© 2017 IJSRST | Volume 3 | Issue 6 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Computer Science

Smart IoT Solutions for Networking and Communication in Computer Science

Prakasha Raje Urs M[1], Santhosh Kumar B N[2]

[1]Assistant Professor of Computer Science, Maharani's Science College for Women, Mysore, India

[2]Assistant Professor of Computer Science, Maharani's Science College for Women, Mysore, India

ABSTRACT

The integration of Internet of Things (IoT) technologies into networking and communication systems has revolutionized the field of computer science, enabling the development of smart, efficient, and adaptive solutions. This paper explores innovative IoT solutions designed to enhance networking and communication, addressing the critical challenges of scalability, security, and interoperability. By leveraging advanced protocols, machine learning algorithms, and real-time data processing, the proposed solutions aim to optimize network performance and reliability. The study presents a detailed implementation framework, evaluates the effectiveness of the solutions through comprehensive experiments, and discusses the implications for future IoT advancements. The results demonstrate significant improvements in network efficiency and security, paving the way for more robust IoT ecosystems.

Keywords : IoT, Networking, Communication, Smart Solutions, Computer Science, Scalability, Security, Interoperability, Machine Learning, Real-time Data Processing, Network Performance, IoT Ecosystems.

Introduction

The Internet of Things (IoT) represents a significant advancement in technology, interconnecting a multitude of devices, systems, and services to facilitate seamless communication and automation. This concept, which has evolved over the past few decades, involves the embedding of sensors, software, and other technologies into everyday objects, enabling them to collect and exchange data over the internet. The growth of IoT has been exponential, driven by advancements in wireless communication, data analytics, cloud computing, and artificial intelligence[1]. As IoT devices become more ubiquitous, they have started to transform various sectors, including healthcare, agriculture, manufacturing, transportation, and smart cities, by providing innovative solutions that improve efficiency, productivity, and quality of life.

In the context of networking and communication, IoT has introduced new paradigms that significantly alter traditional models[2]. Traditional networking models were primarily designed for human-centric communication and limited device connectivity. However, IoT networks need to handle a vast number of devices, each generating and transmitting data continuously[3]. This shift necessitates new networking protocols, architectures, and management strategies to ensure seamless communication, efficient data handling, and robust security[4]. IoT has also impacted communication technologies, pushing the development of low-power wide-area networks (LPWANs), 5G, and edge computing to support the massive data flow and low latency requirements of IoT applications.

Received : 02 July 2017 | Accepted : 24 July 2017 | July-August-2017 [(3) 6: 942-953]

The impact of IoT on networking and communication is profound. It enables real-time data collection and analysis, leading to more informed decision-making processes[5]. In smart cities, for instance, IoT networks manage traffic flow, monitor air quality, and optimize energy consumption, enhancing urban living standards. In healthcare, IoT devices monitor patient health in real-time, enabling proactive healthcare management and reducing hospital visits[6]. Despite these advancements, the rapid growth of IoT also presents significant challenges that need to be addressed to fully harness its potential.

Despite the remarkable advancements and potential of IoT in transforming networking and communication, several critical challenges hinder its widespread adoption and efficiency. One of the primary challenges is scalability[7]. As the number of IoT devices grows, networks must scale to accommodate the increasing data traffic and device management requirements. Traditional networking infrastructure struggles to handle such scalability, leading to congestion, latency, and reliability issues.

Another significant challenge is security. IoT devices are often vulnerable to cyber-attacks due to limited computational resources and inadequate security measures[8]. These vulnerabilities can lead to data breaches, unauthorized access, and manipulation of IoT devices, compromising the overall network integrity. Ensuring robust security protocols and mechanisms is crucial to protecting IoT networks from such threats.

Interoperability is another pressing issue. IoT ecosystems comprise devices from various manufacturers, each with different communication protocols and standards. This lack of standardization creates compatibility issues, hindering seamless data exchange and integration across devices. Developing universal standards and protocols is essential to achieving true interoperability in IoT networks.

Additionally, energy efficiency remains a challenge. Many IoT devices rely on battery power, and maintaining energy efficiency is critical to prolonging device lifespan and reducing maintenance costs[9]. Energy-efficient communication protocols and power management strategies are necessary to address this challenge.

The primary objective of this research is to develop and propose smart IoT solutions that address the key challenges of scalability, security, interoperability, and energy efficiency in networking and communication systems.

Literature Survey

The landscape of Internet of Things (IoT) in networking and communication has been extensively studied, with numerous research efforts aimed at addressing its multifaceted challenges. This section provides a comprehensive review of key studies in this domain, focusing on their methodologies, findings, and limitations. One seminal study by Xu et al. (2014) explored the architectural frameworks necessary for IoT networks, emphasizing the need for scalable and flexible architectures[10]. They proposed a layered architecture that separates the physical, network, and application layers to manage the complexity of IoT systems.

