ISSN 2047-3338

Optimizing IoT Ecosystem through Scalable, Secure and Efficient Network Management

Muhammad Aleem Subhani[1], Muhammad Junaid Arshad[2]

[1,2]Department of Computer Science, University of Engineering and Technology Lahore, Pakistan

***Abstract*— The rapid growth of the Internet of Things (IoT) has transformed numerous industries by enabling seamless communication among billions of devices, sensors, and applications. However, traditional network infrastructures struggle to meet the scalability, security, and efficiency demands of these dynamic and expanding ecosystems. Limitations such as increased latency, inefficient resource allocation, and vulnerability to cyber threats hinder the performance and reliability of IoT networks. This study proposes a comprehensive framework to optimize IoT ecosystems by integrating advanced network management techniques. Scalability is addressed through virtualization, network slicing, and dynamic resource allocation, enabling adaptive responses to device proliferation. To strengthen security, the framework incorporates firewalls, Access Control Lists (ACLs), and Intrusion Detection Systems (IDS) for proactive monitoring and mitigation of network threats. Efficiency is improved using load balancing and algorithmic optimization to ensure effective bandwidth usage and resource distribution. The proposed solution is validated using Cisco Packet Tracer simulations, where traditional and virtualized network models are implemented and analyzed under identical conditions. Key performance metrics latency, throughput, packet loss, and resource utilization are measured to evaluate and compare network behavior. Results demonstrate significant improvements across all metrics, confirming the effectiveness of the virtualized approach. This research offers a practical and scalable model for modern IoT applications, including smart cities, healthcare systems, and industrial automation. By addressing the core limitations of existing network infrastructures, the proposed framework facilitates the development of resilient, secure, and energy-efficient IoT environments.**

***Index Terms*— Internet of things (IoT), Software Defined Networks (SDN), NFV (Networp;k Function Virtualization), Network Management, Security, Scalability and Efficiency**

I. INTRODUCTION

THE Internet of Things (IoT) has revolutionized modern industries by enabling seamless interaction between billions of interconnected devices, sensors, and cloud-based applications. These devices facilitate real-time monitoring, data analysis, and automation in domains such as healthcare, smart cities, industrial systems, and agriculture. According to recent projections, the number of connected IoT devices worldwide is expected to surpass 29 billion by 2030, placing unprecedented demand on existing network infrastructures [1]. Despite the enormous potential of IoT, traditional network architectures are not equipped to handle the scale, complexity, and heterogeneity of modern IoT ecosystems. Key limitations such as static configuration, limited bandwidth, manual device management, and vulnerability to cyber threats contribute to inefficient network performance and compromised security [2], [3].

These limitations have prompted the need for innovative and adaptive approaches to IoT network management. To address scalability, technologies like Software-Defined Networking (SDN) and Network Function Virtualization (NFV) have emerged as promising alternatives. SDN decouples the control and data planes, allowing centralized control and dynamic reconfiguration of network resources [4]. NFV complements SDN by replacing traditional hardware-based network functions with virtualized counterparts, enabling flexible and cost-effective deployment [5].

In tandem, these technologies facilitate automated scaling and reduce operational overhead, making them well-suited for dynamic IoT environments. Security in IoT networks is equally critical due to the sensitivity of transmitted data and the wide attack surface created by numerous endpoints. Conventional security measures often fall short in distributed and resource-constrained IoT environments. As a solution, this research integrates Access Control Lists (ACLs), firewalls, and Intrusion Detection Systems (IDS) to monitor network traffic, prevent unauthorized access, and detect anomalies [6], [7].

These mechanisms collectively improve the resilience of the network against evolving cyber threats. Efficiency is another cornerstone of effective IoT network management. Load balancing algorithms and optimized routing protocols help minimize latency and energy responsiveness. By dynamically allocating resources based on real-time demand, networks can operate at optimal efficiency, particularly in large-scale deployments [8].

This paper presents a comparative study between traditional and virtualized network environments simulated using Cisco Packet Tracer. The evaluation is based on key performance metrics: latency, throughput, packet loss, scalability, security, and efficiency. The objective is to demonstrate that virtualization and software-defined techniques significantly outperform traditional approaches in managing IoT systems.

