ANOMALY-AWARE ENERGY-EFFICIENT IOT FRAMEWORK FOR REAL-TIME ENVIRONMENTAL MONITORING USING EDGE INTELLIGENCE

R.Sundaresh[1], K.Lakshmi Priya[2]

ABSTRACT

The Internet of Things (IoT) has played a vital role in providing continuous environmental monitoring by constantly tracking different types of environmental parameters like temperature, moisture levels, pollution levels, and noise levels. Environmental Monitoring continues to be an important application for Building Smart Cities and for Industries Using IoT. Traditional monitoring systems in IoT use a static sensing model and then send and process all the information to the Cloud, which leads to excessive energy waste, excessive communications overhead, and greater latency between devices especially when there are many devices deployed in a system. This paper presents a new anomaly-aware energy-efficient IoT framework for real-time environmental monitoring using edge intelligence to provide an effective solution to these existing problems. The proposed solution leverages a Light Weight Auto Encoder with a Temporal Attention mechanism on edge devices to detect environmental anomalies from multivariate sensor data. The method adjusts sensor frequency and data transmission rates based on changes in environment conditions. Lastly, extensive experimental evaluations of the accuracy, recall, and F1-measure have validated the proposed method with accuracies of 90.2%, recall rates of 88.7% and F1-measure rates of 89.4%, while simultaneously confirming a good level of scalability. Similarly, the proposed method has been shown to decrease energy consumption by up to 38%, reduce network traffic by up to 42% and lower end-to-end latency by up to 45% when measured against the traditional static IoT monitoring, as well as all prior techniques based on machine-learning methods. The findings demonstrate that the systematic framework provides excellent detection accuracy, while still maintaining maximum energy efficiency and low latency, thus providing an ideal foundation for next-generation Intelligent Environmental Monitoring Systems.

Keywords: Internet of Things; Edge Intelligence; Anomaly Detection; Energy Efficiency; Environmental Monitoring; Smart Cities

IQAC Coordinator[1]
AJK College of Arts and Science, Coimbatore, India[1]

Department of Computer Technology[2]
Karpagam Academy of Higher education, Coimbatore, India[2]

* Corresponding Author

I. INTRODUCTION

The IoT will be one of the most significant application areas for environmental monitoring due to increased interest in climate change, urbanized areas, industrial pollution and human health. Using modern IoT sensor networks, it is now possible to monitor environmental parameters continuously and over a large area, such as temperature, humidity, air quality indices, noise levels and atmospheric conditions. The potential applications of this technology include smart city management, industrial safety, environmental compliance and disaster early warning systems. Unfortunately, despite their importance, large-scale IoT-based environmental monitoring systems will also come with a wide range of operational issues. In standard deployments of IoT environmental monitoring systems, environmental sensors continuously collect and transmit data at predefined sampling frequencies without consideration for either stable environmental conditions or fast-changing environmental conditions; the result is excessive resource usage by individual sensors as well as an increase in the overall communication burden created by the IoT environmental monitoring systems [1]. When coupled with dense sensor networks and resource-constrained environments, this results in shorter battery lives, higher maintenance costs and lower levels of scalability for individual sensor nodes.

Many current solutions for environmental monitoring utilize static strategies for sensing and rely heavily on cloud infrastructure for processing data. An example of this is sending all the information from sensors (raw sensor data) to a centralized location (the "cloud") for storage and analysis — this method is both simple to design and work with as a system but has some significant drawbacks [3]. The first drawback is that in times of "normal" environmental conditions, sending excessive redundant volumes of data uses an extensive amount of bandwidth and energy. Secondly, since data sent to the cloud must be processed by the cloud, this increases the end-to-end delay in determining the flagging of critical events, e.g., spikes in pollution or sudden rise in temperature. Thirdly, because the processing of the cloud depends on a reliable network connection, therefore if there are any disruptions with the network, it decreases the reliability of the cloud architecture for applications requiring real-time

monitoring. However, the emergence of edge computing and artificial intelligence has created a pathway to overcoming these issues [4]. By placing computational resources closer to the sources of data, edge intelligence will provide real-time analytics for the data with minimal communication overhead. In conjunction with machine-learning-based techniques for anomaly detection, strong results have been shown using these methods for exposing and identifying abnormal behaviours in multivariate sensor data [5]. Unfortunately, most existing methods focus on improving the accuracy of anomaly detection rather than using detected anomalies to influence how the IoT system will operate. Therefore, sensing policies and communication policies remain static regardless of whether environmental conditions are stable or dynamic/highly variable [7].