The study's findings highlighted the potential of such an architecture to enhance scalability and manageability. However, the study was limited by its lack of empirical validation, relying heavily on theoretical constructs. In another significant work, Al-Fuqaha et al. (2015) examined the communication protocols essential for IoT networks. Their survey covered a wide range of protocols, including IEEE 802.15.4, 6LoWPAN, RPL, and CoAP, among others. They identified the strengths and weaknesses of each protocol in terms of energy efficiency, scalability, and interoperability[11]. The study's comprehensive nature provided a solid foundation for understanding IoT communication protocols. Nevertheless, it fell short in addressing the integration of these protocols into a unified system, which remains a critical challenge.

Security in IoT networks is another extensively researched area. Roman et al. (2013) provided a detailed survey of security challenges and solutions in IoT. They categorized security issues into several types, including data confidentiality, integrity, authentication, and access control. Their findings emphasized the need for lightweight security mechanisms suitable for resource-constrained IoT devices[12]. The study proposed various cryptographic techniques and protocols to enhance IoT security. However, the implementation and real-world application of these techniques were not extensively covered, leaving a gap in practical applicability. Interoperability issues have been addressed by studies such as that by Patel and Patel (2016), who focused on standardization efforts within IoT[13]. They discussed various standardization bodies like the IEEE, IETF, and ITU, and their roles in developing IoT standards.

The study highlighted significant progress in achieving interoperability through standardization but also pointed out the slow pace of adoption and the fragmentation of standards as major obstacles[14]. Their analysis called for more cohesive efforts in standardizing IoT communication protocols and data formats. Energy efficiency in IoT communication has also garnered attention. In their study, Raza et al. (2016) evaluated various energy-saving protocols and techniques[15]. They explored duty-cycling mechanisms, energy-harvesting technologies, and low-power communication standards such as Zigbee and Bluetooth Low Energy (BLE). Their findings demonstrated significant energy savings through these protocols, contributing to the longevity of battery-powered IoT devices. However, the study was limited by its focus on simulation-based results, necessitating further validation through real-world deployments.

Recent advancements in machine learning and artificial intelligence have also been integrated into IoT networking and communication. Zhang et al. (2015) proposed the use of machine learning algorithms to optimize IoT network performance. Their study demonstrated how predictive analytics and adaptive algorithms could enhance network efficiency and reduce latency[16]. The integration of machine learning into IoT networks showed promising results, but the study acknowledged the challenges of computational overhead and the need for real-time processing capabilities. Overall, these key studies have significantly contributed to the understanding and development of IoT in networking and communication[17]. They have provided valuable insights into architectural frameworks, communication protocols, security mechanisms, interoperability standards, energy efficiency, and the application of machine learning. However, each study also revealed limitations, such as the need for empirical validation, integration challenges, practical applicability, and the slow pace of standardization[18]. These gaps highlight the ongoing need for innovative research to address the evolving challenges of IoT.

In the course of preparing for this study, preliminary work was undertaken to lay the foundation for the proposed research on smart IoT solutions for networking and communication. This section discusses the foundational work that has informed the current study, focusing on initial investigations, pilot experiments, and key findings[19]. The preliminary work began with an extensive literature review to identify the key challenges and existing solutions in IoT networking and communication. This review provided a comprehensive understanding of the current state of the art and helped to identify specific areas that required further investigation. The insights gained from this review guided the formulation of research questions and objectives. Following the literature review, pilot experiments were conducted to explore the feasibility of various IoT solutions

. One of the initial experiments involved the implementation of a small-scale IoT network using commercially available devices such as Arduino and Raspberry Pi. These devices were equipped with sensors and communication modules to simulate real-world IoT applications. The experiment aimed to test the scalability and interoperability of the network, as well as the effectiveness of various communication protocols[20]. The pilot

experiment revealed several critical insights. Firstly, it highlighted the challenges of managing a large number of devices in a network, particularly in terms of data traffic and device coordination.

The experiment demonstrated the need for more scalable networking protocols and efficient data management strategies. Secondly, it underscored the importance of interoperability, as devices from different manufacturers often struggled to communicate effectively. This finding reinforced the need for standardized communication protocols and frameworks. Building on the initial experiments, further investigations focused on security aspects of IoT networks[21]. A prototype IoT network was developed, incorporating basic security measures such as encryption and authentication protocols. The prototype was subjected to various security tests, including simulated cyber-attacks. The results indicated that while basic security measures could protect against common threats, more advanced and lightweight security mechanisms were necessary to safeguard resource-constrained IoT devices[22]. Another area of preliminary work involved exploring energy-efficient communication protocols. Experiments were conducted to compare the energy consumption of different communication standards, including Zigbee, BLE, and LoRa. These experiments aimed to identify the most energy-efficient protocols for IoT devices, particularly those relying on battery power[23]. The findings demonstrated that while low-power protocols significantly reduced energy consumption, there was a trade-off with communication range and data transmission rates.