The remainder of this paper is structured as follows: Section II reviews existing literature and highlights current challenges. Section III details the proposed methodology and simulation setup. Section IV presents and analyzes the experimental results. Section V concludes the paper with insights and future research directions.

II. LITERATURE REVIEW

In the literature review section, an extensive overview of previous research was presented. Key findings from various authors who had published papers on the topic were summarized. The section highlighted significant contributions, methodologies employed, and major outcomes reported in the literature. Specific studies were discussed in detail to underline their findings and relevance to the current research.

Table I: Overview of literature review

Author	Focus Area	Methodology	Key Findings
Rahmati, M. (2025)	Security	Federated Learning for IDS	Enables real-time threat detection with privacy-preserving models in IoT
Chaganti, K. C. (2025)	Security	AI-Driven Security Framework & Game Theory	Lightweight and scalable security for IoT ecosystems
Villegas-Ch, W., et al. (2025)	Security & Efficiency	Hybrid AI and Blockchain	Enhances IoT threat detection with combined models
Kakati, A. (2025)	Scalability	Scalable IoT Solutions for Urban Resource Handling	Optimized urban IoT management and allocation
Ramesh, P. N. (2025)	Efficiency & Security	AI-Driven Communication Systems	Enhances secure and efficient IoT communication systems
Bentayeb, Y., et al. (2025)	Security, Efficiency	Blockchain Computing	Improves distributed IoT performance and resilience
Muhammad, M., et al. (2024)	Security	Big Data-Driven IDS	Enables large-scale analysis for anomaly detection in IoT
Kumar, C., & Chittora, P. (2024)	Security & Efficiency	Smart Grid Privacy Framework	Improves privacy and secure communication
Esmaeili, M., et al. (2024)	Security	ML-Assisted Intrusion Detection	Increases IDS detection accuracy for emerging IoT threats
Naz, I., et al. (2024)	Security	Lightweight Encryption	Protects data with minimum computational load
Singamaneni, K. K., et al. (2024)	Security & Efficiency	Q-KPABE Encryption Framework	Achieves secure cloud-based IoT data access control
Mustafa, R., et al. (2024)	Security & Efficiency	Cross-Layer Secure Framework	Enhances energy efficiency and data protection simultaneously
Fernandez-Carames, T. M. (2024)	Security	Quantum-Resistant Cryptography	Improves long-term security in IoT devices against quantum attacks
Abdulkareem et al. (2024)	Security	Anomaly based Network	Effective threat detection and mitigation
Baniya et al. (2024)	Security	Encryption, multi-layer access control	Balanced security and performance
Altalebi & Ibrahim (2024)	Scalability	Network automation	Improved scalability in traditional networks
Ajagbe et al. (2024)	Efficiency	Deep learning for IoT	Improved prediction accuracy in resource allocation
Nilima et al. (2024)	Efficiency	Resource management in constrained environments	Balanced energy consumption and performance
Al-Suhimat et al. (2024)	Security	Security challenges in IoT	Highlighted encryption and device authentication
Belarbi, O., et al. (2023)	Security	Federated Deep Learning for IDS	Enhances anomaly detection performance in IoT networks
Alotaibi, B. (2023)	Security	Edge Computing & AI	Reduces latency in security
Haggag (2023)	Efficiency	IPv6 compression	Enhanced throughput and minimized delays
Park & Lee (2023)	Security, Efficiency	Cloud-based IoT	Secure data optimized communication

Guero et al. (2023)	Scalability Security	Survey on IoT challenges	Identification of critical gaps in IoT systems
Siddiqui et al. (2022)	Security	SDN frameworks	Improved visibility and control in IoT networks
Benomar et al. (2021)	Scalability, Efficiency	OpenStack-based network	Simplified IoT network management
Haji et al. (2021)	Scalability	Comparison of SDN and traditional networks	SDN enables dynamic scalability
Dotan et al. (2021)	Efficiency	Blockchain networking	Transparency and reliability in resource allocation
Alshahrani et al. (2021)	Efficiency	Machine learning-based resource management	Energy and bandwidth optimization
Alam et al. (2021)	Scalability	Software defined-networks	Improved scalability through static allocation
Overmars & Venkatraman (2020)	Security	IoT infrastructure for smart systems	Enhanced security in water monitoring systems

