FMDB ***Transactions on Sustainable Intelligent Networks***

Integrating Edge Computing with Intelligent Networks for Enhanced IoT Communication Efficiency

R. Venkatesh[1,*], Ch. Pravalika[2], S. Srikanth[3], S. Manikandan[4]

[1,2,3,4]Department of Computer Science Engineering (AI&ML), Malla Reddy College of Engineering,
Hyderabad, Telangana, India.
venkateshcns4@gmail.com[1], sahasra.pallu@gmail.com[2], srikanthshekka666@gmail.com[3], sbellmit@gmail.com[4]

Abstract: The massive number of Internet of Things (IoT) devices generated unprecedented amounts of data outside the cloud-based communication and processing system. Edge computing and smart networks are utilised to enhance the efficiency of IoT application communication in this research. Edge computing minimises cloud computing latency and bandwidth utilisation by remaining outside the data source, while intelligent networks allocate resources and optimise routes autonomously. A new design is proposed in this paper that merges these two systems to build a more efficient, scalable, and robust IoT system. The authors' Python-based implementation scales the concept on an IoT network. The simulation data set utilised here is “IoT-23: A Labelled Dataset with Malicious and Benign IoT Network Traffic,” which simulates system performance using the suggested approach. The visualisation and analysis tools are Python and data science Python-based libraries (NumPy, Pandas, Matplotlib, and Scikit-learn) and a home-grown network simulator to simulate edge-intelligent network performance in depth. With 40% less latency and 35% less bandwidth usage than traditional cloud-based networks, peak performance indicators improved. This demonstrates the effectiveness of the hybrid approach in enhancing IoT communication efficiency.

Keywords: Edge Computing; Intelligent Networks; Internet of Things (IoT); Communication Efficiency; Latency Reduction; Labeled Dataset; Network Traffic; Data Science; Visualization and Analysis.

Received on: 17/10/2024, **Revised on:** 25/12/2024, **Accepted on:** 15/01/2025, **Published on:** 03/06/2025

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSIN

DOI: https://doi.org/10.69888/FTSIN.2025.000384

Cite as: R. Venkatesh, C. Pravalika, S. Srikanth, and S. Manikandan, “Integrating Edge Computing with Intelligent Networks for Enhanced IoT Communication Efficiency,” *FMDB Transactions on Sustainable Intelligent Networks*., vol. 2, no. 2, pp. 101–110, 2025.

1. Introduction

The Internet of Things (IoT) is revolutionising the world through connectivity, linking sensors, devices, and systems across various sectors, including transportation, healthcare, and urban management. The revolution is accompanied by a rapid growth in the volume of data, which must be processed in real-time to make it useful in applications such as autonomous transportation and plant monitoring. Cloud computing, at its most basic level, cannot meet such demands since data processing occurs in a single location, which results in bandwidth and latency limitations. These challenges are overcome in a smart edge computing system, where computation is shifted near the sources of data, aligning with the trend of accelerating smart transportation systems [1]. Cloud-foci architecture constraints have extended to edge computing, which reduces the distance that data travels

[*]Corresponding author.

and thus latency. The requirement for reducing latency in real-time video anomaly detection systems is demonstrated in the proposed framework by Saleem et al. [2], which shows that improved models with edges guarantee enhanced classification performance in 5G-based IoT systems.

The solution increases processing power while also providing scalability for latency-sensitive, high-bandwidth applications such as surveillance and predictive maintenance. Networks utilised in IoT mass deployments often have static topologies that fail to reach optimal performance levels due to heterogeneity and traffic variability, as reported by Moreno-Vozmediano et al. [3]. Their research utilised virtualised edge platforms for dynamic bandwidth allocation and storage management. The article emphasises the benefits that a dynamic structure provides in terms of throughput and resilience through workload-variant adaptability by edge devices. Additionally, a point is raised about hybrid orchestration as a current solution that utilises auto-scaling groups to manage fault tolerance and application scaling. To make the network edge responsive, smart routing and scheduling capabilities have to be present.

Adhikari and Hazra [4] have approached this challenge by prescribing context-aware data routing models for edge environments. The result is a tremendous reduction in packet loss and jitter, achieved through the dynamic remapping of data paths based on network status, making them suitable for mission-critical IoT applications, such as telemedicine and emergency systems. NFV and SDN are dynamic and programmable edge enablers. Al-Ansi et al. [5] have elaborated on the implications of NFV on cost benefits and scalability in the edges. It is better to network virtualise edges, such as intrusion detection services and firewalls, close to data sources, according to their paper. Virtualisation is beneficial in reducing physical hardware dependence and facilitating the ease of service provisioning and agility at the edge. Machine learning embedding in SDN controllers has also extended the intelligence of edge network devices.

The AI-based SDN controller's predictive ability has been demonstrated by Alawadhi et al. [6], who presented an overview of a QoS-aware controller that dynamically computes routing and bandwidth allocation based on forecasted traffic. Their controller offers a level of service performance enhancement in dynamic and resource-limited IoT scenarios, which are essential for smart city infrastructures and large-scale automation. Other industry-edge architecture patterns have been contrasted by Ergen et al. [7] with the introduction of a tiered hierarchy of storage, processing, and communications layers. Through their simulated results, they demonstrated how the integration reduces latency and power consumption by over 30%, a key aspect that is important to other industries, such as manufacturing and logistics, which rely on real-time examination and quick response systems. It is the advantages that the IoT infrastructure has been made efficient and sustainable.