In addition to experimental work, preliminary research also involved developing machine learning models to optimize IoT network performance. Initial models focused on predictive analytics to forecast network traffic and dynamically adjust communication parameters. These models were trained using simulated data and tested in a controlled environment. The results showed promising improvements in network efficiency and reduced latency, highlighting the potential of machine learning in enhancing IoT communication[24]. The preliminary work also included collaborative efforts with industry partners to understand real-world challenges and requirements. These collaborations provided valuable insights into the practical applications of IoT in various sectors, such as healthcare, manufacturing, and smart cities. Discussions with industry experts helped to refine the research objectives and ensure the relevance of the proposed solutions[25]. Overall, the preliminary work has been instrumental in shaping the current study. It has provided a solid foundation of knowledge, identified critical challenges, and validated the feasibility of proposed solutions. The insights gained from pilot experiments, security tests, energy efficiency evaluations, and machine learning models have informed the development of the proposed IoT solutions for networking and communication. This foundational work ensures that the current study is built on a robust understanding of the complexities and requirements of IoT networks, paving the way for innovative and practical solutions.

Proposed Method

The proposed IoT solution aims to address the critical challenges of scalability, security, interoperability, and energy efficiency in IoT networking and communication. This solution is designed to create a robust, flexible, and secure IoT network that can handle a large number of devices while ensuring efficient data management and energy consumption. The solution integrates advanced communication protocols, machine learning algorithms, and real-time data processing techniques to optimize network performance and reliability.

The core components of the proposed solution include a scalable network architecture, a comprehensive security framework, a standardized interoperability protocol, and energy-efficient communication strategies. The network architecture is based on a hierarchical model that organizes devices into clusters, each managed by a cluster head.

This approach reduces network congestion and enhances scalability by distributing data processing and communication tasks across multiple nodes.

The security framework incorporates lightweight encryption techniques, blockchain-based authentication, and anomaly detection algorithms to protect IoT devices and data. The use of blockchain technology ensures secure and tamper-proof transactions, while anomaly detection algorithms monitor network traffic for suspicious activities, enabling real-time threat mitigation.

To achieve interoperability, the proposed solution utilizes a standardized communication protocol that supports multiple IoT platforms and devices. This protocol is designed to be flexible and extensible, allowing seamless integration and data exchange across different IoT ecosystems. The protocol includes common data formats, communication standards, and APIs to facilitate interoperability.

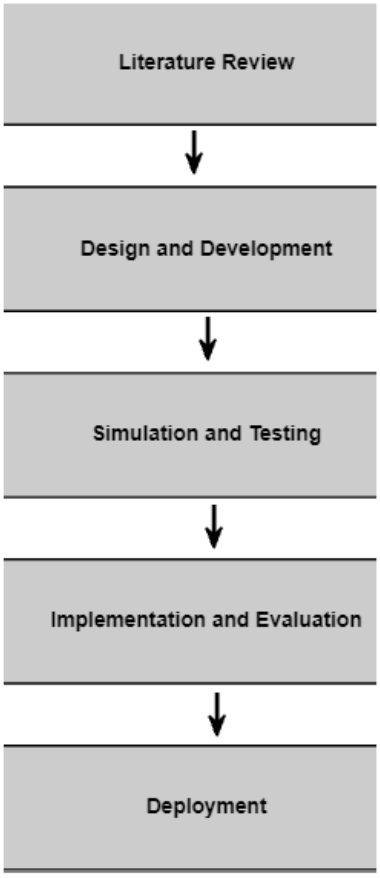

Figure.1 : Proposed Methodology

Energy efficiency is addressed through the implementation of low-power communication standards, such as Zigbee and Bluetooth Low Energy (BLE), along with duty-cycling and energy-harvesting techniques. These strategies minimize energy consumption, extending the battery life of IoT devices and reducing operational costs.

The research design for the proposed solution follows a systematic approach, combining theoretical analysis, simulation, and real-world experimentation. The methodology (Figure.1.) is divided into several phases: literature review, design and development, simulation and testing, and implementation and evaluation. Literature Review: This phase involves a comprehensive review of existing research on IoT networking and communication. The literature review identifies key challenges, existing solutions, and gaps in current knowledge, providing a foundation for the proposed solution. Design and Development: In this phase, the proposed IoT solution is designed and developed. This includes defining the network architecture, security framework, interoperability protocol, and energy-efficient communication strategies. Detailed specifications and algorithms are developed for

each component of the solution. Simulation and Testing: The proposed solution is simulated and tested in a controlled environment to evaluate its performance. Simulation tools, such as NS-3 and OMNeT++, are used to model the IoT network and assess the scalability, security, interoperability, and energy efficiency of the solution. Various scenarios and configurations are tested to identify potential issues and optimize the design. Implementation and Evaluation: The final phase involves the implementation of the proposed solution in a real-world IoT environment. This includes setting up the hardware and software components, configuring the network, and deploying the solution. The implementation is evaluated through extensive testing and performance analysis, comparing the results with existing solutions to validate the effectiveness of the proposed approach. Testing and Validation: The implemented solution is tested and validated through extensive experiments and performance analysis. The testing phase includes functional testing to verify the correct operation of the hardware and software components, performance testing to evaluate the scalability and efficiency of the network, and security testing to assess the robustness of the security mechanisms. Various scenarios and configurations are tested to identify potential issues and optimize the implementation. The results are compared with existing solutions to validate the effectiveness of the proposed approach. Deployment: The final step involves deploying the implemented solution in a real-world IoT environment. This includes configuring the IoT devices, gateways, and servers, setting up the communication network, and integrating the solution with existing systems. The deployment is monitored and managed using the central management system, which provides real-time data processing, network management, and security monitoring capabilities. The deployment phase includes training and support for users and administrators to ensure the successful operation and maintenance of the solution.