III. RESEARCH METHODOLOGY

In this research, the focus is on improving the scalability, security, and efficiency of IoT ecosystems by transitioning from a Traditional Network to a Virtualized Network Environment (Fig. 1). The aim is to demonstrate, through practical implementation, how Software-Defined Networking (SDN) and Network Functions Virtualization (NFV) reduce operational challenges, optimize resource allocation, and enhance flexibility.

IV. RESEARCH GAP

The review identified several research gaps in existing literature. These gaps included areas that had not been sufficiently explored, inconsistencies in findings, and opportunities for further investigation. The identification of these gaps was crucial for highlighting the need for future research and for justifying the focus of the current study.

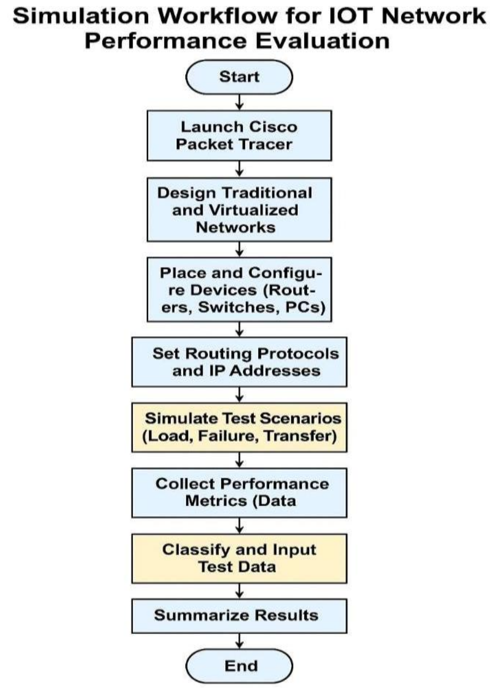

Fig. 1: Graphical Representation of Working System

- Current solutions lack efficiency and scalability in resource-constrained environments [2], [5], [6].
- Need for lightweight and secure systems in various IoT applications [2], [3].
- Limited empirical data on real-world implementations and case studies [1], [4].
- Needs reliable distributed training infrastructure [4].
- Limited scope to city-specific scenarios [9], [2].
- High energy usage in edge devices [8].
- Scalability under network growth needs further testing [10].
- Performance impact under heavy traffic conditions [21].
- Requires high-quality training data sets [13].
- High computational cost for constrained devices [11].
- Limited applicability in dynamic systems [22].

Fig. 1 explains the methodology and entire process of our proposed system, which compares traditional and virtualized network environments. Initially, we design both network architectures using Cisco Packet Tracer simulation tools. In the traditional network, physical devices such as routers and switches are manually configured. For the virtualized network, software-defined networking (SDN) and virtualization technologies like NFV are implemented. Once both networks are set up, a series of predefined test scenarios are run to simulate real-world network operations. During this phase, key performance metrics such as latency, throughput, and CPU usage are recorded. After data collection, the results are analyzed and compared to evaluate performance differences. This process helps in understanding the benefits and drawbacks of each network type, supporting the conclusion of which system is more efficient and scalable.

PSEUDO ALGORITHM

Step 1: *Start*

Step 2: *Launch Cisco Packet Tracer and require devices from the toolse.t*

Step 3: *Design two topology one is traditional and other is virtualized network.*

Step4: *Each network is configured with IP addresses, routing protocols, and end devices.*

Step 5: *Test scenarios are created to simulate data transfer, load handling, and link failures.*

Step 6: *Simulation is executed and packet flow monitored in real-time.*

Step 7: *Performance metrics such as latency, packet delivery rate and throughput are recorded.*

Step 8: *The findings are interpreted to evaluate network scalability, security and efficiency.*

Step 9: *Final results and conclusions are documented for the research study.*

Step 10: *End*

V. SIMMULATION ENVIRONMENT

In this study, Cisco Packet Tracer (version 8.2) was used as the primary simulation platform. It provides a user-friendly interface for designing, configuring, and testing both traditional and virtualized networks. Cisco Packet Tracer supports simulation of various networking protocols, traffic types, and topology customization, making it suitable for performance comparison studies. All simulations were conducted on a system with the following specifications:

- Operating System: Windows 10 (64-bit)
- Processor: Intel Core i7, 2.6 GHz
- RAM: 4 GB
- Storage: 512 GB SSD

These specifications ensured smooth operation and minimized simulation latency due to hardware limitations.

