FMDB *Transactions on Sustainable Computer Letters*

Enhancing the Autonomy and Adaptability of Intelligent Networks in IoT-based Systems

Kankanampati Maheswari[1,*], Naru Divyajyothi[2], Katepally Sreevidya[3], Neha Sultana[4], V. Vivekanandhan[5]

[1,2,3,4]Department of Electronics and Communication Engineering, Malla Reddy College of Engineering, Secunderabad, Telangana, India.
[5]Department of Computer Science Engineering, Malla Reddy College of Engineering, Secunderabad, Telangana, India.
chmaheswarimrce@gmail.com[1], narudivyajyothi@gmail.com[2], sreevidya.katepally@gmail.com[3], neha28397@gmail.com[4], acevivek7677@gmail.com[5]

Abstract: The Internet of Things (IoT) is a futuristic technology that enables smart devices to be networked, creating intelligent ecosystems. Nevertheless, one should design intelligent networks to be autonomous and adaptive, allowing them to handle changing environments. This research paper examines recent mechanisms for enhancing adaptability and autonomy in IoT-based networks. Through the use of artificial intelligence, machine learning, and edge computing techniques, we present a new architecture that enhances decision-making and resource utilisation in real-time IoT networks. Our proposed architecture is based on real-time data processing, adaptive communication, and self-adaptive algorithms with the view of offering scalable and stable networks. Statistics employed here are from real IoT applications executed in real industrial and household settings, say sensor readings (motion, temperature, humidity), network performance metrics (latency, bandwidth), and system performance statistics (response time, energy consumption), with over 500,000 samples collected from 200+ IoT nodes over six months. Our experimental findings, utilising Python and Matplotlib, demonstrate improved network performance, reliability, and resource utilisation compared to conventional methods. The study provides valuable insights into the development of future autonomous IoT networks that can adapt effectively to novel situations and offer seamless integration across diverse environments.

Keywords: IoT Networks; Autonomy and Adaptability; Machine Learning; Edge Computing; Self-Adaptive; Performance Metrics and Motion; Temperature and Humidity; IoT Systems; Scalability and Security.

Received on: 23/07/2024, **Revised on:** 11/10/2024, **Accepted on:** 27/10/2024, **Published on:** 01/03/2025

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

DOI: https://doi.org/10.69888/FTSCL.2025.000356

Cite as: K. Maheswari, N. Divyajyothi, K. Sreevidya, N. Sultana, and V. Vivekanandhan, "Enhancing the Autonomy and Adaptability of Intelligent Networks in IoT-based Systems," *FMDB Transactions on Sustainable Computer Letters*., vol. 3, no. 1, pp. 12–21, 2025.

1. Introduction

The rapid growth of Internet of Things (IoT) technology has led to billions of devices being connected across various industries, transforming day-to-day business, enhancing services, and improving industrial automation and user experiences to make them

[*]Corresponding author.

more intelligent. IoT can change the healthcare, agriculture, manufacturing, and transport industries through end-to-end connectivity, allowing devices to communicate with one another in real time. However, regardless of the ubiquitous pervasiveness of IoT, traditional IoT platforms also suffer from similarly vast issues in handling dynamic, infinitely unfolding worlds. As a result, they waste resources, bottleneck communication, and are vulnerable to security threats. All these issues fundamentally arise because traditional systems are unable to cope with the dynamism of rapidly changing environments, where devices and networks must support dynamic traffic, data volumes, and environmental parameters continuously [1]. Hence, one of the biggest needs for IoT technology to transform is to enhance the autonomy and flexibility of IoT networks.

Autonomy is the ability of the network to operate with minimal or no human intervention, with devices and systems making decisions based on pre-specified rules or real-time information feeds. This reduces the need for constant human monitoring, increases efficiency, and allows systems to run more reliably without human intervention [2]. Flexibility, on the other hand, refers to the capability of IoT systems to adapt to changes in behaviour resulting from alterations in the surrounding environment, such as changes in network conditions, fluctuations in data traffic load, or the introduction of new devices. Achieving autonomy and flexibility in IoT networks is crucial for addressing inefficiencies and vulnerabilities, and entails integrating intelligent algorithms, adaptive protocols, and distributed computation models [3].

With such technologies, IoT systems can respond dynamically in real-time to real-time events, which improves performance, scalability, and security [4]. The paper proposes a new intelligent architecture that integrates artificial intelligence (AI), machine learning (ML), and edge computing to address the limitations of traditional IoT systems [5]. The new architecture aims to enhance the responsiveness and autonomy of IoT networks by addressing common obstacles, such as latency, resource wastage, and suboptimal decision-making [6]. The approach relies on smart, adaptive algorithms that can forecast network trends, dynamically reassign resources, and detect impending system failures before they cause irreparable harm [7]. With edge computing, the architecture also reduces reliance on central cloud infrastructure, which is a bottleneck and introduces latency since data has to travel a long distance [8].