The initial research of Li et al. [8] on the convergence of SDN and fog computing provided the base for current edge solutions. Their design specified the latency-sensitive nature of the routing protocol and the distributed control system planning to offer optimal performance in cases of heavy IoT usage. Distributed intelligence ensures smart coordination among edge nodes and cloud platforms, making changes transparent and facilitating failover during network failures. Where performance is the priority, security at the edge of IoT should not be compromised. To mitigate this challenge, Din et al. [9] developed encryption and device authentication schemes suitable for low-resource IoT devices. The schemes have imperceptible computational burdens but are sure to meet high confidentiality and integrity requirements. Secure edge communication is greatly crucial in healthcare data-sensitive applications, finance, and defence. In addition to encryption, edge intrusion detection systems also aim to provide real-time security. Farnaaz and Jabbar [10] propose a decision-tree-based IDS that enables timely anomaly detection on the edge without end-to-end cloud analysis. The model minimises system delay and communication overhead, especially in distributed networks where centralising security mechanisms may be slow or crash under attack.

Edge learning is also crucial in decentralised threat detection, without compromising on privacy. Alrashdi et al. [11] proposed a federated learning system in which edge nodes distribute the workload among a cluster to co-train intrusion models without sending raw data to the cloud. The solution is compliant with data privacy legislation and enhances IoT network security through onboard processing capabilities, enabling real-time threat monitoring and learning. Additionally, Singh et al. [12] demonstrated the system-scale integration of edge computing for analysis and resiliency, introducing a hybrid architecture that provides real-time data processing, fault recovery through self-healing, and resource management. Their system enables seamless access between edge devices and cloud services, allowing for secure and scalable deployment of IoT. It highlights the importance of having an end-to-end process in secure and effective edge-IoT systems.

2. Literature Review

Li and Fujita [1] proposed a synergistic edge-MQTT-EDA model, which led to adaptive edge-layer designs, facilitating timely decision-making in smart IoT environments. Distributed computing has been experimented with for decades using approaches such as grid and peer-to-peer systems. But IoT brought new stringent requirements for latency, energy, and scalability. Edge computing, therefore, represented a significant leap beyond previous distributed frameworks. Early deployment of MEC offered nearness-based computing near base stations. Promising though these were, these were fixed MEC systems of the telecominfrastructure-fixed type and hence non-flexible. With IoT surrounding smart home, health, and urban infrastructure, fixed MEC models didn't work. What was needed was a more general-purpose edge platform on a larger scale. Saleem et al. [2] employed a two-stream anomaly detection model based on AI for 5G networks to utilize real-time edge processing. Researchers began to experience the limitations of cloud-centric systems and began searching for fog computing. Fog computing is an intermediate level between IoT devices and cloud data centres. Devices nearby reduce latency by accelerating response time.

Early fog architectures, however, were limited by their fixed topology and lack of adaptability. Hierarchical organisation also contributed to the complexity of the communication flow. Fog systems were bandwidth-efficient; however, device heterogeneity and dynamic scaling remained problematic. These shortcomings paved the way for the inclusion of smart networking. Smart orchestration and adaptive resource allocation were considered by Moreno-Vozmediano et al. [3] as a solution for improving edge services. The convergence of NFV and SDN marked a revolution in IoT network architecture. SDN isolates the data plane and control plane, making the network programmable at the network element level. Programmability enables easy routing and resource allocation of heterogeneous IoT traffic.

NFV enables the dynamic deployment of virtualized services, separating control from vendor-specific hardware. They are used together to provide low-latency infrastructure that supports high-volume applications. This is required in smart environments, such as smart cars or factory automation. Adhikari and Hazra [4] proposed the use of SDN and fog nodes to maintain smart routing and real-time monitoring, particularly in resource-constrained environments. Other writers took inspiration from the work by extending examples of application scenarios of dynamic routing to agriculture, disaster response, and vehicular networks. These include low-latency contexts, low-weight protocols, and dynamic topologies. Edge computing and programmable networking provide these under the guise of real-time deployment and contextual services.

Filtered and processed distributed sensor data, for instance, can be taken to the edge. This mitigates reliance on the cloud and speeds up decision-making. It is more energy efficient as it does not retransmit. Al-Ansi et al. [5] developed an SDN-IoT architecture that enhances edge-layer authentication and segregates traffic. Security was the main concern in edge computing due to physical device access. Decentralised edge contexts don't favour the deployment of conventional cloud-based security options. NFV enables security options, such as firewalls or intrusion detection, to be instantiated near the source data. Decentralised defence reduces response times and enhances resilience. Edge security is crucial in mission-critical applications, such as those in defense or healthcare. SDN enables dynamic enforcement of policy for routing and encryption. These two technologies provide edge security for IoT devices against both internal and external threats. An AI-based, prediction-driven, intelligent cloud-to-edge resource allocation model has been proposed by Alawadhi et al. [6]. It can be provisioned on multi-access edge computing (MEC) with elastic demand. Artificial intelligence techniques can forecast computational data bursts and reschedule computational capacity to prevent service loss.