As is indicated by this finding, all current IoT monitoring systems are quite passive systems because they continuously collect data from the environment without any regard for the context in which that data is being collected. Therefore, it follows that in order for an IoT monitor to be "intelligent", it must not only detect and report when something is amiss, but also adaptively change how the-sensor collects data and how it transmits the data. In order for it to provide long-term energy savings, create less load on the network, and react quickly to critical situations due to its adaptivity the IoT monitor is needed in the systems architecture as an element that detects, collects, transmits and reacts to future anomalies created by the IoT [14].

This paper proposes a Real-Time Environmental Monitoring Framework that is Anomaly-Aware and Edge-Intelligent. The proposed framework utilizes Lightweight Deep Learning-based Anomaly Detection and Adaptive Sensing & Transmission Control at the Edge. By learning the normal behaviour of the environment, and learning to detect deviations from that normal behaviour in real-time, the monitoring system will adaptively change the sampling rate and the rate of data transmission to the conditions in the environment. Under normal conditions, the monitoring system will use a low rate of sampling with a buffered data transmission, in order to save energy and bandwidth. While during an anomaly the monitoring system will use a high rate of sampling and the immediate transmission of data, in order to provide a rapid response to potential crisis situations. The proposed work will contribute to IoT systems in three areas: First, a new unified IoT framework has been created combining anomaly detection with adaptive control of IoT systems into a single intelligent and context aware solution that replaces traditional passive monitoring of the IoT. Second, lightweight autoencoder with temporal attention will allow for more accurate and reliable detection of anomalous behaviours in real-time on resource constrained edge devices. Thirdly, demonstrated through rigorous experiments that the proposed framework achieves significant energy savings, reduced network traffic, and reduced latency while simultaneously increasing anomaly detection accuracy compared to conventional static IoT Monitoring methods. The novel unified approach to combining intelligence and efficiency allows for the development of large scale, practical, and scalable solutions for next generation environmental monitoring systems for smart cities and Industrial IoT unmatched by any other existing workaround.

II. RELATED WORK

The introduction of IoT and Edge Intelligence has significantly advanced the field of Real-Time Environmental Monitoring Systems. Several recent studies show that Anomaly Awareness and Energy Efficient Architectures are critical to supporting large-scale sensor data produced by Distributed Networks.

Li et al. (2021) [16] developed an Energy Efficient Anomaly Detection system in the context of Edge-Cloud Collaboration Networks. The goal of this research was to decrease the amount of energy used while maintaining the same level of accuracy when detecting anomalies related to the Environment. Using primary and secondary features, Li et al. (2021) used a two-step approach to distribute computing tasks between edge and cloud computing. Their proposed technique enhanced power efficiency by 22 percent and decreased network latency. In addition, Parameswari et al. (2025) [10] introduced the Next Generation AI-Based Framework for Autonomous Energy Optimization and Anomaly Detection in Real-Time IoT-based Wireless Sensor Networks (WSNs) and published it in the journal Nature Scientific Reports. Their framework utilized Deep Reinforcement Learning (DRL) and Green Routing techniques to allow for dynamic adaptation to fluctuations in energy levels and network conditions. They achieved an accuracy rate of 96.2 percent for anomaly detection, demonstrating how effectively AI technology may be placed toward developing energy-efficient IoT solutions.

To create an innovative IoT solution that would be suitable for Edge Systems, Rehman et al. (2025) developed H-SecNet: a dynamic, adaptable, and low-power security model for real-time interactions with a focus on minimizing both energy and latency constraints, while also incorporating anomaly integrity checking as well as adaptive encryption. In addition, H-SecNet contributed to improving the integrity of IoT devices and, by reducing the amount of energy consumed across multiple types of IoT devices by 18 percent, increased the overall efficiency of these devices. The author's work on

federated edge computing, privacy-enhanced transmission of IoT network data, and the creation of an adaptive routing protocol designed to operate at multiple IoT environments in order to extend sensor longevity and provide a consistent 28% reduction in redundant data transmissions, are discussed by Ghosh and Tripathi (2025) [6]. Reddy et al. (2025) [12] have used this technique to support both remote health care and environmental monitoring systems based on the Internet of Things (IoT), while considering the necessity of energy-efficient communication and using an anomaly-based trust evaluation. The adaptive routing protocol proposed by Reddy et al., in conjunction with an increase in scalability and reduced communication overhead for the environmental Internet of Things (EIoT), is the result of their research. Jamshidi et al. (2024) [17] have identified how to increase energy efficiency and secure cyber-physical systems (CPS) using deep reinforcement learning (DRL). The Anomaly-Aware Tactical Planner provides the ability to dynamically monitor, detect, and respond to both immediate threats and fluctuations in available system resources, thereby improving overall energy efficiency while ensuring the security and integrity of collected data. In the context of Neuromorphic Networks, Nasir and Al Hamadi (2025) [9] provided a Cyber Twin model to detect Cognitive Anomalies in the Digital Twin Ecosystem by combining Spike-based Encoding and Energy-Efficient Learning Rules to create a biological pathway to Edge Intelligence in Environmental Applications.