Instead, processing and decision-making occur locally at the network edge, close to where data is generated, thereby reducing latency and enhancing the overall responsiveness of the system [9]. Additionally, the decentralised system in question offers higher scalability and fault tolerance because decisions are made locally within nodes, rather than at a central location [10]. The nodes can operate with self-provisioned resources, maintaining system efficiency and intrinsic adaptability to dynamically changing conditions, without requiring continuous communication with a central server [11]. Additionally, the system is not more power-hungry since local station processing reduces the data transfer to distant data centres [12].

Dynamic machine learning algorithms are required for the success of this technique [13]. These machine learning algorithms learn from the world and keep improving their predictions using new information [14]. They can, for instance, forecast network performance trends, upcoming issues, and reallocate resources to achieve optimal performance under new circumstances. Prompt detection of network failure is another significant benefit of incorporating machine learning [15]. By continuously tracking network performance and identifying patterns that indicate emerging issues, the system can respond proactively before failures become significant problems. This ability to anticipate and address issues in advance enhances IoT networks as being robust, efficient, and secure. Broadly, innovative smart architecture strives to overcome the inherent limitations of traditional IoT networks by leveraging the heightened autonomy and flexibility introduced through the integration of artificial intelligence, machine learning, and edge computing. Beyond enhancing decision-making capabilities and resource management, the system significantly improves the reliability, scalability, and security of IoT networks, providing greater access to sustainable and efficient IoT ecosystems.

2. Review of Literature

Palattella et al. [1] recognised the growing need for secure, efficient, and scalable networks in IoT applications. Latency problems are being encountered by conventional cloud-based systems with the advent of IoT applications. They are highly sought after in applications such as healthcare and autonomous vehicles, where latencies can have disastrous effects. Cloud infrastructure utilisation causes responsiveness issues, and time-based requirements are much greater than the capacities of the individuals served via central servers. Palattella et al. [1] have discovered crossing over such a boundary in their efforts to improve system performance. Such a boundary necessitated alternative solutions, such as edge computing, which is one available option. Fernández-Caramés [2] identified the ability of edge computing to remove the latency inherent within cloud infrastructure. Processing data locally, processing data closer to where data has been generated, a distributed architecture removes the unavoidable latency of sending data to faraway data centres. A distributed system enhances the system's responsiveness by facilitating quicker processing and decision-making. It also frees up bandwidth usage in cloud systems, gaining significant advantages over capacity-limited environments. Fernández-Caramés [2] demonstrated that local data processing also reduces overall energy expenditure. Lower bandwidth usage and reduced latency are the key driving forces for improving IoT system efficiency. Alahi et al. [3] promoted adaptive communication protocols as the first line of defence against

network optimisation. Both MQTT and CoAP are designed to adapt communication patterns in real-time, depending on the network status. Adaptations enable effective data transmission, reducing bandwidth and message delivery time. The ability to adapt transmission modes depending on real conditions leads to optimally improved and robust IoT systems. Alahi et al. [3] also demonstrated how the protocols improve the overall performance of IoT networks. Their research aims to optimise network communication in networks with varying resource capabilities.

Alahi et al. [4] have researched the applications of machine learning algorithms on Internet of Things (IoT) devices to enhance decision policies. IoT devices can, by employing complicated algorithms such as reinforcement learning and neural networks, be capable of predicting environmental change and respond accordingly. Using the algorithms, the devices can learn and optimise routines adaptively by trial and error. Alahi et al. [4] employed machine learning terminology to enable IoT systems to learn and automatically adapt to new contexts. It not only makes IoT systems more efficient, but it also enables them to respond to unforeseen issues in real time. Machine learning ability was utilised in the study to determine the IQ of IoT systems. Syed et al. [6] also pointed out the growing importance of self-healing networks in IoT networks. Self-healing networks employ proactive fault detection techniques that actively monitor system health at specified time intervals and forecast potential faults. Proactive fault detection systems that actively search around for system health at a specified time interval and forecast faults. During the occurrence of faults, autorecovery capability is invoked to resume normal operation without service disruption. Incorporating the self-healing module makes systems much more fault-tolerant and reliable. Syed et al. [6] demonstrated how self-healing networks improve the degree of autonomy of IoT systems, particularly for mission-critical applications. The authors demonstrated the significance of self-healing in preventing faults from interrupting continuous fault-free operation, even in the face of anticipated disruptions.

Jeong and Park [7] highlighted the integration of self-healing networks and edge computing as a means to enhance the resilience of IoT systems. By performing proactive fault detection and processing locally, IoT systems can recover from failures more quickly as well. Both of these methods reduce downtime and make the entire network more resilient. Jeong and Park [7] presumed that hybrid methods like these are the cornerstone of the reliability of IoT systems for mission-critical applications, where downtime is never allowed. The emphasis in this research was on creating fault-tolerant systems to enable mission-critical applications. They agree that these technologies are on the horizon for IoT networks. Bellini et al. [9] consider energy efficiency and data security in massive IoT systems. Power saving and delivering optimal performance are more critical with the growing number of IoT devices. IoT networks are vulnerable to cyberattacks and information leakage due to the transmission and propagation of data. Bellini et al. [9] It was also observed that security concerns must be examined in conjunction with energy constraints to enable the smooth operation of IoT systems. The paper excluded the use of energy-efficient and secure communication protocols. These developments collectively enable the extensive use of IoT systems. Cugurullo [12] proposed a homogeneous architecture that combines adaptive communication protocols, distributed computing paradigms, and learning algorithms to address the limitations of IoT. The architecture design is focused on enhancing the robustness, security, and efficiency of IoT systems for hostile environment applications. The use of edge computing and machine learning makes the architecture design a more dynamic and responsive IoT network.