A) Network Design Scenarios

To compare the performance of traditional and virtualized networks, two distinct network models were developed.

Traditional Network Topology

The traditional network was manually configured with physical routing and switching setups. Devices such as routers, switches, and end-user PCs were interconnected using Ethernet cables. Static IP addressing and routing protocols were configured without any form of virtualization.

Virtualized Network Topology

The virtualized network utilized logical segmentation techniques such as VLANs and subnetting. Despite using similar hardware components, the design enabled logical separation of network segments, simulating a cloud or virtual environment. This setup allowed isolation of traffic flows and better resource utilization.

B) Experimental Setup

For each network type, similar configurations and simulation steps were followed:

- IP addressing schemes were uniformly assigned across devices.
- Routing protocols such as RIP or OSPF were configured for internal communication.
- Virtual LANs (VLANs) were created in the virtualized network to simulate departmental isolation.

Simulation scenarios were defined, including:

- File transfers between end devices
- Network congestion tests
- Failover scenarios using disabled links or devices

Each experiment was conducted multiple times to ensure reliability and repeatability.

C) Performance Metrics

To evaluate the performance of each network topology, the following metrics were measured:

- Latency: Time taken for a data packet to travel from source to destination.
- Throughput: Total data successfully delivered over a period, measured in bits per second.
- Packet Loss: Percentage of packets lost during transmission, indicating network reliability.

These metrics were selected to represent both the efficiency and reliability of network performance under similar loads.

D) Data Collection and Analysis

During the simulation process, observational data was collected by monitoring the flow of traffic and network behavior under predefined scenarios. Key performance indicators such as latency, throughput, and packet loss were recorded using built-in monitoring tools within Cisco Packet Tracer.

For consistency, each simulation was repeated multiple times under identical conditions to minimize variance and capture representative results. The collected data was systematically categorized and examined to highlight behavioral trends and discrepancies between the traditional and virtualized network models.

Comparative analysis was conducted by evaluating the performance indicators under controlled conditions, allowing clear identification of strengths and limitations associated with each topology. The findings served as the basis for drawing conclusions regarding network efficiency, reliability, and scalability.

Table II: Results from Traditional Network

Metric	Result	Performance
Latency	58 ms	High
Throughput	2.1 Mbps	Low
Packet Loss	10.8 %	High
Scalability	60%	Low
Security	55%	Low
Efficiency	50%	Low

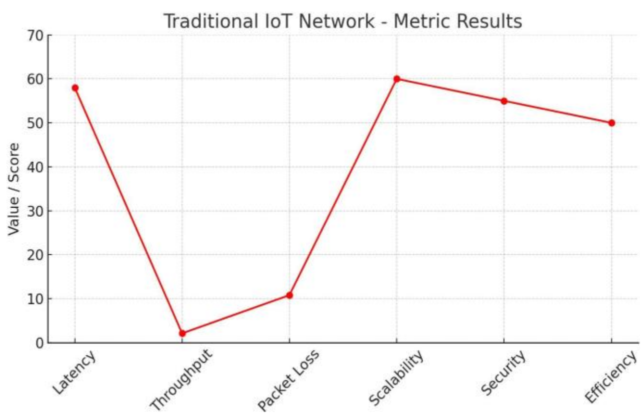

Fig. 2. Traditional IoT Network-Metrics Results

VI. RESULTS

This section outlines the simulation results of traditional and virtualized networks modeled in Cisco Packet Tracer. Both setups were tested under identical scenarios to measure key performance metrics latency, throughput, packet loss as well as qualitative factors like scalability, security, and efficiency. Each simulation was repeated to ensure consistency, and results were averaged. The findings are presented using tables and charts to provide a clear comparison of network performance.