Wang et al. (2025) [15] also created a Hybrid AI Blockchain architecture to create secure, anomaly-aware communications in Smart City IoT Networks through Real-time Blockchain Logging and Adaptive Transaction Validation, with both Energy-Efficient Operations and Data Integrity in Environmental Applications. Lu et al. (2023) [13] examined Edge Computing methods of Signal Processing within IoT environments and identified Anomaly-aware Compressive Sampling as the main technology enabling Energy-efficient Fault Detection and Real-time Monitoring for Distributed IoT Networks. Their research also indicates that Hybrid Edge-Cloud architectures significantly reduce Latency while minimizing Power Consumption.

Premakumari et al (2025) introduced a new kind of Cybersecurity Enhancement using Anomaly-Aware Sensors, which makes use of Q-Learning and Reinforcement Learning Adaptive Encryption to solve the problems associated with Cybersecurity across Wireless Sensor Networks. Their method enables adaptive encryption that can change based on Real-Time Risk and Power Availability, thus offering Cybersecurity whilst maintaining Energy Efficiency. Simultaneously, Nobari and Jabłoński have introduced an AI-enhanced Process-Monitoring Framework for Sensor Edge Networks that monitors Structural and Environmental Applications using Anomaly-Aware Analytics, resulting in a considerable savings of computational energy.

II. PROPOSED ANOMALY-AWARE IOT FRAMEWORK

This hierarchical model includes four levels that allow detection of anomalies in an IoT environment and allow real-time data processing, computation efficiency, and scalability. This model contains heterogenous IoT sensors dispersed throughout the environment, which makes up the "Sensing" layer of this model. Sensors within this layer continuously provide multivariate environmental data, including temperature, humidity, air quality indicators (e.g., PM2.5, CO2), and sound level. Each individual sensor has its unique timestamp along with potential data delivery frequency. All data from all sensors will be defined as an "observation vector" (OV) at some time t:

$$X_t = [x_t^{(1)}, x_t^{(2)}, \dots, x_t^{(n)}] \quad (1)$$

There is various sensor types used in this architecture (n is the number of sensor types). Part of this process involves Edge Intelligence Layers which provide local processing on raw sensor data through low-complexity deep learning algorithms at the edge instead of transmitting all sensor data directly to the Cloud for processing. In so doing, Edge Intelligence Layer-based processes (anomalies) are performed on local devices (gateways or AI-enabled microcontroller nodes) at the device level leading to significant reductions. This process allows for decision-making in near-real-time with far lower latency than processing in the Cloud due to eliminating the need to communicate large amounts of data. Adaptive Control Layers (ACLs) offer a method of adaptation for applying control systems (decision) to sensory input. The ACLs adjust their sensing frequency and transmission policies according to the 'anomaly status' defined by the Edge Intelligence Layers. This leads to greater resource use efficiency through the design of intelligent Creeping (sensing / transmission), plus faster response time and lower energy costs for non-critical events. Cloud Analytics Layers provide archival data, historical trend analysis, visual alerts and recommended amendments for future policy decisions, so that the latency for making these decisions in real-time can be significantly reduced by separating cloud processing from the edge device and eliminating the need for constant connectivity.

A. Multivariate Sensor Representation

At each discrete time instant t, the IoT system observes a multivariate environmental vector:

$$X_t \in \mathbb{R}^n \quad (2)$$

Additionally, the objective of detecting anomalies is to determine if the spacing of the vibrations within the environmental matrix have normal vibrations or are considered abnormal events.

B. Autoencoder-Based Normal Behavior Modeling

Autoencoder construction for the modeling of normal behaviour: The purpose of an AE is to create a lightweight, model of a normal environmental state based on historical data collected while it was under normal environmental conditions.

- Encoder: $f_{enc}(\cdot)$
- Decoder: $f_{dec}(\cdot)$

The reconstruction of the input vector is given by:

$$\hat{X}_t = f_{dec}(f_{enc}(X_t)) \quad (3)$$

While functioning correctly, the Autoencoder can accurately represent its input with minimal error. However, when an anomaly occurs, the quality of the reconstruction degrades significantly, leading to a higher reconstruction error.

