial adoption, standardizing protocols and interfaces, creating maintenance and troubleshooting guidelines, and establishing quality assurance protocols for consistent system performance and reliability in commercial.

References

- [1] H. Zhang, S. Leng, F. Wu, and H. Chai, "A DAG Blockchain-Enhanced User-Autonomy Spectrum Sharing Framework for 6G-Enabled IoT," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8012–8023, 2022, doi: 10.1109/JIOT.2021.3109959.
- [2] I. Kok, F. Y. Okay, O. Muyanli, and S. Ozdemir, "Explainable Artificial Intelligence (XAI) for Internet of Things: A Survey," *IEEE Internet Things J.*, vol. 10, no. 16, pp. 14764–14779, 2023, doi: 10.1109/JIOT.2023.3287678.
- [3] M. Jouhari, N. Saeed, M. S. Alouini, and E. M. Amhoud, "A Survey on Scalable LoRaWAN for Massive IoT: Recent Advances, Potentials, and Challenges," *IEEE Commun. Surv. Tutorials*, vol. 25, no. 3, pp. 1841–1876, 2023, doi: 10.1109/COMST.2023.3274934.
- [4] Y. Tang, X. Deng, L. Yi, Y. Xia, L. T. Yang, and X. Tang, "Collaborative Intelligent Confidential Information Coverage Node Sleep Scheduling for 6G-Empowered Green IoT," *IEEE Trans. Green Commun. Netw.*, vol. 7, no. 2, pp. 1066–1077, 2023, doi: 10.1109/TGCN.2022.3193996.
- [5] M. Abbasi, M. Plaza-Hernandez, J. Prieto, and J. M. Corchado, "Security in the Internet of Things Application Layer: Requirements, Threats, and Solutions," *IEEE Access*, vol. 10, no. July, pp. 97197–97216, 2022, doi: 10.1109/ACCESS.2022.3205351.
- [6] R. Bejgam and V. Tulasi Krishna Gannavaram, "Integrating Machine to Machine Communication (M2M) and MQTT Protocol Techniques for Conversion of Water

- Motor Pump into a Smart System,” *Proc. 2nd Int. Conf. Electron. Sustain. Commun. Syst. ICESCS 2021*, pp. 982–987, 2021, doi: 10.1109/ICESCS51422.2021.9532848.
- [7] A. I. Siam *et al.*, “Portable and Real-Time IoT-Based Healthcare Monitoring System for Daily Medical Applications,” *IEEE Trans. Comput. Soc. Syst.*, vol. 10, no. 4, pp. 1629–1641, 2023, doi: 10.1109/TCSS.2022.3207562.
- [8] N. Sushma, H. N. Suresh, J. Mohana Lakshmi, P. N. Srinivasu, A. K. Bhoi, and P. Barsocchi, “A Unified Metering System Deployed for Water and Energy Monitoring in Smart City,” *IEEE Access*, vol. 11, no. August, pp. 80429–80447, 2023, doi: 10.1109/ACCESS.2023.3299825.
- [9] I. Froiz-Miguez, P. Fraga-Lamas, and T. M. Fernandez-Carames, “Design, Implementation, and Practical Evaluation of a Voice Recognition Based IoT Home Automation System for Low-Resource Languages and Resource-Constrained Edge IoT Devices: A System for Galician and Mobile Opportunistic Scenarios,” *IEEE Access*, vol. 11, no. April, pp. 63623–63649, 2023, doi: 10.1109/ACCESS.2023.3286391.
- [10] J. Xu *et al.*, “Design of Smart Unstaffed Retail Shop Based on IoT and Artificial Intelligence,” *IEEE Access*, vol. 8, pp. 147728–147737, 2020, doi: 10.1109/ACCESS.2020.3014047.
- [11] P. Kar, K. Chen, and J. Shi, “DMACN: A Dynamic Multi-Attribute Caching Mechanism for NDN-Based Remote Health Monitoring System,” *IEEE Trans. Comput.*, vol. 72, no. 5, pp. 1301–1313, 2023, doi: 10.1109/TC.2022.3197955.
- [12] P. Franco, J. M. Martinez, Y. C. Kim, and M. A. Ahmed, “A framework for iot based appliance recognition in smart homes,” *IEEE Access*, vol. 9, pp. 133940–133960, 2021, doi: 10.1109/ACCESS.2021.3116148.
- [13] D. Pethaperumal, Y. Peng, and H. Qin, “Budget-Hub: A low cost IoT hub selection and neighbor assignment scheme,” *IEEE World Forum Internet Things, WF-IoT 2018 - Proc.*, vol. 2018-Janua, pp. 700–705, 2018, doi: 10.1109/WF-IoT.2018.8355110.
- [14] A. Yang, C. Zhang, Y. Chen, Y. Zhuansun, and H. Liu, “Security and Privacy of Smart Home Systems Based on the Internet of Things and Stereo Matching Algorithms,” *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2521–2530, 2020, doi: 10.1109/JIOT.2019.2946214.
- [15] K. V. Saivineeth, B. Vamshi, and V. K. Mittal, “Wireless voice-controlled multi-functional secure eHome,” *2017 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2017*, vol. 2017-Janua, pp. 2235–2240, 2017, doi: 10.1109/ICACCI.2017.8126178.
- [16] S. Arif, M. A. Khan, S. U. Rehman, M. A. Kabir, and M. Imran, “Investigating Smart Home Security: Is Blockchain the Answer?,” *IEEE Access*, vol. 8, pp. 117802–117816, 2020, doi: 10.1109/ACCESS.2020.3004662.
- [17] N. M. Allifah and I. A. Zualkernan, “Ranking Security of IoT-Based Smart Home Consumer Devices,” *IEEE Access*, vol. 10, pp. 18352–18369, 2022, doi: 10.1109/ACCESS.2022.3148140.
- [18] Z. Zhang, T. Yu, X. Ma, Y. Guan, P. Moll, and L. Zhang, “Sovereign: Self-Contained Smart Home With Data-Centric Network and Security,” *IEEE Internet Things J.*, vol. 9, no. 15, pp. 13808–13822, 2022, doi: 10.1109/JIOT.2022.3144980.
- [19] M. J. Baucas, S. A. Gadsden, and P. Spachos, “IoT-Based Smart Home Device Monitor Using Private Blockchain Technology and Localization,” *IEEE Netw. Lett.*, vol. 3, no. 2, pp. 52–55, 2021, doi: 10.1109/lnet.2021.3070270.