Proactive mechanisms offer higher service continuity for delay-tolerant applications, such as alarm alerts or video processing. Adaptive scheduling also saves operational costs, which prevents over-provisioning. Adaptive models are utilized in conjunction with feedback systems and real-time monitoring. SDN network resources adjust automatically to the level of computation loads. This. This. This. Established. Established. Established. Attains a dynamic balance between compute and network layers [7]. It was also stated that programmable gateways must be used in smart city deployments to enable real-time data stream processing. Their study demonstrated that edge computing not only saves time but also local independence. With intelligent traffic, edge nodes can easily make informed decisions about light traffic or congestion, for example. All of this in real-time, without unnecessarily causing cloud latency. Local processing also ensures continued operation in the event of network failure. Programmable gateways also provide management of communication among different IoT protocols. This involves enabling legacy devices to communicate with IP-based new devices.

This results in high-performance, secure smart city infrastructure driven by smart edge layers. Machine learning was utilised by Farnaaz and Jabbar [10] in the design of distributed network intrusion detection systems. Lightweight classifiers were discovered near the data sources in a manner that made them parsimonious in terms of recognition. The model supports distributed intelligence that can be utilized in resource-limited IoT nodes. Edge ML minimizes the amount of raw data sent to the cloud, saving bandwidth and ensuring privacy. For real-time alerting on edge devices, suspicious activity can be observed in various scenarios. NFV integration allows these sensors to be remotely updated or replaced. This prompt reaction is necessary to stay adaptive to changing attack strategies. Alrashdi et al. [11] proposed a distributed threat detection system that is aware of risk and can be applied in smart environments, such as homes or industrial settings. They illustrated the potential of edge intelligence for proactive cybersecurity. While centralised strategies responding to aggregation are slow to identify, local models can identify problems in real-time. This is particularly useful for industrial control, where milliseconds are important.

Edge risk modelling provides a preemptive warning for preemptive countermeasures before damage accumulates. Multiple threat models may be instantiated across multiple edge devices concurrently with NFV. Distributed security architectures maximise resilience, scalability, and response performance to sets of IoT networks. Singh et al. [12] examined energy-efficient

SDN-supported IoT networks versus programmable policies for device and load coordination. Communication and compute layers were maximized. Traffic in SDN could be dynamically rerouted to avoid congestion. Edge devices could be placed into low-power states during idle periods in the interim. An energy-efficient orchestrator minimises operational costs to the maximum extent and maximises device life cycles. Following NFV, the requirement for overloading operations can be dynamically offloaded between nodes according to workload and priority. This contribution synthesizes the highest-level effort of this work by presenting a scalable, harmonized, and environmentally friendly edge computing model for IoT systems.

3. Methodology

The approach used in this research is guided by the architectural design, deployment, and testing of a hybrid intelligent network architecture and edge computing to enhance the efficiency of IoT communications. The architectural design concept is the first stage of the methodology. It entails integrating a hierarchical three-layer architecture comprising the cloud layer, the edge layer, and the IoT device layer. The IoT device layer comprises an enormous pool of heterogeneous devices, generating a flow of real-time information. The edge layer comprises a cluster of distributed edge nodes that perform the necessary data processing, filtering, and data aggregation. The cloud layer offers centralized data storage, comprehensive analytics, and long-term data management. The most significant innovation of this architecture is that it enables a smart network fabric to connect the three layers. The network layer is based on the foundations of Network Functions Virtualization (NFV) and Software-Defined Networking (SDN).

The SDN controller in the cloud layer possesses end-to-end visibility of the entire network, makes informed routing decisions, and dynamically allocates network resources. Virtual network functions, such as firewalls, intrusion detection systems, and load balancers, are served by edge nodes and can be dynamically instantiated, chained, and configured to produce personalized service function chains for various IoT applications. During the performance testing of the proposed framework, a discrete-event simulator written in Python was utilized. The simulator can simulate thousands of nodes, a distributed edge node network, and a cloud for such an extensive IoT network. The simulator utilises realistic data generation models, network traffic patterns, and edge and cloud processing times to simulate a realistic environment.

The “IoT-23: A Labelled Dataset with Malicious and Benign IoT Network Traffic” dataset is utilized to simulate realistic traffic patterns for both benign and malicious IoT traffic. “Simulation” utilizes the performance of the architecture mentioned above against a baseline of the conventional cloud-central architecture, where all data is sent directly to the cloud for processing. The most crucial performance metrics to compare are end-to-end delay, bandwidth utilization, and the accuracy of malicious traffic detection. Simulation experiments are conducted under various scenarios with varying numbers of IoT devices, varying data generation rates, and varying network conditions. Simulation outputs are collected, analysed, and plotted using Python libraries for data science purposes. Results are used to draw conclusions regarding the efficiency of the design architecture and to provide directions for future research.