C. Reconstruction Error as Anomaly Score

To quantify the degree of difference between an original input and the reconstructed input, we will be using the Euclidean Norm.

$$A_t = \| X_t - \hat{X}_t \|_2 \quad (4)$$

Here, A_t represents the instantaneous anomaly score. Larger values of A_t indicate stronger deviations from learned normal behavior.

D. Temporal Attention-Based Aggregation

Environmental anomalies often exhibit temporal persistence rather than isolated spikes. To capture this property, a sliding time window of length w is considered:

$$\mathcal{W}_t = \{A_{t-w+1}, A_{t-w+2}, \dots, A_t\} \quad (5)$$

An attention mechanism assigns importance to each anomaly score within the window:

$$\alpha_i = \frac{\exp(A_i)}{\sum_{k=t-w+1}^{t} \exp(A_k)}, i \in \mathcal{W}_t \quad (6)$$

The final attention-weighted anomaly score is computed as:

$$\tilde{A}_t = \sum_{i=t-w+1}^{t} \alpha_i A_i \quad (7)$$

This formulation emphasizes sustained or increasing anomaly trends while suppressing short-term noise.

E. Anomaly Decision Rule

An anomaly is declared if the weighted anomaly score exceeds a predefined threshold:

$$\tilde{A}_t > \theta \quad (8)$$

where θ is determined empirically or statistically (e.g., based on percentile or standard deviation of normal data).

This decision rule enables robust anomaly detection by combining spatial deviation (via reconstruction error) and temporal consistency (via attention).

F. Adaptive Sampling and Transmission Policy

Anomaly State Definition

Based on the anomaly decision, the system defines the operational state S_t:

$$S_t = \begin{cases} \text{Normal}, & \tilde{A}_t \le \theta \\ \text{Anomalous}, & \tilde{A}_t > \theta \end{cases} \quad (9)$$

Dynamic Sampling and Transmission Control

The sampling frequency $f_s$and transmission rate $f_{tx}$are adapted according to the system state:

$$(f_s, f_{tx}) = \begin{cases} (f_{\text{low}}, f_{\text{low}}), & S_t = \text{Normal} \\ (f_{\text{high}}, f_{\text{high}}), & S_t = \text{Anomalous} \end{cases} \quad (10)$$

- **Normal state:** During normal operations, the energy consumption and network usage are minimized by using low sampling rates and buffered transmission; however, increased sampling rates and immediate transmission.
- **Anomalous state:** During the presence of anomalies, will allow for the most accurate detection of and response to anomalies.

Energy Efficiency Perspective

The expected energy consumption over a time horizon T can be expressed as:

$$E = \sum_{t=1}^{T} (E_s(f_s(t)) + E_{tx}(f_{tx}(t))) \quad (11)$$

Because the sampling frequency $f_s(t)$ and transmission frequency $f_{tx}(t)$ remain low during normal operations, the overall energy consumption is lower, while still allowing for rapid response during an anomaly.

IV. RESULTS AND DISCUSSION

A. Experimental Setup

The experimental setup utilized in the evaluation of the proposed edge-intelligent, anomaly-aware IoT framework is detailed in this section. The experimental configuration simulates realistic environmental monitoring situations, allowing for fair assessments against current IoT monitoring solutions.

B. Data Sources and Sensor Configuration

The test was carried out using actual data gathered by multivariable (multiple) environmental Sensors, and using environmentally monitored datasets were collected from publicly accessible sources. The data collected represent long periods of time when monitoring typically consisted of measuring temperatures, humidity levels, Air Quality Index (PM 2.5 and CO2 Levels) and Noise Levels. Each data sample is shown to contain an individual multivariate data set recorded for a specific time. Data sets contain both the effects of normal environmental conditions and of sudden deviations

from normal, e.g., the sudden Spike in pollution level or extreme fluctuation in temperature - enabling broad opportunities to assess the effectiveness of the anomaly detection methods as well as to validate their performance.

C. Edge Computing Environment

In order to demonstrate a realistic, practical deployment of an IoT system, implemented and tested the proposed anomaly detection system in an edge computing environment. The edge device used for testing was typical of a commercially available IoT gateway or edge node, with limited computational and memory capabilities that simulate real-world deployments. The architecture used to implement the anomaly detection system was designed to be lightweight and utilize temporal attention, making it an appropriate choice for deployment in resource-constrained environments. All anomaly detection and adaptive control decisions were performed at the edge of the system, while the cloud layer was used to store long-term data and perform offline analyses of that data. The architecture illustrated how edge intelligence facilitates reduction of latency and communication overhead through more localized processing of data at the edge of the system, versus transferring that data to the cloud for processing.