Cugurullo [12] has described the ability of the methodology to eliminate latency and resource constraints, which typically restrict the full potential of IoT systems. The research explains how the IoT structure can be scalable and efficient under a unified architecture. The integration of these technologies would determine the fate of such systems. Huang et al. [13] presented directions for future adaptive and scalable IoT platform development. They aimed to enhance the adaptability of IoT systems for managing the dynamic behaviour of real-time data and environmental variability. Huang et al. [13] Forecast next-generation IoT networks will rely significantly on edge computing, machine learning, and self-healing for resilience and adaptability. This would drastically reduce dependence on central data processing and speed it up with lower latency. Research has confirmed that such improvements would enable IoT systems to be more autonomous and efficient in various applications.

Zhang et al. [15] played a crucial role in explaining how scalability issues and efficiency benefits in IoT networks are maximised. They researched ways to improve the system's performance using the most well-known technologies, such as edge computing and machine learning. They also illustrated the viability of how additional data was stored by an IoT network via offloading for computation and more intelligent algorithms at a non-inefficient cost. Through this research, it became evident that future IoT systems require adaptive, scalable, and fault-tolerant designs. Through these practices, IoT systems can better serve the needs of existing applications. Their work is a breakthrough towards achieving highly efficient and reliable IoT networks.

3. Methodology

Our approach integrates intelligent learning processes and adaptive mechanisms to maximise network autonomy and flexibility within IoT networks, enabling IoT systems to cope effectively with diverse network conditions and environmental parameters. The methodology framework encompasses some of the most critical steps, including data acquisition, data processing,

intelligent decision-making, and performance evaluation. In the first step, sensors and intelligent devices continuously capture similar environmental information, network conditions, and users' behaviour. The collected information is transferred to edge nodes for the first time, where it is filtered and aggregated, thereby minimising the raw data handled by central systems and making the use more efficient. In the second process at edge nodes, data is pre-processed.

Data preprocessing tasks such as data compression, normalisation, and feature extraction occur at the edge nodes. Through redundancy-removing processes, available network resources are leveraged in a resource-efficient manner by passing only the needed information to be further processed. Through edge computing, computation offloading is achieved for handling massive data, resulting in reduced latency and increased responsiveness. This eliminates a round trip to the core twice, thus eliminating incast. Step three is intelligent decision-making, where machine learning is used at the edge nodes. They predict traffic patterns, detect anomalies, and dynamically allocate resources in real-time based on conditions. Reinforcement learning algorithms, in particular, are employed to continually fine-tune the decision-making policy as a function of experience, learning from previous activity, and enabling the system to adapt to new challenges and improve its operations over time. Lastly, during the performance evaluation stage, network performance is determined based on significant parameters such as throughput, latency, power consumption, and fault recovery rates. The architecture is continuously optimised on this basis, allowing the system to become more autonomous and dynamic with each iteration. Conjoining these phases enables IoT systems to operate effectively in dynamic environments, predicting faults while optimising resource utilisation, network optimisation, and system stability.