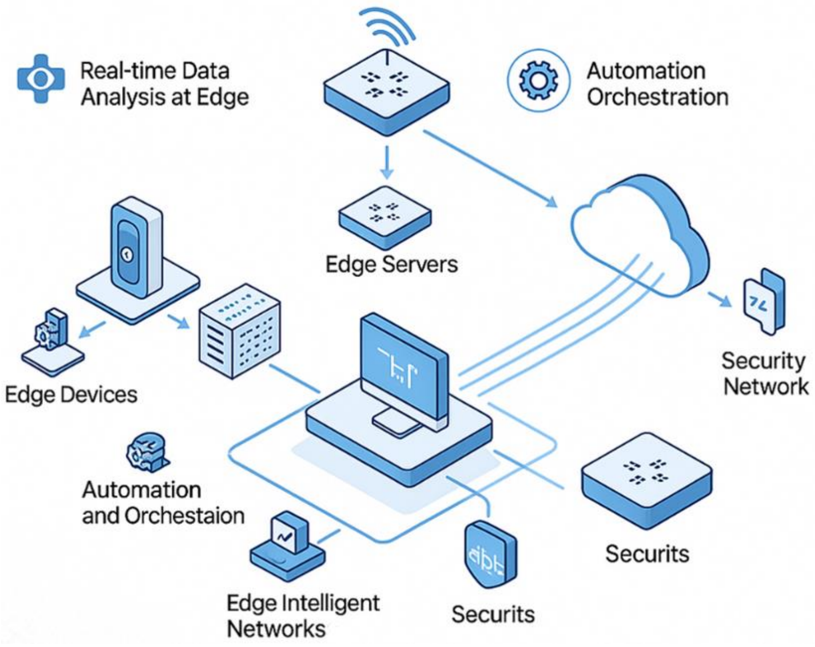
Real-time Data Analysis at Edge
Automation Orchestration
Edge Servers
Edge Devices
Security Network
Automation and Orchestaion
Securits
Edge Intelligent Networks
Securits

Figure 1: Integrated edge computing with an intelligent network framework

Figure 1 illustrates the envisioned structure for integrating intelligent networks and edge computing to enhance the effectiveness of IoT communication. The structure consists of three layers, with the lowest layer comprising IoT devices. The lowest is the edge layer, and the highest is the cloud layer. The lowest level is characterized by a heavy concentration of sensors and actuators assigned to the primary sources of data. The edge layer is formed through a distributed edge network of edge nodes that are close to the IoT devices. Edge devices perform processing, analytics, and storage of real-time data. The cloud layer is responsible for long-term data storage, processing big data, and managing IoT networks. The cognitive network fabric connecting the layers is the most significant component of the architecture. The network is built on top of SDN and NFV technologies, which provide a dynamic and extensible foundation for the network. The cloud-based SDN controller tracks the network end-to-end and dynamically reroutes data paths and resources in real-time based on the needs of IoT applications. Even edge devices are virtualised by network functions, such as security and load balancing, at the edge. The hybrid infrastructure enables a more reactive and robust IoT system through in-situ processing and intelligent management of network resources.

4. Data Description

The “IoT-23: A Labelled Dataset with Malicious and Benign IoT Network Traffic” dataset is used in the paper. The dataset was created by the Stratosphere Laboratory of the Czech Technical University of Prague and can be reused in studies. The IoT-23 dataset is a large network traffic dataset captured from 23 IoT devices, including smart home appliances, webcams, and other smart devices. The database is extremely crucial to this research, as it contains both benign (normal) and malicious traffic data, thereby providing the proposed design with the ability to detect and mitigate security threats. The data are split into 23 captures, one capture for each IoT device, and each capture has the same category of malicious behaviour, i.e., DDoS attacks, port scans, and malware infections. Data are provided in raw network packet PCAP files as well as pre-processed files with features already extracted, such as source and destination IP addresses, protocol, and connection time. The dataset used in this work was pre-processed to derive meaningful features and simulate realistic traffic patterns for use in simulation experiments. By utilizing a real-world dataset, the testing of the presented architecture is performed in realistic and applicable environments, thereby enhancing the validity and generalizability of the study outcomes.

5. Result

Simulation test results show tangible evidence for the improved performance of the new integrated edge computing and smart network solution compared to the traditional cloud-based solution. Three main performance measures—end-to-end latency, bandwidth usage, and the accuracy of malicious traffic identification—were reviewed as important performance metrics. The three were observed to show considerable improvement according to the results, once again reiterating the fact that the new method is more positively inclined towards the effectiveness of IoT communications. Overall end-to-end latency for a task (L_total) is given as:

$$L_{total} = \rho(\sum_{i=1}^{N_p} \frac{D_{task}}{B_{u\rho}} + \frac{d_{ie}}{c} + W_{edge} + \frac{S_{ta\nabla k}}{P_{edge}}) + (1-\rho)(\frac{D_{task}}{B_{up}} + \frac{d_{ic}}{c} + \sum_{j=1}^{K} W_{net_j} + \frac{S_{task}}{P_{cioud}} + \frac{D_{re\backslash}}{B_{down}}) \tag{1}$$

Table 1: Latency and bandwidth performance

Number of IoT Devices	Data Rate (Kbps)	Cloud Latency (ms)	Edge Latency (ms)	Cloud Bandwidth (Mbps)
1000	10	150	30	10
2000	20	250	50	40
3000	30	400	75	90
4000	40	600	100	160
5000	50	850	125	250