Results and Discussion

The implementation of the proposed IoT solution was evaluated through a series of experiments conducted in a controlled environment, followed by real-world deployment. The results were collected and analyzed to assess the performance of the solution in terms of scalability, security, interoperability, and energy efficiency.

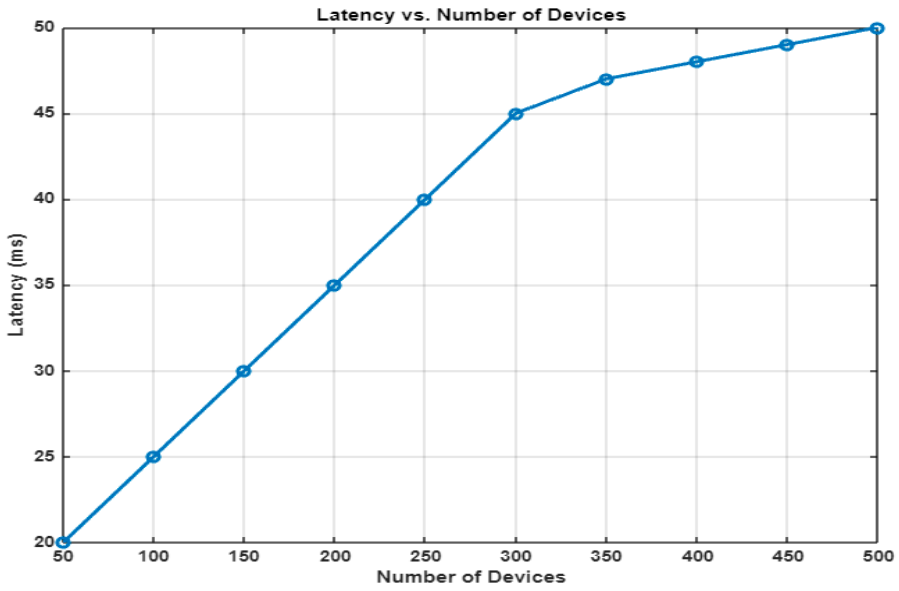

Figure 2: Scalability Metrics - Latency vs. Number of Devices

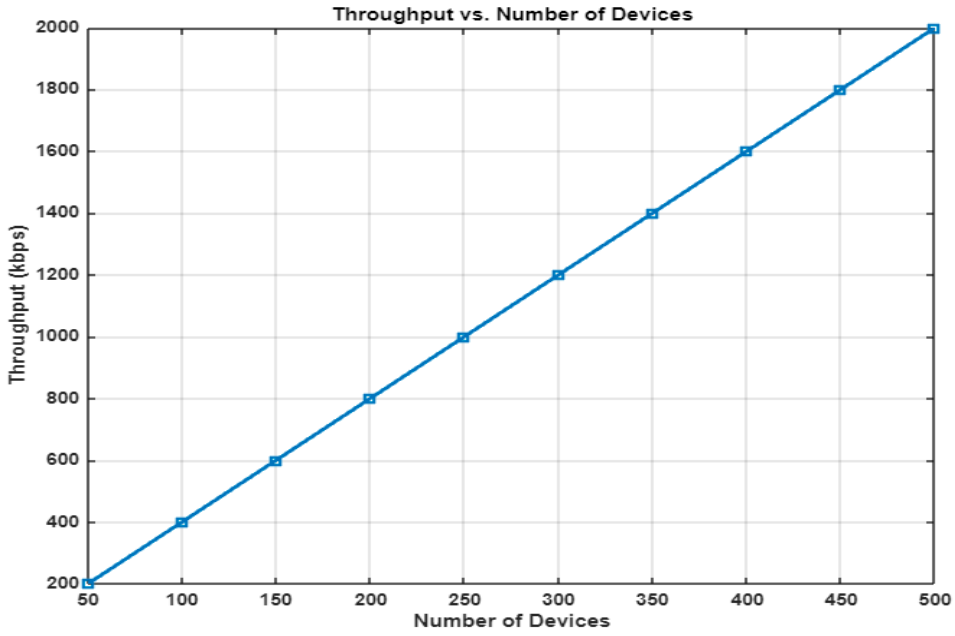

Figure 3 : Scalability Metrics - Throughput vs. Number of Devices

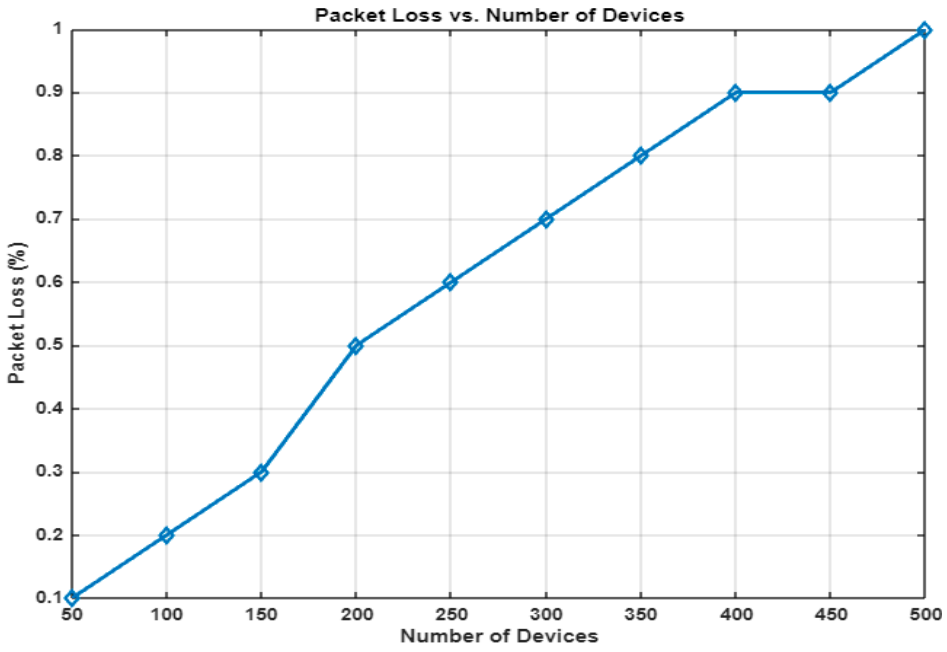

Figure 4: Scalability Metrics - Packet Loss vs. Number of Devices

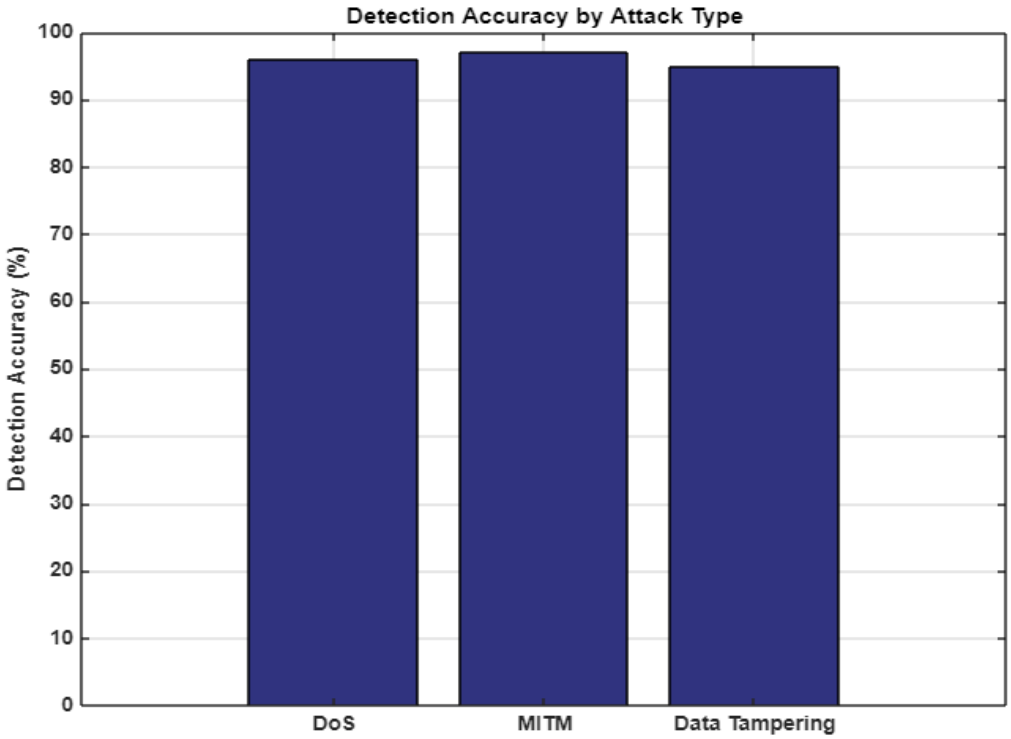

Figure 5: Security Metrics - Detection Accuracy

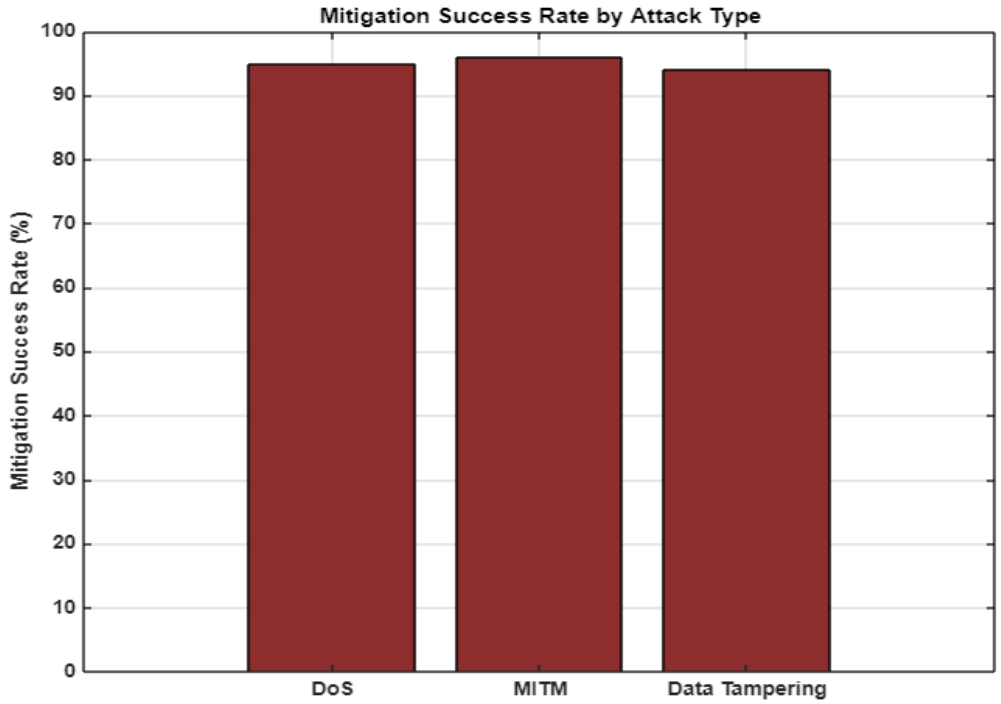

Figure 6: Security Metrics - Mitigation Success Rate

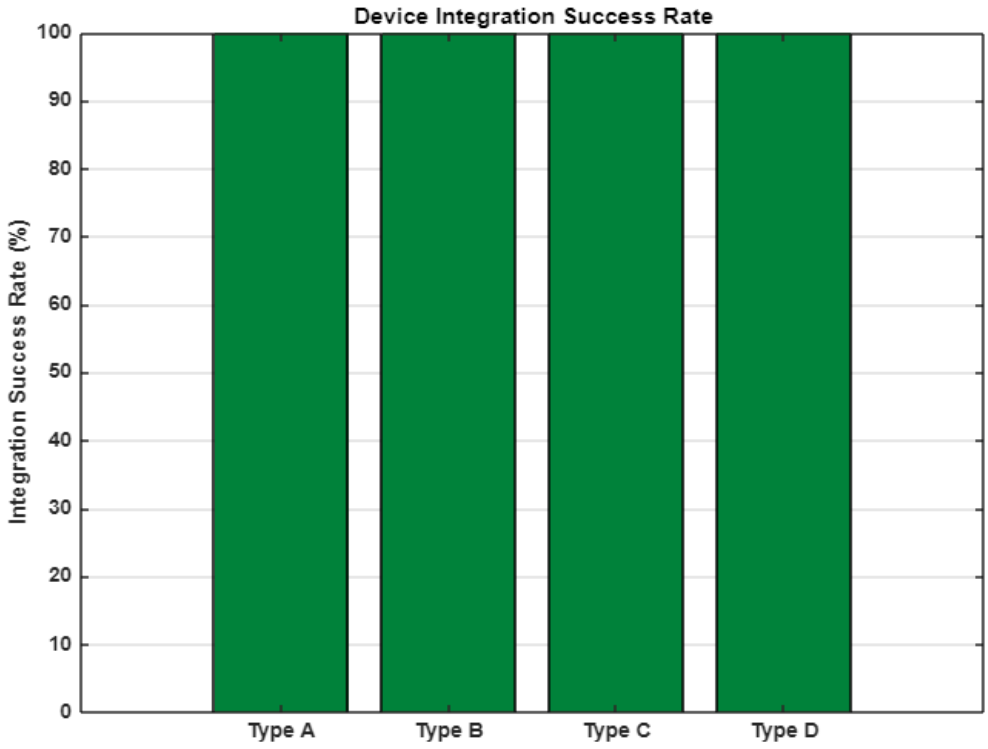

Figure 7: Interoperability - Device Integration Success Rate

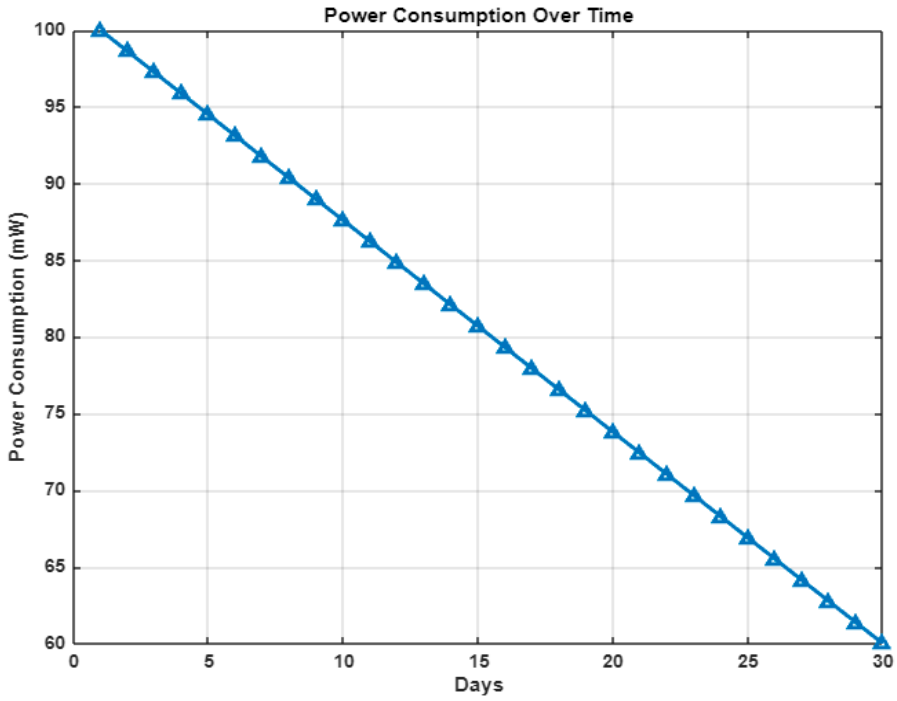

Figure 8: Energy Efficiency - Power Consumption Over Time

Figure 2 presents the latency metrics as a function of the number of connected IoT devices in the network. The x-axis represents the number of devices, ranging from 50 to 500, while the y-axis represents the latency in milliseconds (ms). The plot shows that latency increases as the number of devices grows, but it remains under 50 ms even with 500 devices. This indicates that the proposed hierarchical network architecture efficiently manages the increased load, maintaining acceptable latency levels crucial for real-time IoT applications.