A) Performance Metrics Observed

The performance of each network was evaluated using these primary metrics.

- Latency: Measures the time taken for data to travel from source to destination (ms).
- Throughput: Indicates the rate of successful data transmission over the network, typically measured in Mega bits per second (Mbps).
- Packet Loss: Represents the percentage of data packets that fail to reach their destination (%).
- Scalability: Ability to handle increasing number of devices.
- Security Measures: Ability to detect threats and enforce access control.
- Efficiency: Resource usage and energy optimization.

These metrics were recorded during multiple simulation runs and averaged to ensure reliability and accuracy.

B) Results From Traditional Network

The traditional network topology was developed using a manual configuration approach involving routers, switches, and end-user PCs. All network devices were physically interconnected using Ethernet links within the Cisco Packet Tracer simulation environment. Communication between devices was established using static IP addressing, where IPs were manually assigned to each node without the use of DHCP. Static routing protocols, such as RIP or manually defined route tables, were employed to manage inter-device communication paths.

As a result, the setup lacked dynamic adaptability and had limited capability to handle increasing loads or secure data traffic effectively. The simplicity of the design reflected the baseline IoT deployment served.

C) Results From Virtualized Network

The virtualized network was structured using a combination of VLANs (Virtual Local Area Networks**)** and subnets to achieve logical separation of devices and efficient traffic management within the infrastructure. Each VLAN represented a distinct network segment, allowing isolation of departments or services while still enabling inter-VLAN communication through a router-on-a-stick configuration. This design provided enhanced control over data flow, minimized broadcast traffic, and reduced congestion. Subnetting further supported address management and security. Overall, the topology emulated a scalable and modular network architecture, aligning with modern enterprise and cloud-based IoT systems where flexibility, resource optimization, and scalability are critical. By employing these virtualization techniques, the network demonstrated greater flexibility, scalability, and resilience, making it more suitable for real-world IoT applications where adaptability, reliability, and security are paramount.

Table III: Results from Virtualized Network

Metric	Result	Performance
Latency	21 ms	Low
Throughput	4.2 Mbps	High
Packet Loss	1.4%	Low
Scalability	92 %	High
Security	90 %	High
Efficiency	88%	High

Table IV: Comparative Analysis

Metric	Traditional Network	Virtualized Network	Improvement (%)
Latency	58 ms	21 ms	63.8% ↓
Throughput	2.1 Mbps	4.2 Mbps	100% ↑
Packet Loss	10.8%	1.4%	87% ↓
Scalability	Score: 60% (manual setup)	Score: 92% (dynamic integration)	53.3% ↑
Security	Score: 55% (no ACL/VLANs)	Score: 90% (with ACLs, VLANs, WPA2)	63.6% ↑
Efficiency	Score: 50% (high CPU, no optimization)	Score: 88% (optimized routing, energy)	76% ↑

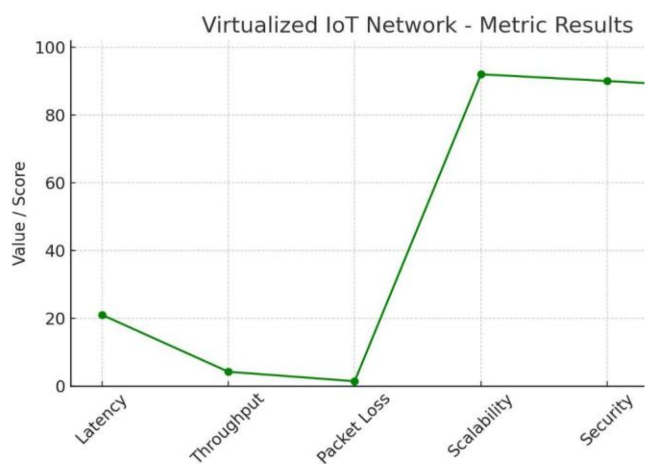

Fig. 3: Virtualized IoT Network-Metrics Results

D) Comparative Analysis

This section presents a direct comparison between the traditional and virtualized IoT network architectures across key performance metrics: latency, throughput, packet loss, scalability, security, and efficiency. The comparative evaluation is based on both simulation observations and quantifiable performance scores recorded during multiple test scenarios. The following table summarizes the performance of both network types:

From the above comparison:

- Latency in the virtualized network is significantly lower, indicating faster data delivery even under load.
- Throughput doubles in the optimized setup due to better resource management and segmentation.
- Packet loss is drastically reduced, enhancing overall reliability.
- Scalability is improved by over 50%, with the virtualized environment allowing seamless integration of devices.
- Security benefits from logical segmentation, access control, and encryption techniques that are absent from the traditional setup.
- Efficiency is noticeably higher due to reduced CPU usage and energy-aware configurations.

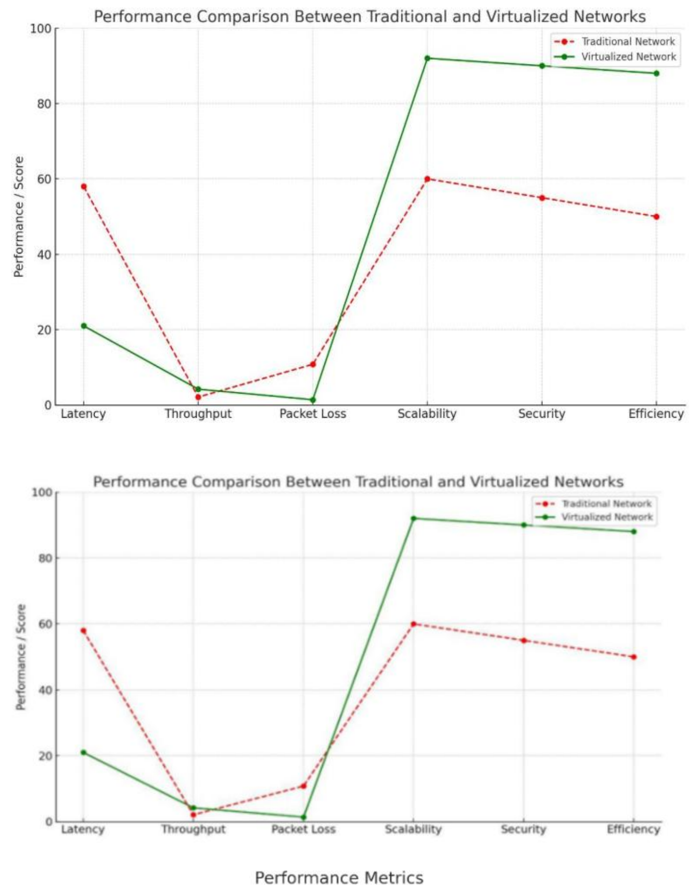

Fig. 4. Performance Comparison B/W Traditional and Virtualized Networks

These results validate the hypothesis that virtualized, software-defined networking approaches provide superior performance, especially for complex and dynamic IoT ecosystems. The performance improvements across all metrics confirm that the proposed network model is well-suited for modern IoT applications demanding scalability, security, and operational efficiency.

VI. CONCLUSIONS AND FUTURE DIRECTIONS

This research addressed the critical limitations in traditional IoT network infrastructures by proposing a virtualized network model that leverages Software-Defined Networking (SDN), Network Function Virtualization (NFV), and logical segmentation techniques. The goal was to optimize IoT ecosystems in terms of scalability, security, and efficiency. Simulation results demonstrated that the traditional network suffered from high latency (58 ms), limited throughput (2.1 Mbps), and considerable packet loss (10.8%), along with poor scalability and security due to static configurations and lack of isolation. In contrast, the proposed virtualized model significantly improved performance: latency was reduced to 21 ms, throughput doubled to 4.2 Mbps, and packet loss dropped to 1.4%. Furthermore, scalability, security, and efficiency scores improved by over 50%, highlighting the benefits of dynamic routing, access control mechanisms, and optimized resource utilization. These findings validate the hypothesis that advanced network management techniques substantially enhance IoT network performance. The results support the thesis objectives and provide a robust foundation for designing intelligent, adaptable, and secure IoT infrastructures suitable for modern applications such as smart cities, industrial automation, and healthcare.