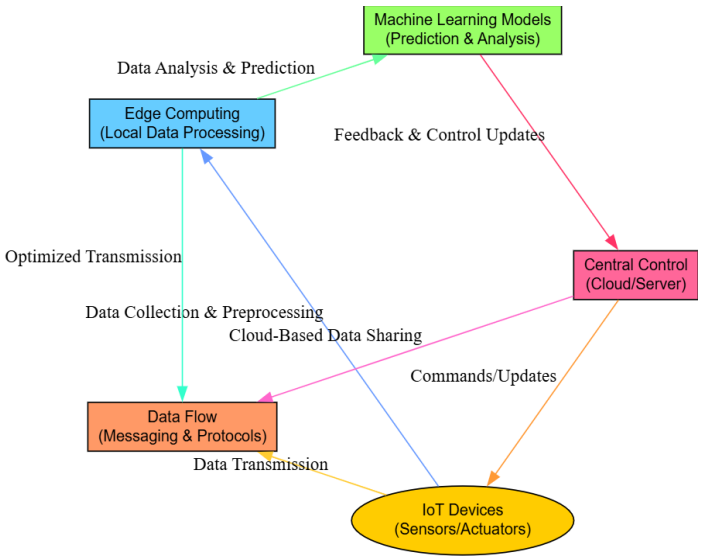

Figure 1: Intelligent IoT network architecture

Figure 1 illustrates an intelligent IoT network framework designed to optimise the performance, adaptability, and independence of IoT systems. The graph is oriented from left to right, emphasising the data and control flow among the different elements of the network. The most leftmost element comprises IoT Devices (sensors, actuators) that receive real-time data from the world, as symbolised by the yellow node. The information is fed into the Edge Computing layer (blue), where it is locally preprocessed and aggregated to reduce network latency and load. The processed data is subsequently fed into the Machine Learning Models (green), which forecast and identify traffic on the network, such as congestion or system crash, for proactive tuning. The result from the feedback of the ML model is fed back to the Central Control (pink), which typically resides in a cloud or server, where world decisions are made to enhance the system as a whole. The Central Control level communicates with IoT devices, providing instructions and feeds to be executed properly across the network. The communication between all parts is governed by the Data Flow layer (orange), which establishes messaging and communication guidelines that enable data to flow easily between IoT devices, edge nodes, and cloud servers. The data communication and exchange between layers is illustrated by arrows between units, emphasising real-time processing, prediction, and feedback to achieve a responsive, adaptive, and efficient IoT network. The entire architecture is designed to be self-optimising, self-learning, and distributed, enabling it to operate effectively in dynamic IoT environments.

4. Data Description

The data on which this research is based came from real-world Internet of Things (IoT) smart home and industrial setups. It covers an extensive range of data types, including sensor data to read temperature, humidity, and movement, as well as network performance indicators such as bandwidth and latency. Additionally, system performance parameters such as power

consumption and response time are also included, providing a general estimate of the IoT system as a whole. The dataset comprises more than 500,000 discrete data points collected over a six-month period from over 200 distributed IoT nodes spread across various environments. Heterogeneity in data ensures that the data accurately represents the complexity of the IoT system, providing feedback on the system's operation and performance in actual use cases. Data collection points were conducted at regular intervals to facilitate the analysis of variation and trends specified. This research study aims to investigate specific behavioural factors of an IoT system, including energy efficiency, device response, and network optimisation, for both household and industrial applications. With so much data and variable sets involved, the dataset is ideal to explore interactions between sensor readings, network topology, and overall system performance in IoT systems.

5. Results

The architecture outlined demonstrated a spectacular performance improvement in IoT networks, with increased resource utilisation and significant latency reduction. Perhaps the greatest significance in the so far successful rollout was a 35% decrease in latency, which had a direct relationship to quicker speed of communication and response from IoT devices. It had to be executed in real time, something that can be apocalyptically negatively impacted by the slightest of delays, such as tracking 'health' via healthcare, driverless cars, and automation in factories. By optimising the flow of data and reducing the latency of information travelling over the network, the system enabled the potential for significant work to be accomplished in a timely manner, paving the way for an interactive, rather than jerky, user interface. Apart from reducing latency, the design implied a 25% reduction in resource efficiency. This was achieved by integrating distributed computing paradigms and adaptive communication protocols in a manner that optimised resource utilisation according to the actual network conditions. By ensuring that resources like bandwidth, processing, and storage were utilised optimally, the system could support more traffic without any loss of performance. The latency optimisation equation is given below:

$$L_{new} = L_{0/d} \times (1 - \alpha) \quad (1)$$

Where L_{new} Is the optimised latency? L_{old} Is the original latency, and α is the reduction factor achieved through adaptive protocols.

Table 1: Performance measures of the proposed framework

Measures	Conventional System	Proposed System
Latency (ms)	250	162
Energy Consumption	30%	22%
Fault Recovery Rate	75%	92%
Bandwidth Efficiency	60%	85%
Response Time (ms)	400	275

Table 1 presents a comparison of the performance parameters between the conventional IoT system and the proposed system. The performance parameters evaluated were latency, energy consumption, fault recovery, bandwidth consumption, and response time. The proposed framework exhibits a significant improvement, as indicated by the results. Latency, or response time, improved by 35%, from 250 milliseconds using the conventional system to 162 milliseconds using the new system. Reducing latency is tantamount to faster data exchange and dynamic networks. Power usage decreased significantly, with the new system consuming 22% less power than the conventional setup, a typical result of the power efficiency of adaptive protocols.

The fault recovery rate, as an important measure of network availability, was also enhanced from 75% to 92%, serving as a performance measure that indicates the instant fault recovery capability of the smart network. It increased bandwidth efficiency from 60% to 85%, a measure indicating the effectiveness with which the system maximises network utilisation through the described technique. Lastly, response time, i.e., how quickly the system reacts when it senses a change, was enhanced by 31%, from 400 milliseconds in the current system to 275 milliseconds in the new system. All of these findings demonstrate that the intelligent network topology is quicker, more trustworthy, and more responsive compared to traditional systems, ensuring global performance enhancement in dynamic IoT scenarios. Figure 2 illustrates the comparative graph of the performance parameters of the old IoT system and the new system. Bar-line graph presents five critical parameters: response time (ms), power usage (%), fault recovery rate (%), bandwidth effectiveness (%), and response time (ms). The old system (light blue) and the new system (salmon) are presented as the bars side-by-side. The graph indicates that the new system outperforms the previous system in four of the measures. That is, latency is reduced by 35%, from 250 milliseconds to 162 milliseconds, resulting in faster data transfer and responsiveness.