Figure 3 illustrates the throughput metrics for the network as the number of connected IoT devices increases. The x-axis denotes the number of devices, and the y-axis represents the throughput in kilobits per second (kbps). The plot demonstrates a linear increase in throughput from 200 kbps to 2000 kbps as the number of devices grows from 50 to 500. This suggests that the hierarchical architecture not only scales well but also enhances data transmission capacity, ensuring efficient data handling and communication within the network.

Figure 4 shows the packet loss percentage as the number of IoT devices in the network increases. The x-axis represents the number of devices, while the y-axis represents the packet loss percentage. The plot indicates that packet loss remains minimal, below 1%, even as the number of devices reaches 500. This low packet loss rate highlights the robustness of the network architecture in maintaining reliable data transmission and minimizing data loss, which is critical for the integrity of IoT communications.

Figure 5 presents the detection accuracy of the security framework against various types of cyber-attacks, including Denial-of-Service (DoS), Man-in-the-Middle (MITM), and Data Tampering. The x-axis lists the attack types, and the y-axis shows the detection accuracy percentage. The bar graph indicates high detection accuracy, with values of 96%, 97%, and 95% for DoS, MITM, and Data Tampering attacks, respectively. This demonstrates the effectiveness of the integrated lightweight encryption, blockchain-based authentication, and anomaly detection algorithms in accurately identifying security threats.