For future work, implementing this model in real-world scenarios is essential to evaluate practical effectiveness and limitations. Further enhancements can include integration with artificial intelligence for predictive traffic management, anomaly detection, and autonomous fault recovery. Additionally, energy efficiency can be improved through the adoption of green networking practices and low-power hardware. Enhancing security with zero-trust models, blockchain-based authentication, and quantum-resistant encryption is also a promising direction. Finally, combining edge and cloud computing technologies may further extend the model's capabilities by offering scalable computation closer to data sources, reducing latency and bandwidth usage.

In conclusion, this research contributes a practical and scalable framework for optimizing IoT network management and opens the door for continued innovation in building resilient for scalability, efficient, and secure IoT ecosystems.

REFERENCES

[1] Chaganti, K. C. (2025). A Scalable, Lightweight AI- Driven Security Framework for IoT Ecosystems: Optimization and Game Theory Approaches. *IEEE Access*

[2] Villegas-Ch, W., Govea, J., Gurierrez, R., & Mera- Navarrete, A. (2025). Optimizing Security in IoT Ecosystems Using Hybrid Artificial Intelligence and Blockchain Models: A Scalable and Efficient Approach for Threat Detection. *IEEE Access*.

[3] Kakati, A. (2025). Scalable IoT Solutions for Urban Resource Management. *Research Annals of Industrial and Systems Engineering*, *2*(1), 36-47.

[4] Ramesh, P. N. (2025). Advancements in AI-Driven Communication Systems: Enhancing Efficiency and Security in Next-Generation Networks.

[5] Bentayeb, Y., Chaoui, K., & Badir, H. (2025). Integrating Blockchain and Edge Computing: A Systematic Analysis of Security, Efficiency, and Scalability. *International Journal of Advanced Computer Science & Applications*, *16*(1).

[6] Rahmati, M. (2025). Federated learning-driven cybersecurity framework for IoT networks with privacy- preserving and real-time threat detection capabilities. *arXiv preprint*.

[7] Nilima, S. I., Bhuyan, M. K., Kamruzzaman, M., Akter, J., Hasan, R., & Johora, F. T. (2024). Optimizing Resource Management for IoT Devices in Constrained Environments. *Journal of Computer and Communications*, *12*(8), 81-98.

[8] Altalebi, O., & Ibrahim, A. A. (2024, June). Automation of traditional networks: a mini-review. In *2024 International Conference on Circuit, Systems and Communication (ICCSC)* (pp. 1-8). IEEE.

[9] Baniya, P., Agrawal, A., Abid, K., Nath, J., Chaudhary, B. K., & Kunwar, B. (2024, February). The Internet of Things: Security Challenges and Opportunities. In *2024 3rd International conference on Power Electronics and IoT Applications in Renewable Energy and its Control (PARC)* (pp. 153-158). IEEE.

[10] Fernandez-Carames, T. M. (2024). From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the internet of things. *arXiv preprint*.

[11] Esmaeili, M., et al. (2024). Machine learning-assisted intrusion detection for enhancing internet of things security. *arXiv preprint*.

[12] Naz, I., et al. (2024). Lightweight encryption model for IoT security and privacy protection. *Advances, 5*(3), 84- 92.

[13] Singamaneni, K. K., et al. (2024). An efficient Q-KPABE framework to enhance cloud-based IoT security and privacy. *Wireless Personal Communications*.

[14] Mustafa, R., et al. (2024). A cross-layer secure and energy-efficient framework for the Internet of Things: A comprehensive survey. *Sensors, 24*(22), 7209.

[15] Muhammad, M., et al. (2024). A systematic literature review on the role of big data in IoT security. *Journal of Telecommunications and the Digital Economy, 12*(1), 39– 64.

[16] Kumar, C., & Chittora, P. (2024). Secure and privacy-preserving framework for IoT-enabled smart grid environment. *Arabian Journal for Science and Engineering, 49*, 3063–3078.