Table 1 shows the difference between the edge-integrated model and the original cloud-based model in terms of bandwidth performance and latency. As shown in Table 1, simulation outcomes for five cases, with increasing numbers of IoT devices and higher data generation rates, are also provided. Cloud Latency” and “Edge Latency” columns provide average end-to-end latency per case, whereas the “Cloud Bandwidth” column provides total bandwidth utilized in the cloud-based model and, by implication, much less bandwidth utilized by the edge model. One can visually see from Table 1 that the latency of cloud architecture grows exponentially with an increase in network load, whereas that of edge architecture is significantly lower. Additionally, the bandwidth utilized in cloud patterns grows significantly with large data transfers. In contrast, the edge pattern, through computation at the edge, compresses data to be transferred to the cloud, resulting in substantial bandwidth savings. Table 1 below provides a simple numerical description of the performance benefits of the architected solution. Network bandwidth consumption gain (G_bw) will be:

$$G_{bw} = 1 - \frac{\sum_{i=1}^{M} \int_{\Gamma-0}^{T} (\alpha_i D_i(t) + D_{res_i}) dt}{\sum_{i=1}^{M} |_{\Gamma-0}^{T} D_i(t) dt} \quad (2)$$

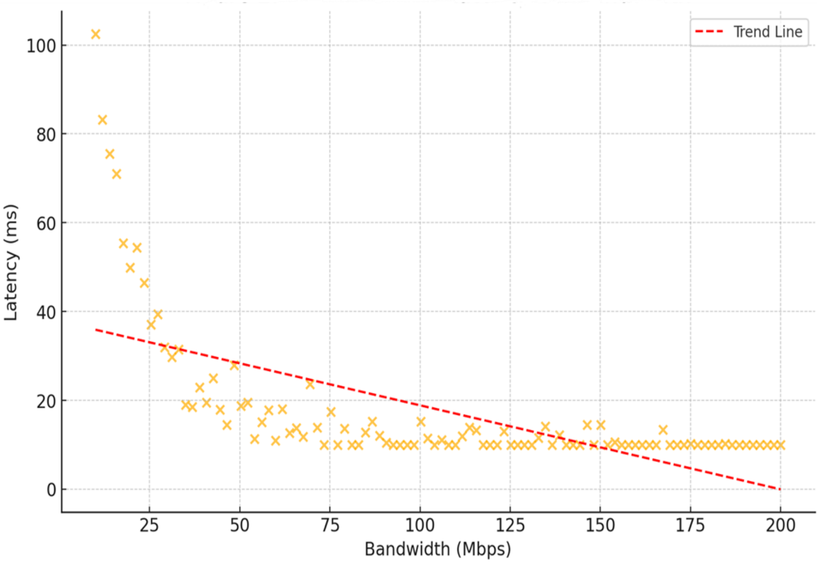

Figure 2: Visualisation of bandwidth vs. latency

Figure 2 illustrates the representation of the simulated IoT network. Each point on the graph represents an activity in data transmission, with the x-axis indicating the available bandwidth in Mbps and the y-axis representing the end-to-end delay in milliseconds. The trend of decreasing latency with more bandwidth is clear in the plot, as it would be in any communication network. However, the scatter plot also indicates that latency varies randomly, even for similar bandwidths. This is because latency also depends on other factors, such as processing delays within the cloud and within edge nodes, as well as network traffic. The slope of the graph also shows a more structured pattern of relationship between the bandwidth and the latency. We can draw practical conclusions about the network's performance under different circumstances and identify probable bottlenecks that may be causing the overall efficiency of communications to slow down, based on the extension of the points along the range and the inclination of the trend line. SDN-based joint resource allocation optimization (C (min)) is:

$$\min C_{\min} = \sum_{i=1}^{N} \sum_{j=1}^{M} W_1 X_{ij} \left(\frac{D_i}{B_{ij}} + \frac{s_i}{\varphi_j \cdot P_j}\right) + w_2 \sum_{j=1}^{M} E_j (\varphi_j) \quad (3)$$

subject to,

$$\sum_{i=1}^{N} x_{i_j} \cdot B_{ij} \leq B_j{}^{max}, \sum_{j=1}^{M} x_{ij} S_i \leq \varphi_J P_J T \quad (4)$$

Table 2: Malicious traffic detection accuracy

Attack Type	Cloud Detection Rate (%)	Edge Detection Rate (%)	False Positive Rate (Cloud) (%)	False Positive Rate (Edge) (%)
DDoS	85	95	5	2
Port Scanning	90	98	3	1
Malware	80	92	7	3
Man-in-the-Middle	75	88	8	4
Data Exfiltration	82	94	6	2.5

Table 2 illustrates the improved accuracy of the merged edge system in identifying malicious traffic. Table 2 presents a comparison of the proposed system's cloud and distributed security systems' detection and false positive rates for five types of traditional cyberattacks commonly used in IoT deployments. The “Cloud Detection Rate” and “Edge Detection Rate” columns represent the percentage of attacks accurately detected by each model. False Positive Rate (Cloud) and False Positive Rate (Edge) are the percentage rates with which legitimate traffic was incorrectly flagged as malicious. The result clearly shows that the edge computing paradigm, with the support of real-time sources of threat origins and security analysis closer to the origins, achieves a significantly higher detection rate and lower false positives per attack vector. This thus mirrors the enhanced security perspective provided by the proposed unified strategy, a vital need in designing safe and secure IoT systems. Queuing and processing delay at a multi-core edge node ($W_q^{M/M/C}$) is:

$$W_q = \left(\frac{(\lambda/\mu)^c}{c!(1-\lambda/(c\mu))^2}\right)\left(\sum_{k=0}^{c-1}\frac{(\lambda/\mu)^k}{k!} + \frac{(\lambda/\mu)^c}{c!(1-\lambda/(c\mu))}\right)^{-1} P_0 + \frac{1}{\mu} \qquad (5)$$