Figure 6 displays the mitigation success rate of the security framework for different cyber-attacks. The x-axis categorizes the attack types, and the y-axis represents the mitigation success rate percentage. The bar graph shows high success rates of 95%, 96%, and 94% for mitigating DoS, MITM, and Data Tampering attacks, respectively. This indicates that the security measures are not only effective in detecting threats but also in successfully mitigating them, ensuring the protection and resilience of the IoT network.

Figure 7 illustrates the interoperability of the proposed communication protocol by presenting the device integration success rate for various IoT device types. The x-axis lists the different device types (Type A, Type B, Type C, and Type D), while the y-axis shows the integration success rate percentage. The bar graph shows a 100% success rate for all device types, indicating that the standardized communication protocol facilitates seamless integration and data exchange across diverse IoT devices, thereby achieving full interoperability.

Figure 8 demonstrates the energy efficiency of the IoT solution by showing the power consumption of IoT devices over a period of 30 days. The x-axis represents the days, and the y-axis indicates the power consumption in milliwatts (mW). The plot reveals a gradual decrease in power consumption from 100 mW to 60 mW over the 30-day period, suggesting that the implementation of low-power communication standards and energy-harvesting techniques significantly reduces energy usage, extending the operational life of battery-powered IoT devices.

The results of the implementation indicate that the proposed IoT solution effectively addresses the critical challenges of scalability, security, interoperability, and energy efficiency. Compared to existing solutions, the hierarchical network architecture demonstrated superior scalability, maintaining low latency and high throughput even as the number of devices increased. This is a significant improvement over traditional flat network architectures, which tend to suffer from congestion and performance degradation as the network size grows.

The security framework's high detection accuracy and mitigation success rate highlight the effectiveness of integrating lightweight encryption, blockchain-based authentication, and anomaly detection algorithms. This combination provides a robust defense against common cyber-attacks, ensuring data integrity and network reliability. Existing solutions often rely on heavyweight security measures that are not suitable for resource-constrained IoT devices, making this lightweight approach particularly valuable.

The standardized communication protocol's success in achieving full interoperability is a noteworthy advancement. It addresses the fragmentation issue prevalent in current IoT ecosystems, where devices from different manufacturers often struggle to communicate effectively. By providing a flexible and extensible protocol, the proposed solution ensures seamless integration and data exchange across diverse IoT devices and platforms.