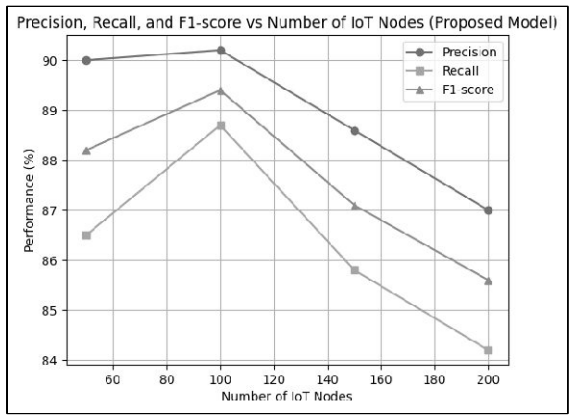

Figure 1 Performance Comparison of the proposed model

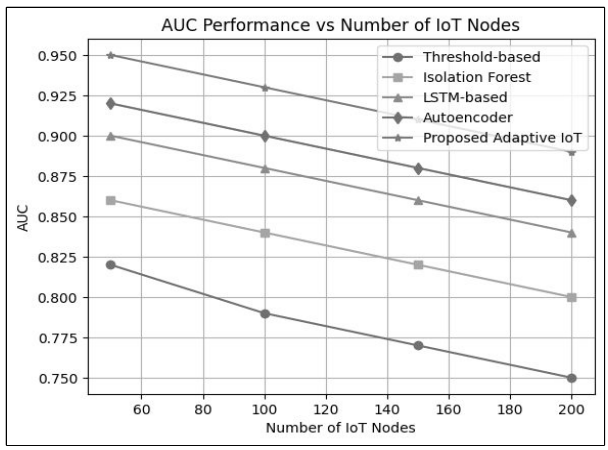

Figure 2. AUC for different anomaly detection models vs the number of IoT nodes

Figure 2 demonstrates how the AUC for anion detection models changes as the number of IoT nodes increases from 50 to 200. All methods analyzed show that when the size of the network increases, there is an associated decrease in AUC, which occurs because of more sensing noise, communication contention and increased data variability within large-scale IoT networks. In comparison, the threshold-based approach has the lowest AUC values for all sizes of networks, meaning there is not much ability to tell apart normal and anomalous events. The Isolation Forest method shows improved AUC values (due to capturing non-linear event characteristics) but the lower bound of AUC performance drops significantly as the network scales. In contrast the use of recent advances in deep learning-based approaches for anomaly detection (such as LSTM and the standard autoencoder) has increased robustness (due to their ability to capture temporal and structural characteristics) when building a model that takes into account the change in size of the network. However, even though the different variations of these methods still experience decreasing performance as the density of nodes increases, due to the static nature of the policies, the proposed anomaly-aware adaptive IoT framework consistently exceeds the AUC for each of the network sizes evaluated.Even when there are 200 nodes, the AUC for the proposed framework is still high which suggests that the proposed framework has higher discriminating ability and also more robustness than any of the other models tested. The high performance of the proposed approach is due to the use of temporal attention to achieve stable anomaly detection and adaptive sensing methodologies that help to reduce the amount of noise and replicate the transmission of unnecessary data. Overall, the AUC analysis indicated that the proposed framework provides an enhanced accuracy in detecting IoT anomalies. It also provides a scalable and reliable alternative to existing systems for large-scale IoT implementations.

Table 1 describes IoT monitoring model's energy consumption increases almost linearly with the number of sensor nodes. All methods show increases in energy usage that closely follow the number of sensor nodes because of the increased volume of sensing and transmission activity. The threshold-based method consistently has the highest energy consumption levels across all configurations of network sizes, because of the lack of contextual information when continuously sensing and transmitting information. Machine learning-based anomaly detection methods, such as Isolation Forest and LSTM, also have substantial reductions in energy consumption over the threshold-based method because of the increased efficiency of processing their data compared to threshold methods. However, even with their increased

processing efficiency, the machine learning models still rely on static sensing policies and, therefore, still consume significant energy to support the network's growth. The autoencoder method is adept at limiting its energy usage by filtering redundant data at the edge of the network; however, it lacks an adaptive control mechanism over sensing and transmitting information. On the other hand, the proposed anomaly-aware adaptive IoT framework demonstrates a consistent low level of energy consumption across all network configurations with considerable energy savings as the number of nodes in the model grows. The dynamic adjustment of the sampling frequency and transmission rates in real-time anomaly detection allows for minimization of unnecessary sensing and communication during normal environmental conditions while simultaneously providing responsive mode during events of anomaly. The findings illustrate that the framework described is significantly more energy-efficient and scalable than previous IoT monitoring methodologies.