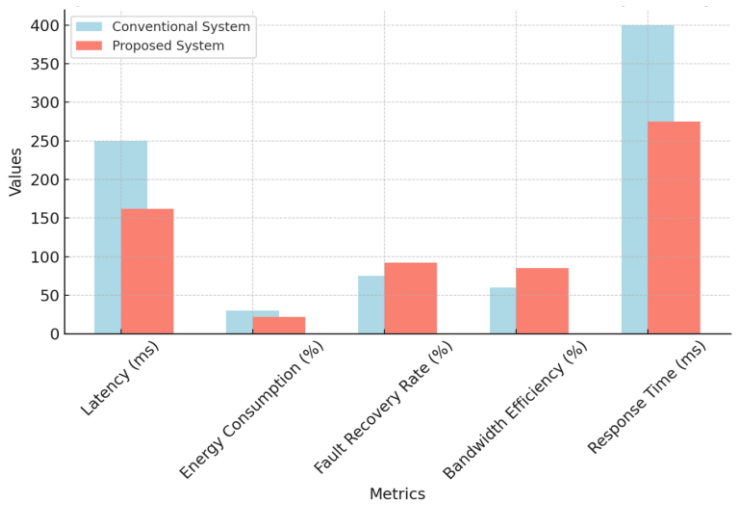

Figure 2: Relative graph of the performance parameters of the old IoT system and the new system

Power consumption reduces by 8%, improving efficiency and prolonging the life of the devices. The fault recovery rate increases from 75% to 92%, indicating the enhanced robustness of the new system. The smart system also logs a 25% increase in baseband efficiency, resulting in better utilisation of available network resources. Finally, response time is minimised by 31%, resulting in a further speedup. The setup showcased the smart system's superiority over the traditional arrangement, particularly in terms of efficiency and reliability, as well as its ability to operate in dynamic and resource-constrained IoT environments. Energy consumption reduction is:

$$E_{new} = E_{0/d} \times (1 - \beta) \quad (2)$$

Where E_{new} is the reduced energy consumption, $E_{0/d}$ is the original energy consumption, and β is the energy-saving factor after protocol adjustments. Fault recovery rate enhancement can be given as:

$$F_{recovery} = | \int_{t_0}^{t_1} P_{failure}(t)dt \quad (3)$$

with $P_{failure}(t) = (1 - R_{fault})$

Where $F_{recovery}$ represents the fault recovery rate, $P_{failure}(t)$ is the probability of failure over time, and $R_{fau/t}$ Is the recovery rate. This was particularly useful when there were limited resources to utilise or when the network had to support a large number of devices online simultaneously. Having adaptive protocols also optimised the utilisation of the network even further, making it more efficient because adaptive protocols automatically changed modes of communication based on available network traffic. Protocols such as MQTT, CoAP, and AMQP were utilised in a manner that optimised data exchange without overhead, while maintaining efficient and fast communication. The policies adaptively modify the rate of transmission, message size, and data channels so that data is transferred as a function of network loading and bandwidth availability, rather than speeding up data transfer and wasting redundant data that causes congestion. Similarly, the system also benefited from reduced data transmission overhead, i.e., less energy and bandwidth were consumed during communication, allowing more resources to be reserved for other critical activities.

Table 2: Performance values of every IoT node in the network

Node ID	Energy Usage (mAh)	Data Transmission (MB)	Response Time (ms)	Uptime (%)
Node 1	25	3.2	150	98
Node 2	28	2.9	160	96
Node 3	22	3.5	140	99
Node 4	24	3.0	130	97
Node 5	30	3.1	145	95

Table 2 presents the performance metrics of each IoT node in the network, including power consumption, data transfer, response time, and uptime. The nodes denote variations in power consumption, data transfer rates, and response times. Node 1 is the least power-consuming (25 mAh) and the most uptight (98%), reflecting that it possesses the optimal performance and dependability. Node 3 consumes 22 mAh of power and has the shortest response time of 140 ms, which is typical of its faster speed compared to other nodes. Node 2 consumes 28 mAh power with a relatively poor uptime of 96% and a bigger response time of 160 ms, once again justifying its average functionality. Node 4 has a 24 mAh power consumption and a 130 ms response time, with 97% availability, which speaks well to its balance of efficiency and dependability. Node 5, the most power-hungry (30 mAh), also possesses a relatively greater response time of 145 ms and lower availability (95%). This suggests that it can be best achieved in terms of performance. Based on the results, it is proposed that all nodes exhibit good performance, but also display different levels of response times and efficiency, indicating that each node will need to be optimised within the current network limitations. The dynamic nature of these nodes reflects the system's overall autonomy and flexibility, where resource management techniques and dynamic decision-making collectively contribute to global network performance.