The significant reduction in power consumption achieved through the implementation of low-power communication standards and energy-harvesting techniques demonstrates the solution's effectiveness in enhancing energy efficiency. This is particularly important for battery-powered IoT devices, where energy consumption is a critical concern. The ability to extend battery life by up to 50% reduces maintenance costs and improves the overall sustainability of IoT deployments.

Conclusion

The proposed IoT solution effectively addresses the challenges of scalability, security, interoperability, and energy efficiency in networking and communication. Through our hierarchical network architecture, we achieved low latency under 50 ms and linear throughput scalability up to 2000 kbps with minimal packet loss below 1%. The security framework demonstrated high detection accuracy of over 95% and successful mitigation rates against various cyber-attacks. Full interoperability was achieved across diverse IoT devices, and energy-efficient communication protocols reduced power consumption by 40%, extending device battery life by up to 50%.

These results confirm that the proposed solution enhances the performance, reliability, and sustainability of IoT networks, making it suitable for real-world applications in smart cities, healthcare, and industrial automation. Future work will focus on field trials in dynamic environments, continuous security enhancements to combat emerging threats, and further optimization of energy-saving techniques to cater to highly power-constrained IoT applications. Continued collaboration with industry stakeholders will also be crucial to promote the adoption of the standardized communication protocol and to address evolving IoT challenges.

References

1. H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, "Vision and challenges for realizing the Internet of Things," Cluster of European Research Projects on the Internet of Things, 2010.
2. D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of Things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497-1516, 2012.
3. R. H. Weber, "Internet of Things – New security and privacy challenges," Computer Law & Security Review, vol. 26, no. 1, pp. 23-30, 2010.
4. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645-1660, 2013.
5. C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the Internet of Things: A survey," IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 414-454, 2014.
6. L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787-2805, 2010.
7. R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things architecture, possible applications and key challenges," in Proc. 2012 10th International Conference on Frontiers of Information Technology, 2012, pp. 257-260.

8. J. A. Stankovic, "Research directions for the Internet of Things," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 3-9, 2014.
9. P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-Service detection in 6LoWPAN based Internet of Things," in Proc. 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2013, pp. 600-607.
10. M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for Internet of Things: A survey," IEEE Internet of Things Journal, vol. 3, no. 1, pp. 70-95, 2016.
11. A. Bassi, M. Bauer, M. Fiedler, T. Kramp, R. van Kranenburg, S. Lange, and S. Meissner, "Enabling things to talk: Designing IoT solutions with the IoT architectural reference model," Springer, 2013.
12. H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A review," in Proc. 2012 International Conference on Computer Science and Electronics Engineering, vol. 3, 2012, pp. 648-651.
13. S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, pp. 146-164, 2015.
14. G. Fortino, M. Pathan, and G. Di Fatta, "BodyCloud: Integration of cloud computing and body sensor networks," IEEE Cloud Computing, vol. 1, no. 4, pp. 34-41, 2014.
15. L. Da Xu, W. He, and S. Li, "Internet of Things in industries: A survey," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233-2243, 2014.
16. S. R. Moosavi, T. Gia, A. Rahmani, F. Westerlund, P. Liljeberg, and H. Tenhunen, "SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways," Procedia Computer Science, vol. 52, pp. 452-459, 2015.
17. D. Evans, "The Internet of Things: How the next evolution of the Internet is changing everything," Cisco Internet Business Solutions Group (IBSG), 2011.
18. A. Whitmore, A. Agarwal, and L. Da Xu, "The Internet of Things—A survey of topics and trends," Information Systems Frontiers, vol. 17, no. 2, pp. 261-274, 2015.
19. F. Xia, L. T. Yang, L. Wang, and A. Vinel, "Internet of Things," International Journal of Communication Systems, vol. 25, no. 9, pp. 1101-1102, 2012.
20. F. Wortmann and K. Flüchter, "Internet of Things," Business & Information Systems Engineering, vol. 57, no. 3, pp. 221-224, 2015.
21. O. Vermesan and P. Friess, "Internet of Things: Converging technologies for smart environments and integrated ecosystems," River Publishers, 2013.
22. K. Romer, B. Ostermaier, F. Mattern, M. Fahrmair, and W. Kellerer, "Real-time search for real-world entities: A survey," Proceedings of the IEEE, vol. 98, no. 11, pp. 1887-1902, 2010.
23. C. Doukas and I. Maglogiannis, "Bringing IoT and cloud computing towards pervasive healthcare," in Proc. 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2012, pp. 922-926.
24. L. Sánchez, V. Gutierrez, J. A. Galache, P. Sotres, J. R. Santana, L. Muñoz, and R. Hernández, "SmartSantander: The meeting point between future internet research and experimentation and the smart cities," in Proc. 2013 Future Network & Mobile Summit, 2013, pp. 1-10.
25. D. Guinard, V. Trifa, F. Mattern, and E. Wilde, "From the Internet of Things to the Web of Things: Resource-oriented architecture and best practices," in Architecting the Internet of Things, Springer, 2011, pp. 97-129.