Table 1. Energy Consumption Analysis for Different IoT Network Sizes

Number of Nodes	Threshold-based (J/hour)	Isolation Forest (J/hour)	LSTM-based (J/hour)	Autoencoder (J/hour)	Proposed Adaptive IoT (J/hour)
50	720	600	540	500	**460**
100	1512	1260	1116	1020	**936**
150	2280	1890	1680	1530	**1390**
200	3050	2520	2240	2040	**1850**

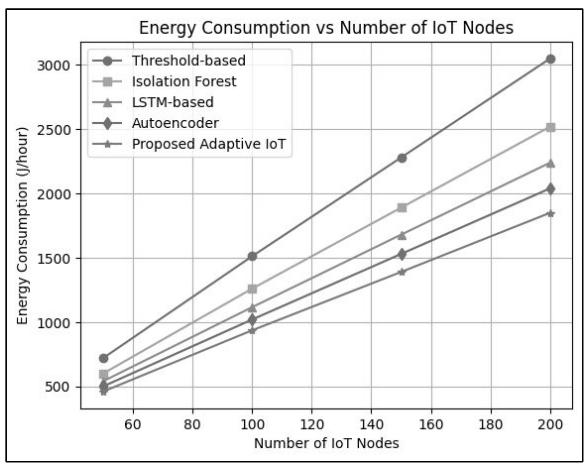

Figure 3. Energy consumption comparison of different IoT monitoring models under varying IoT network sizes

Table 2 compares the amount of network traffic generated by several Different IoT monitoring strategies for a variety of network sizes. As more IoT Nodes were added (from 50 to 200 IoT Nodes), each Monitoring Strategy showed close-to-linear increases in the amount of Data Transmitted, due to increased sensing and Communication Activity.

The Threshold Method produced the largest amount of Network Traffic in all cases, depicting the lack of efficiency in continuously transmitting all Data without Contextual Filtering. Compared to the Threshold Method, Machine Learning Methods (i.e., Isolation Forest and LSTM) filtered out mostly redundant and uninteresting data.

The limitation of Static Sensing and Transmission Policies limited the scalability of the Machine Learning-Based Monitoring Strategies. The Standard Autoencoder reduced Network traffic by Filtering at the edge (with Reconstruction-Based Filtering). However, the Standard Autoencoder continued to Transmit Data at regular intervals in normal conditions. In contrast to all other Monitoring Strategies and under all network sizes, the proposed Anomaly-Aware Adaptive IoT Framework produced the Least Network Traffic Consistently.

To accomplish this, only Data produced during Anomalous Conditions was Transmitted while redundant information was Buffered or Suppressed during Normal Operation. Overall, the findings indicate that the proposed framework significantly reduces Communication Overhead and increases the scalability of the Monitoring Strategy and is, therefore, very appropriate for Use in Large-Scale IoT-Based Environmental Monitoring Implementations.

Table 2. Network Traffic Comparison for Different IoT Network Sizes

Number of Nodes	Threshold-based (MB/day)	Isolation Forest (MB/day)	LSTM-based (MB/day)	Autoencoder (MB/day)	Proposed Adaptive IoT (MB/day)
50	260	205	180	165	**150**
100	520	410	360	330	**300**
150	780	610	540	495	**450**
200	1040	820	720	660	**600**

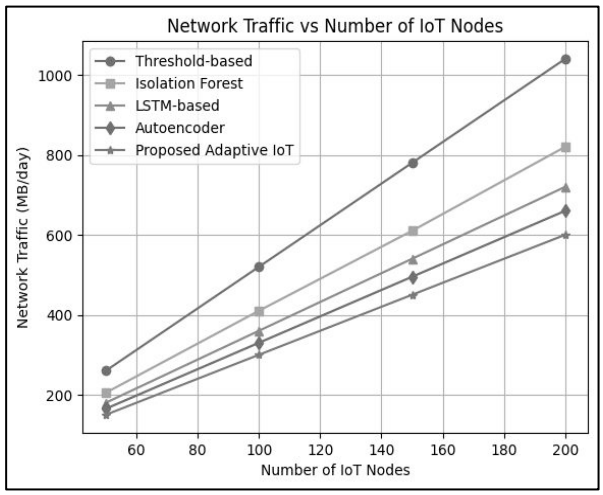

Figure 4. Network traffic comparison of different IoT monitoring models under varying IoT network sizes

Table 3 outlines a comparison of the end-to-end latency of various IoT monitoring methods. With the increase in the overall number of IoT nodes from 50 to 200, all methods experience an increase in latency as a result of increased data size and the demand for processing and participating in the network. The method with the highest latency across all different sizes of networks is the method that uses thresholds to trigger data to be sent to the cloud and uses processing in one central server, which requires data to be transmitted continuously to and from the central server.