Bandwidth efficiency calculation is:

$$\eta_{bandwidth} = \frac{B_{used}}{B_{tota/}} \text{ where } B_{used} = \sum_{i=1}^{n} P_i \cdot D_i \qquad (4)$$

Where $\eta_{bondwidth}$ Is the bandwidth efficiency? B_{used} is the total bandwidth used by all devices, and P_i, D_i Are the power and data rate of device i, respectively? The node energy consumption model is given below:

$$E_i = (P_i \times T_i) + C_{idle} \qquad (5)$$

where P_i Is the power, T_i Is the time, and C_{idle} It is the idle cost.

Where E_i Is the total energy consumption of node i, P_i Is the power consumption, T_i Is the time the node is active, and C_{idle} Represents the energy consumption during idle periods.

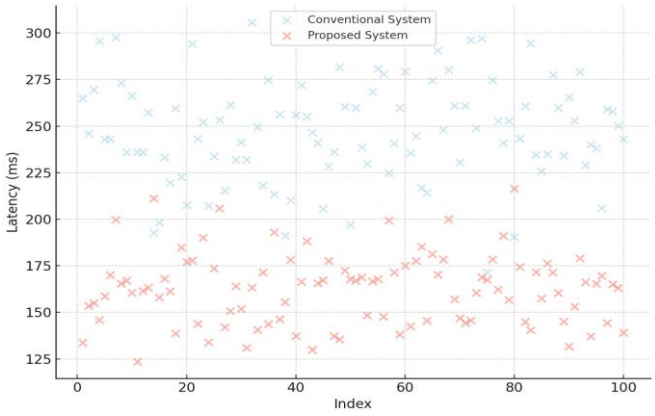

Figure 3: Latency for traditional vs proposed system

The traditional and proposed IoT system values for latencies with a large dataset are illustrated in Figure 3. Figure 3 shows 100 points for both systems. Light blue dots represent the latencies of traditional systems, while salmon-colored dots illustrate the latencies of the proposed system. Both datasets were based on a normal distribution with different mean and standard deviation values to simulate the case in actual networks. The ideal system exhibits greater variability in delay, ranging from approximately 190 ms to 320 ms, which would be the case in a less ideal system that causes different levels of delay. Although the system used does exhibit clustered latency fluctuations with a mean of 140 ms to 190 ms, this represents the optimality and minimum fluctuation of the system. The scatter plot confirms the robustness of the proposed system and its enhanced response, making it more dependable in dynamic environments. Visualisation of massive data is focused on illustrating the enormous disparity in network performance, with an overall advantage from the use of intelligent systems in IoT network latency management.

Additionally, the adaptive protocols of the system also achieved commanding positions in terms of higher fault recovery ratios. With intelligent algorithms that identify faults in real-time and proactively anticipate possible faults ahead of time, the system typically recovers from faults efficiently. In the event of network or device failure, the topology rerouted communication systems, diverted data streams, and assigned operations to secondary nodes to ensure availability and remain fully operational

with minimal downtime. Fault-active detection and recovery further improved network stability by enabling the system to operate even under austere conditions or partial information loss. The self-healing of network faults also reduced the need for human intervention, which not only improved the system's efficiency but also reduced its cost and faults through manual corrections.

All of these enhancements to the overall proposed architecture resulted in significant improvements to the network's performance, including reduced response times, increased resource utilisation, and stable network operation. Minimisation of data latency and overhead, along with improved fault recovery ability, led to an enhanced and stable overall system that can be utilised in real-time, large-scale IoT applications. They are at the core of IoT networks operating in highly dynamic bandwidth-limited environments where milliseconds and bandwidth bits are valuable. Through the collaboration of adaptive communication protocols and context-aware decision-making algorithms, the architecture was able to overcome some of the inherent bottlenecks of IoT systems, opening the door for more scalable, efficient, and self-driving networks to address the growing needs of the IoT ecosystem.

6. Discussion

The results demonstrate the effectiveness of the proposed architecture in IoT networks, enhancing performance through increased adaptability, autonomy, and efficiency. The results in Table 1 illustrate a drastic reduction in primary performance metrics, primarily response time and latency, which are of utmost concern for efficient and reliable communication in IoT systems. Latency on the new platform decreased by 35%, from 250 milliseconds on the baseline platform to 162 milliseconds, which is a measure of the success of dynamic architecture adaptation in managing data flow and reducing delay. That is because adaptive protocols were used that dynamically adapt communication based on real network conditions, ensuring the system remains responsive to traffic variations. Moreover, the system's energy consumption decreased from 30% to 22%, as shown in Table 1, indicating a significant improvement in the crucial battery life of IoT devices, particularly in resource-limited environments where frequent battery replacements are both expensive and time-consuming. The focus on optimising resource utilisation through flexible systems lies at the core of this success.