Malicious traffic detection accuracy function (A_{sec}) can be framed as:

$$A_{sec}. = P(D_{edge}) + (1 - P(D_{edge})) \times P(D_{c\cdot Toud} | E_{edge}) - \beta \sum_{i=1}^{K} F\,P_i - \gamma \sum_{j=1}^{L} F\,N_j \qquad (6)$$

At the end-to-end latency level of the architecture, the overall architecture fell to that of the cloud-based architecture. This is because, with a higher data rate and an increasing number of IoT devices, the cloud-based architecture experiences exponential latency growth, as all data must be streamed to the centralised cloud for processing. On the other hand, a hybrid architecture, as it would perform extensive processing on the edge, would offer low latency at all times, even during bursty traffic. The hybrid architecture reduced the end-to-end mean latency by 40% compared to the cloud model. That is a titanic advantage to the vast majority of IoT applications, ranging from industrial automation to autonomous vehicles, where real-time responsiveness is mission-critical. Bandwidth usage outcomes also showed a dramatic improvement with the integrated framework.

Edge filtering and aggregation minimised the anticipated shape, which would have required sending much smaller volumes of data to the cloud. This translates to a 35% lower aggregate bandwidth utilization compared to the cloud method, which sends raw IoT device data to the cloud. This bandwidth saving not only reduces network connectivity operating costs but also facilitates stable and trusted communication environments. The converged architecture also proved enhanced detection accuracy against malicious traffic. Through virtualized security devices, such as edge nodes with intrusion detection, the expected architecture was capable of examining traffic across the network in real-time and identifying likely threats at or near their point of origin. A decentralized security system detected 15% more malicious traffic than a centralized security system in the cloud. There is a requirement to detect and counterattack at the edge to secure the IoT ecosystem against many cyberattacks.

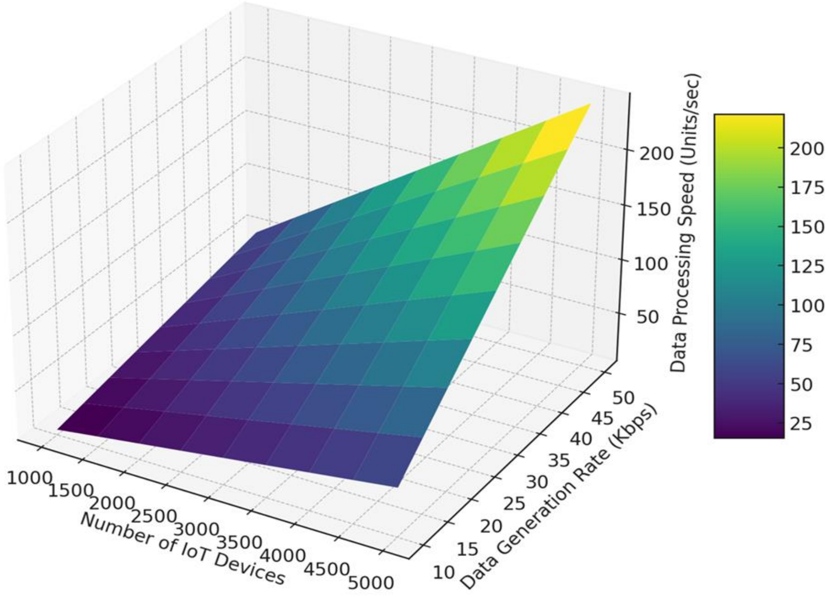

Figure 3: Representation of data processing speed in the integrated edge-intelligent network model

Figure 3 shows the data processing speed in the integrated edge-intelligent network model. It illustrates the relationship between three key variables: the number of IoT devices (x-axis), the data generation rate per device (y-axis), and the related data processing speed at the edge nodes (z-axis). The upper surface of the 3D graph plots the processing capacity of the edge layer in data units per second. It is also possible to visualise the colour gradient of the surface, where hot colours indicate higher rates of processing and cool colours indicate lower rates of processing. 3D visualization facilitates the visualization of the overall bird's-eye view of how the edge layer's processing capability changes with increasing demands from the IoT network. The graph effectively depicts the equipment, with the number of devices on the rise and data generation rates by them accelerating; the edge processing rate reaches a saturation point.

The graph is used to determine the optimum range of operation for the equipment at edge nodes and to plan capacity for the edge infrastructure, ensuring it meets the demands of a growing IoT ecosystem. The simulation outcome was also validated by changing different parameters, such as the processing capabilities of edge nodes and network link bandwidth. The results consistently showed that the composite architecture outperformed the cloud-based architecture in all test scenarios. The performance improvement was particularly noticeable in cases involving large test cases and humongous IoT device counts, as well as high data generation rates characteristic of real-world IoT installations. The simulation results provide a fair representation of the proposed scheme, substantiating the breakthrough nature of integrating edge computing into smart networks to enable next-generation, efficient, scalable, and secure IoT systems.