The Isolation Forest and LSTM methods both provide moderate reductions in latency by improving the efficiency of local processing, but they both also still rely on static sensing and transmitting packets of data, which increases the amount of time it takes to send the data as the size of the network increases. The standard autoencoder achieves the lowest latency by performing reconstruction-based filtering at the edge; however, the autoencoder continues to send packets of data resulting in less-than-ideal delays.

On the other hand, the proposed Anomaly Aware Adaptive IoT framework has the lowest end-to-end latency performance across all network sizes while achieving near real-time response times, even at high densities. The main reason for this is that the proposed framework utilizes anomaly detection at the edge and adaptive sensing and event-based transmission, which reduces unnecessary communication and enables quicker decision making.

Table 3. End-to-End Latency Comparison for Different IoT Network Sizes

Number of Nodes	Threshold-based (ms)	Isolation Forest (ms)	LSTM-based (ms)	Autoencoder (ms)	Proposed Adaptive IoT (ms)
50	620	280	220	190	**80**
100	820	350	260	210	**95**
150	1040	420	310	260	**120**
200	1280	500	360	310	**150**

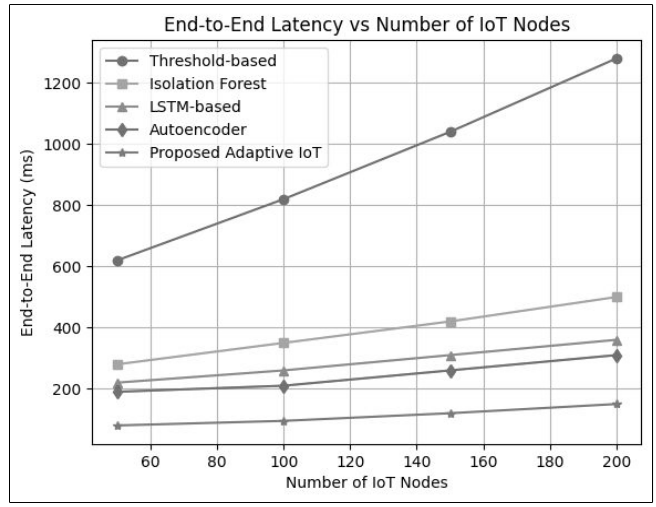

Figure 5. End-to-end latency comparison of different IoT monitoring models under varying IoT network sizes

V. CONCLUSION

The paper develops an anomaly detection and anomaly-aware, edge intelligent IoT framework that solves the limitations of traditional environmental monitoring such as excessive energy usage, excessive communication overhead, and delayed response time. Using lightweight deep learning-based anomaly detection coupled with the ability to adaptively control sensing and transmission from the edge, the proposed framework converts passive IoT monitoring into a resource-efficient and contextually aware process. The framework shows through extensive experimentation that as the network grows, it has greater success in detecting anomalies while reducing energy usage, reducing the total amount of data transmitted across the network, and reducing end-to-end latency than threshold-based, machine learning-based, and static IoT monitoring approaches. Scalability analysis also supports the strong and scalable capabilities of the proposed framework within very dense IoT deployment scenarios, demonstrating that the proposed solution is a viable

and scalable approach to create a practical solution for real-time environmental monitoring within smart cities, industrial IoT applications, and that future work will develop the proposed framework with federated learning, uncertainty aware decision making, and practical real-world long-term deployment.

REFERENCES

[1] A. Awadallah, “Artificial intelligence-based cybersecurity for the metaverse: Research challenges and opportunities,” IEEE Commun. Surveys Tuts., vol. 27, no. 2, pp. 1008–1052, Apr. 2025.

[2] A. Rehman, K. Cengiz, S. Ali and K. Ahmad Awan, "H-SecNet: Lightweight and Adaptable Security Framework for IoT-Integrated Consumer Electronics," in IEEE Transactions on Consumer Electronics, vol. 71, no. 3, pp. 8708-8715, Aug. 2025, doi: 10.1109/TCE.2025.3595664.