[17] Ajagbe, S. A., Mudali, P., & Adigun, M. O. (2024). Internet of things with deep learning techniques for pandemic detection: A comprehensive review of current trends and open issues. *Electronics*, *13*(13), 2630.

[18] Adil, M., Khan, M. K., Kumar, N., Attique, M., Farouk, A., Guizani, M., & Jin, Z. (2024). Healthcare internet of things: Security threats, challenges and future research directions. *IEEE Internet of Things Journal*.

[19] Idhalama, O. U., & Oredo, J. O. (2024). Exploring the next generation Internet of Things (IoT) requirements and applications: A comprehensive overview. *Information Development*, 02666669241267852.

[20] Abdulkareem, S. A., Foh, C. H., Shojafar, M., Carrez, F., & Moessner, K. (2024). Network Intrusion Detection: An IoT and Non IoT-Related Survey. *IEEE Access*.

[21] Al-Suhimat, R. I., Ibrahim, A., Maaitah, N. O., & Al- Dmour, N. A. (2024, February). Review of Security Challenges Encountered in Internet of Things Technology. In *2024 2nd International Conference on Cyber Resilience (ICCR)* (pp. 1-6). IEEE.

[22] Guero, A. M. M., Chiba, Z., & Abghour, N. (2023). Challenges and issues for Internet of Things (IoT): recent survey. *Math. Model. Comput*, *10*(3), 796-806.

[23] Park, J., & Lee, S. (2023) Cloud-Based IoT Networks: An Approach to Secure and EfficientNetwork Management. *Journal of Cloud Computing Research*, 15(2), 89-101.

[24] Haggag, A. (2023). Implementation and evaluation of IPv6 with compression and fragmentation for throughput improvement of internet of things networks over IEEE 802.15. 4. *Wireless Personal Communications*, *130*(2), 1449-1477.

[25] Alotaibi, B. (2023). A survey on industrial internet of things security: Requirements, attacks, AI-based solutions, and edge computing opportunities. *Sensors, 23*(17), 7470.

[26] Wójcicki, K., Biegańska, M., Paliwoda, B., & Górna, J. (2022). Internet of things in industry: Research profiling, application, challenges and opportunities—a review.

Energies, *15*(5), 1806.

[27] Siddiqui, S., Hameed, S., Shah, S. A., Ahmad, I., Aneiba, A., Draheim, D., & Dustdar, S. (2022). Toward software- defined networking-based IoT frameworks: A systematic literature review, taxonomy, open challenges and prospects. *IEEE Access*, *10*, 70850-70901.

[28] Haji, S. H., Zeebaree, S. R., Saeed, R. H., Ameen, S. Y., Shukur, H. M., Omar, N., ... & Yasin, H. M. (2021). Comparison of software defined networking with traditional networking. *Asian Journal of Research in Computer Science*, *9*(2), 1-18.

[29] Alshahrani, A., Fayaz, M., Alghamdi, A. M., & Gwak, J. (2021). A topical review on machine learning, software defined networking, internet of things applications: Research limitations and challenges. *Electronics*, *10*(8), 880.

[30] Alam, I., Sharif, K., et al. (2021) IoT Virtualization: A Survey of Software Definition & Function Virtualization Techniques for IoT. *arXiv preprint arXiv:1902.10910*.

[31] Imran, Ghaffar, Z.. (2021). A internet of things applications: Research limitations and challenges. *Electronics*, *10*(8), 880.

[32] Benomar, Z., Longo, F., Merlino, G., & Puliafito, A. (2021). Cloud-based network virtualization in iot with openstack. *ACM Transactions on Internet Technology (TOIT)*, *22*(1), 1-26.

[33] Dotan, M., Pignolet, Y. A., Schmid, S., Tochner, S., & Zohar, A. (2021). Survey on blockchain networking: Context, state-of-the-art, challenges. *ACM Computing Surveys (CSUR)*, *54*(5), 1-34.

[34] Patrono, L., Atzori, L., Šolić, P., Mongiello, M., & Almeida, A. (2020). Challenges to be addressed to realize Internet of Things solutions for smart environments. *Future generation computer systems*, *111*, 873-878.