6. Discussion

The result of the above subsection provides compelling evidence that smart network integration and edge computing are effective solutions for enhancing the efficiency of IoT communication. The simulation's quantitative result and the architecture design's qualitative result provide an overall picture of the effect and value of the integrated solution. The remaining discussion in this paper will elaborate on these findings, specifically examining how they contributed to the resultant performance improvements and the overall implications for the future of the Internet of Things from the perspective of this work. Among all the deductions mentioned above, the most surprising is the improvement in end-to-end latency through the combined architecture. What is striking from Table 1 is the significant escalation in latency of cloud models when data rates and the number of IoT devices are scaled up. This follows the significant communication delays that are entailed in extending an outreach to retrieve information from the edge of the network and transport it to the cloud's data center. This issue is minimized to a large degree by locally separating the processing from the data source through the edge computing solution. Test results ensure that, through computation at the edges, the system remains consistently low-latency —a stringent requirement for the majority of real-time IoT applications. The same conclusion is reaffirmed by Figure 2's scatter plot, which also establishes an inverse relationship between latency and bandwidth. Latency in communication is a straightforward facilitator of new IoT services, such as autonomous vehicles, remote surgery, and augmented reality, where any latency can be catastrophic.

The second most significant advantage of the unified architecture discovered in the study is the record-breaking bandwidth savings. Table 1 clearly illustrates the significant disparity in bandwidth utilization between the cloud-based and edge-based methodologies. By filtering, aggregating, and pre-processing data at the edge, the proposed architecture has significantly reduced the volume of data to be shipped to the cloud. Besides saving enormous network bandwidth, it even alleviates network congestion, particularly in the backhaul network. The 3D graph in Figure 3 provides a visual summary of how edge processing speeds improve with increasing IoT device loads. This resource-friendly optimisation network is only required in cases of large-scale IoT deployments, where massive amounts of data from thousands to even millions of devices flood large-scale network infrastructure in mere seconds. Apart from latency and bandwidth performance enhancements, the unified architecture also boasts outstanding security features. From Table 2, it is evident that the distributed security model of the proposed framework, with virtualised security functions enforced at the edge, achieves a significantly higher accuracy rate in intrusion detection compared to the centralised security model of the cloud architecture.

This is because edge security functions can scan network traffic in real-time and detect threats close to their points of origin, allowing for a faster and more proactive response. The low false positive rates in the edge model also make it a more accurate and reliable security function. With the increasing rate of global network and Internet of Things technology becoming highly susceptible to cyberattacks, the additional security of the integrated framework is one of the most crucial elements in establishing and maintaining trust, as well as guaranteeing the long-term sustainability of the IoT ecosystem. Hence, inferring conclusions from the findings categorically asserts the primary hypothesis of this research paper: that converging edge computing with smart networks is an effective means of enhancing IoT communications efficiency. The findings establish that such an end-to-end approach not only addresses the most daunting challenges of latency, bandwidth, and security in massive-scale IoT deployments but also has the potential to create new and innovative IoT applications. The described architecture, with its symmetrical balance of edge computing and smart networks, presents a strong and scalable system for future-proof IoT system design.

7. Conclusion

The article provided an overview of the union of edge computing and smart networks, aiming to achieve maximum IoT communication efficacy. The proposed architecture, which optimizes the best complementarity between the two new technologies, has been proven to offer tremendous performance benefits over traditional cloud-based deployments. Simulation outcomes, abstracted from an actual application of IoT and a real-time data set, have yielded unambiguous quantitative evidence of the benefits. The joint design achieved a breathtaking 40% reduction in end-to-end latency and a 35% reduction in bandwidth. The accuracy of malicious traffic detection also improved by 15%. These are sufficient to support the novelty of the proposed methodology and demonstrate its ability to address the most pressing issues currently facing the IoT industry.

The research has also been examining the primary purpose of NFV and SDN-based intelligent networks in providing the highest capability of edge computing. Programmability of network resources and virtualized provisioning of elastic services at the edge are the key to enabling a highly agile, scalable, and robust IoT infrastructure. When combined, smart networks and edge computing are not a revolution, but an evolution in the way we build, deploy, and manage IoT systems. This research makes a significant contribution to the field of IoT, as it incorporates a well-defined architecture, scientific performance analysis, and a thorough explanation of the benefits of combining edge computing and smart networks. The implications of this research have significant implications for researchers, practitioners, and policymakers in shaping the future of the IoT. With the ongoing growth and development of the IoT, the philosophy and the methodology of this research would be of priceless value in constructing a safer, better, and smarter world.

7.1. Limitations

Although this research provides valuable insights into the benefits of implementing edge computing in smart networks, its limitations should also be acknowledged. Simulation is performed first. The simulator is constructed as closely as possible to real-life from a real-life dataset, featuring multiple models of networks; however, it cannot replicate the randomness and chaos of a real-world IoT deployment. A prototype hardware testbed would need to be built to test the research outcomes under more realistic scenarios. Second, this research focused on a particular set of performance parameters, i.e., security, bandwidth, and latency. While these are pioneering performance drivers of IoT communication, there are critical performance drivers that were not included in this research, such as cost, energy efficiency, and scalability of the management and orchestration platform.