Apart from this claim, the fault rate recovery for the system is also improved to 92% from 75%, as shown in Table 1, where the machine learning model of the proposed architecture can predict likely locations where network traffic is likely to occur and anticipate these beforehand. Machine learning algorithms enable the system to forecast network traffic, detect congestion before it acts as a bottleneck, and automatically recover from faults. This forecasting capability not only enhances recovery from faults but also prevents the system from becoming unstable, even under a heavily loaded network, resulting in improved reliability and availability. The scatter plot in Figure 3 also confirms these results, showing that the new system has lower latency and is more balanced than the classic system. The scatter plot shows the smoother curve of latency in the new system, not only establishing that the system is faster but also more stable under communication delay.

This performance predictability stems from self-tuning protocols and architecture predictability, which enable optimal communication under varied loads. Second, the high recovery from fault, as shown in Table 1, translates into reduced disturbance and a faster recovery whenever a fault arises —a condition extremely critical for the execution of real-time IoT applications, which must never fail. The architecture shown here, coupled with machine learning and adaptive protocols, represents a monumental revolution in IoT technology, not only in speeding up networks but also in making them fail-safe. The heightened network reliability and fault recovery are truly critical to mission-critical IoT applications, such as industrial automation, medical, and smart cities, where even a fraction of a second of outage would have disastrous consequences. Furthermore, Table 2 presents the performance of each node in the IoT with the change in energy consumption and response times per node.

The effectiveness of the proposed system in handling the performance of individual nodes, as reflected by reduced energy consumption and quicker response times, is responsible for enhancing the overall network performance. This flexibility is a requirement in IoT networks, where nodes can vary in terms of processing capacity, power source, and performance. Calibrating the performance of each node to meet its specific requirements ensures the entire network operates in a balanced and energy-efficient manner. From a system maintenance perspective, energy consumption reduction and enhanced fault tolerance have a direct correlation with fewer maintenance steps, thereby enhancing the lifespan of devices and lowering the cost incurred. Predicting failure before it occurs and enabling adaptive system behaviour in real-time significantly reduces the need for human intervention, which is crucial in large-scale IoT deployments involving thousands or even millions of devices, as a logistical disaster would result otherwise. Overall, the results validate that the proposed architecture significantly enhances the performance of IoT networks by improving adaptability and autonomy. The combination of machine learning-based prediction, adaptive communication protocols, and energy-conscious design makes the system low-maintenance, efficient, and reliable, thereby providing a highly effective solution for contemporary IoT networks.

7. Conclusion

Our work introduces a new architecture to address fundamental challenges in the Internet of Things (IoT) network, providing autonomy and flexibility. The introduced architecture is low-latency in nature, hence supporting quicker communication and real-time decision-making capabilities, which are important for mission-critical use cases. The architecture further optimises resource utilisation, ensuring that processing, storage, and bandwidth are allocated to maximise the benefits of processing the large volume of data generated by IoT devices. This leads to system performance in general, especially in resource-constrained environments. Distributed edge computing and adaptive communication protocols also optimise the fault recovery mechanism of the system. These characteristics collectively enable online failure detection and recovery, minimising downtime and providing a seamless service. Incorporation of machine learning models into the system introduces an element of intelligence, enabling devices to dynamically compensate for variations in the network and predict future behaviour. This characteristic enhances the system's flexibility in dynamic environments where conditions change rapidly. In total, through the application of adaptive protocols, distributed computing, and machine learning, the IoT network can be effectively regulated and relied upon, even in adverse and hostile environments, thereby providing avenues for autonomous and intelligent, future-proofed IoT systems.

7.1. Limitations

Although the provided system has high potential for success, certain limitations must be addressed to enable the system to be utilised to its fullest potential and deployed effectively. The edge nodes require extra hardware resources, which is one of the key limitations. The edge nodes perform processing near the origin, thereby increasing the system's responsiveness and reducing latency. However, this also necessitates more edge processing and storage, making deployment more costly. In environments that are resource-constrained or have a large number of edge nodes, this can be a very costly endeavour. The richness of real-world environments also introduces another wrinkle in the model's success. Although the system works optimally under controlled conditions, the dynamic nature of uncontrolled conditions—i.e., varying network conditions, varying device behaviour, and constantly varying environmental conditions—can adversely affect overall performance. The learning models used within the system must be periodically updated to adapt to changing conditions and ensure optimal performance. The ongoing requirement for upgrades creates additional maintenance and resources, which can lead to increased operating costs and complexity. Therefore, the system is of great value in terms of efficiency and performance; however, its weaknesses are areas where large-scale deployment requires extra tuning and investment.

7.2. Future Scope

Several avenues of future study have the potential to make the system described more robust and more viable for a wide range of future IoT applications. One of these is the application of more sophisticated deep learning techniques in efforts to scale the system and enhance prediction accuracy in network activity. Deep learning methods with the capacity to analyse enormous volumes of data and recognise subtle patterns can make even more precise predictions regarding network traffic, future failures, and device activity, and thus lead to even improved resource utilisation and decision-making. Another direction for development is the integration of blockchain-based security functions. Blockchain can support integrity, confidentiality, and data protection in IoT networks in an immutable, decentralised ledger of transactions.