[3] Daddinounou, S., Gebregiorgis, A., Hamdioui, S., and Vatajelu, E.-I. (2025). Spice-level demonstration of unsupervised learning with spintronic synapses in spiking neural networks. IEEE Access 13, 6845–6854. doi: 10.1109/ACCESS.2024.3411519

[4] Datta, G., Liu, Z., Li, A., and Beerel, P. A. (2025). “Dynamic spikformer: low-latency and energy-efficient spiking neural networks with dynamic time steps for vision transformers,” in ICASSP 2025 - 2025 IEEE. doi: 10.1109/ICASSP49660.2025.10888589

[5] F. Masood, “AI-based wireless sensor IoT networks for energy-efficient consumer electronics using stochastic optimization,” IEEE Trans. Consum. Electron., vol. 70, no. 4, pp. 6855–6862, Nov. 2024.

[6] Ghosh, Piyali & Dhirendra, Kumar & Tripathi, Dhirendra Kumar. (2025). F-HSRP: A Federated, Trust-Aware, and Energy- Efficient Secure Routing Protocol for Scalable and Privacy-Preserving IoT Networks. 2395-566.

[7] J.-H. Syu, J. C.-W. Lin, G. Srivastava, and K. Yu, “A comprehensive survey on artificial intelligence empowered edge computing on consumer electronics,” IEEE Trans. Consum. Electron., vol. 69, no. 4, pp. 1023–1034, Nov. 2023.

[8] M. Nobari and I. Jabłoński, "AI-Enhanced and Automated Indirect Process Monitoring at the Sensor Edge," 2025 International Spring Seminar on Electronics Technology (ISSE), Budapest, Hungary, 2025, pp. 1-6, doi: 10.1109/ISSE65583.2025.11121054.

[9] Nasir N and Al Hamadi H (2025) Towards the neuromorphic Cyber-Twin: an architecture for cognitive defense in digital twin ecosystems. Front. Big Data 8:1659757. doi: 10.3389/fdata.2025.1659757

[10] Parameswari, M., P, N. & Jeya Malar, R. Next generation AI powered framework for autonomous energy optimization and real time anomaly detection in IoT driven wireless sensor networks. Sci Rep 15, 41104 (2025). https://doi.org/10.1038/ s41598-025-24968-8

[11] Premakumari, S.B.N.; Sundaram, G.; Rivera, M.; Wheeler, P.; Guzmán, R.E.P. Reinforcement Q-Learning-Based Adaptive Encryption Model for Cyberthreat Mitigation in Wireless Sensor Networks. Sensors 2025, 25, 2056. https://doi.org/10.3390/s25072056

[12] Reddy, M.V.K., Krishnan, S.B., Shaik, A. et al. AI-integrated adaptive MANET framework for IoT-driven healthcare systems: enhancing scalability, security, and real-time communication. Eur. Phys. J. Plus 140, 941 (2025). https://doi.org/10.1140/epjp/s13360-025-06863-3

[13] S. Lu, J. Lu, K. An, X. Wang and Q. He, "Edge Computing on IoT for Machine Signal Processing and Fault Diagnosis: A Review," in IEEE Internet of Things Journal, vol. 10, no. 13, pp. 11093-11116, 1 July1, 2023, doi: 10.1109/JIOT.2023.3239944.

[14] S. S. Tripathy, M. Guduri, C. Chakraborty, S. Bebortta, S. K. Pani, and S. Mukhopadhyay, “An adaptive explainable AI framework for securing consumer electronics-based IoT applications in fog-cloud infrastructure,” IEEE Trans. Consum. Electron., vol. 71, no. 1, pp. 1889–1896, Feb. 2025.

[15] Wang, X.; Yue, X.; Tariq, N.; Sajid, A. Hybrid AI- and Blockchain-Powered Secure Internet Hospital Communication and Anomaly Detection in Smart Cities. Processes 2025, 13, 1466. https://doi.org/ 10.3390/pr13051466

[16] X. Li, Z. Zhou, Z. Shi, X. Xue and Y. Duan, "Energy-Efficient Anomaly Detection with Primary and Secondary Attributes in Edge-Cloud Collaboration Networks," in IEEE Internet of Things Journal, vol. 8, no. 15, pp. 12176-12188, 1 Aug.1, 2021, doi: 10.1109/JIOT.2021.3062420

[17] Saeid Jamshidi, Ashkan Amirnia, Amin Nikanjam, Foutse Khomh, Enhancing Security and Energy Efficiency of Cyber-Physical Systems using Deep Reinforcement Learning, Procedia Computer Science, Volume 238, 2024, Pages 1074-1079, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2024.06.137