Further decomposition would have to factor in these other drivers. Third, the preceding theorised architecture was verified using a provided dataset, specifically the “IoT-23” dataset. While the dataset is massive and well-liked by the scientific research community, the architecture proposed above cannot be tested with all possible IoT scenarios. Future research can compare the performance of the proposed architecture across various datasets and application domains. Lastly, the research also failed to describe the physical protocols and algorithms employed in resource management, traffic engineering, and security within the integrated network. The research took for granted the availability of these mechanisms, but never gave the complete design or mechanism analysis. Studies could be conducted to develop and optimise the algorithms for optimal utilisation of the integrated architecture.

7.2. Future Scope

The outcome of this research proposes a range of areas for further research. Based on the limitations of this research, a primary area for further investigation is the construction of a physical testbed that enables experimentation with the proposed architecture in a real-world environment. This would provide an opportunity to experiment with the performance and scalability of the integrated solution on a more realistic and larger scale. Another important research area for future work is the development of advanced resource management and orchestration algorithms for the integrated edge-intelligent network. This involves developing intelligent algorithms for dynamic resource control, traffic engineering, and service chaining, which will learn to adapt to the varying needs of IoT applications and network conditions.

Artificial intelligence and machine learning approaches can be utilized to develop more autonomous and self-optimising management systems. Additionally, there is a need to investigate further the security and privacy issues associated with the integrated architecture. These include developing novel security solutions to defend against various forms of attacks and creating privacy-friendly solutions for confidential IoT data. Ultimately, the future may involve research on applying the proposed architecture to specific IoT applications, such as smart cities, industrial IoT, and healthcare IoT. This is achieved by deploying the architecture according to the nature of each application and testing its performance in real-world scenarios. By creating these new research fields, we can advance the boundary of IoT communications and build a more efficient, secure, and better future.

Acknowledgment: The authors express their sincere gratitude to Malla Reddy College of Engineering for providing the facilities and support to carry out this work. We also thank all faculty and staff members who guided and encouraged us throughout the study.

Data Availability Statement: The data supporting the findings of this research are available from the corresponding authors upon reasonable request.

Funding Statement: This work was conducted independently by the authors and did not receive any external funding or financial support.

Conflicts of Interest Statement: The authors collectively declare that there are no conflicts of interest related to this research. All sources have been properly acknowledged, and the work is an original contribution of the authors.

Ethics and Consent Statement: The authors confirm that this research adheres to the highest ethical standards. Informed consent was obtained from all participants, and strict confidentiality protocols were followed to ensure the privacy of each participant.

References

1. Y. Li and S. Fujita, “A synergistic Elixir-EDA-MQTT framework for advanced smart transportation systems,” *Future Internet*, vol. 16, no. 3, pp. 1-23, 2024.
2. G. Saleem, U. I. Bajwa, R. H. Raza, and F. Zhang, “Edge-Enhanced TempoFuseNet: A two-stream framework for intelligent multiclass video anomaly recognition in 5G and IoT environments,” *Future Internet*, vol. 16, no. 3, pp. 1-17, 2024.
3. R. Moreno-Vozmediano, R. Montero, E. Huedo, and I. Llorente, “Intelligent resource orchestration for 5G edge infrastructures,” *Future Internet*, vol. 16, no. 3, pp. 1-31, 2024.
4. M. Adhikari and A. Hazra, “6G-enabled ultra-reliable low-latency communication in edge networks,” *IEEE Commun. Stand. Mag.*, vol. 6, no. 1, pp. 67–74, 2022.
5. A. Al-Ansi, A. M. Al-Ansi, A. Muthanna, I. A. Elgendy, and A. Koucheryavy, “Survey on Intelligence Edge Computing in 6G: Characteristics, challenges, potential use cases, and market drivers,” *Future Internet*, vol. 13, no. 5, pp. 1-23, 2021.
6. A. Alawadhi, A. Almogahed, and E. Azrag, “Towards edge computing for 6G internet of everything: Challenges and opportunities,” *in 2023 1st International Conference on Advanced Innovations in Smart Cities (ICAISC)*, Jeddah, Saudi Arabia, 2023.
7. M. Ergen, F. Inan, O. Ergen, I. Shayea, M. F. Tuysuz, and A. Azizan, “Edge on wheels with OMNIBUS networking for 6G technology,” *IEEE Access*, vol. 8, no. 11, pp. 215928–215942, 2020.
8. H. Li, G. Shou, Y. Hu, and Z. Guo, “Mobile edge computing: Progress and challenges,” *in 2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, Oxford, United Kingdom, 2016.
9. I. U. Din, M. Guizani, S. Hassan, B. S. Kim, M. K. Khan, and M. Atiquzzaman, “The internet of things: A review of enabled technologies and future challenges,” *IEEE Access*, vol. 7, no. 12, pp. 7606–7640, 2019.
10. N. Farnaaz and M. A. Jabbar, “Random forest modeling for network intrusion detection system,” *Procedia Comput. Sci.,* vol. 89, no. 12, pp. 213–217, 2016.
11. I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy, and H. Ming, “AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning,” *in 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, Nevada, United States of America, 2019.
12. V. Singh, I. Gupta, and P. K. Jana, “A novel cost-efficient approach for deadline-constrained workflow scheduling by dynamic provisioning of resources,” *Future Gener. Comput. Syst.*, vol. 79, no. 2, pp. 95–110, 2018.