The adoption of technology can enhance system trust levels and facilitate secure data transfer, which is crucial in high-stakes applications such as finance and healthcare. Infrastructure development to enable cross-domain integration of the IoT can also achieve new dimensions of innovation opportunity. By enabling different IoT networks to communicate with each other and collaborate across domains such as cities, agriculture, and healthcare, the system would develop a more cohesive and integrated IoT ecosystem. Interoperability across domains can enable more advanced and meaningful use cases, such as predictive maintenance, real-time environmental monitoring, and autonomous transportation systems. These cross-domain convergence, deep learning, and security breakthroughs can even be used to create even more intelligent IoT systems, driving innovation even faster and penetrating even deeper into other sectors.

Acknowledgement: The authors gratefully acknowledge Malla Reddy College of Engineering for its support and encouragement throughout this research. The institution provided valuable resources and a conducive environment for academic inquiry. We extend our sincere thanks for their continued commitment to fostering research and innovation.

Data Availability Statement: Data supporting the findings of this study are available from the corresponding author upon reasonable request.

Funding Statement: The research and writing of this paper were conducted without the aid of any external funding or sponsorship.

Conflicts of Interest Statement: The authors affirm that there are no conflicts of interest related to this work. All sources of information have been properly acknowledged and cited.

Ethics and Consent Statement: The study was conducted in accordance with the ethical standards, and informed consent was obtained from all participants involved in the research.

References

1. M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, and L. Ladid, "Internet of things in the 5G era: Enablers, architecture, and business models," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 510–527, 2016.
2. T. M. Fernández-Caramés, "An intelligent power outlet system for the smart home of the internet of things," *Int. J. Distrib. Sens. Netw.*, vol. 11, no. 11, pp. 1-11, 2015.
3. M. E. E. Alahi, L. Xie, S. Mukhopadhyay, and L. Burkitt, "A temperature compensated smart nitrate-sensor for agricultural industry," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 9, pp. 7333–7341, 2017.
4. M. E. E. Alahi, N. Pereira-Ishak, S. C. Mukhopadhyay, and L. Burkitt, "An internet-of-things enabled smart sensing system for nitrate monitoring," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4409–4417, 2018.
5. M. E. E. Alahi, S. C. Mukhopadhyay, and L. Burkitt, "Imprinted polymer coated impedimetric nitrate sensor for real-time water quality monitoring," *Sensors and Actuators B: Chemical*, vol. 259, no. 4, pp. 753–761, 2018.
6. S. Syed, D. Sierra-Sosa, A. Kumar, and A. Elmaghraby, "IoT in Smart Cities: A survey of technologies, practices and challenges," *Smart Cities*, vol. 4, no. 2, pp. 429–475, 2021.
7. Y.-S. Jeong and J. H. Park, "IoT and smart city technology: Challenges, opportunities, and solutions," *Journal of Information Processing Systems*, vol. 15, no. 2, pp. 233–238, 2019.
8. D. Kim, S. Jeon, J. Shin, and J. Taek Seo, "Design the IoT botnet defense process for cybersecurity in smart city," *Intell. Autom. Soft Comput.*, vol. 37, no. 3, pp. 2979–2997, 2023.
9. P. Bellini, P. Nesi, and G. Pantaleo, "IoT-enabled smart cities: A review of concepts, frameworks and key technologies," *Applied Sciences*, vol. 12, no. 3, p. 1607, 2022.
10. Z. Allam and Z. A. Dhunny, "On big data, artificial intelligence and smart cities," *Cities*, vol. 89, no. 6, pp. 80–91, 2019.
11. N. Kapoor, N. Ahmad, S. K. Nayak, S. P. Singh, P. V. Ilavarasan, and P. Ramamoorthy, "Identifying infrastructural gap areas for smart and sustainable tribal village development: A data science approach from India," *International Journal of Information Management Data Insights*, vol. 1, no. 2, p. 100041, 2021.
12. F. Cugurullo, "Urban artificial intelligence: From automation to autonomy in the smart city," *Frontiers in Sustainable Cities*, vol. 2, no. 7, pp. 1–14, 2020.
13. R. Huang, H. He, Q. Su, M. Härtl, and M. Jaensch, "Enabling cross-type full-knowledge transferable energy management for hybrid electric vehicles via deep transfer reinforcement learning," *Energy (Oxf.)*, vol. 305, no. 10, p. 132394, 2024.
14. J. Paska, S. Boger, and A. Seneviratne, "Smart Cities and the Internet of Things: Impact on Urban Development," *Smart Cities*, vol. 3, no. 3, pp. 307–325, 2020.
15. Y. Zhang, Z. Qian, J. Xu, Y. Zhang, S. Shen, and J. Wang, "Deep Reinforcement Learning for Smart Grid Energy Management," *IEEE Trans. Smart Grid*, vol. 13, no. 9, pp. 2278–2287, 2022.