K.Jagadeesh, 2026, 14:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Integration of IoT Sensors and Cloud Analytics for Intelligent Threat Response

[1]K.Jagadeesh, [2]Betapudi Gagana, [3]Kota Chekitha Nagalakshmi, [4]Beeraka Yasaswi Subhagatri, [5]Kunduru Keerthi.

[1]Associate Professor, Department of IT, Vignan's Nirula Institute of Technology and Science for Women, Guntur.
[2,3,4,5]B.Tech, Department of IT, Vignan's Nirula Institute of Technology and Science for Women, Guntur.

Abstract- The number of Internet of Things (IoT) devices has exponentially increased the amount of fresh data from real-time sources in various fields such as smart cities, healthcare, manufacturing, and critical infrastructure. Nevertheless, the problem of handling and interpreting the huge volume of diverse data produced by these devices still stands, especially when it comes to promptly identifying threats and reacting to them. This paper presents a merged IoT-cloud threat response system that interconnects the heterogeneous IoT sensors with the cloud-based processing accompanied by machine learning techniques to sense the irregularities and foresee the security risks even before they emerge. At the same time, edge computing is cutting down on the delay and improving the responsiveness. Notably, the system is overcoming the issues of infinite scalability, data diversification, communication lags, and security loopholes via the effective handling of data, the initializing of self-adjusting learning models, and the use of the safe transmission protocols. The experimental results confirm the system's superiority in terms of detection accuracy, response time, and operational efficiency over the competitive methods. As the discussed scheme makes threat management more proactive and predictive, it can be considered as a versatile and scalable next-gen solution for smart surveillance and cybersecurity scenarios.

Keywords— IoT Sensors, Cloud Analytics, Intelligent Threat Response, Real-Time Monitoring, Anomaly Detection, Machine Learning, Smart Surveillance, Data Security, Predictive Analytics, Edge Computing.

I. INTRODUCTION

IoT devices with their sensors have brought a fundamental change in the way we collect, transfer, and analyze data in various fields [1]. IoT sensors, being a part of physical devices, are always ready to take the newest data, thus providing organizations with the ability of real-time monitoring, tracking, and anomaly detection at their own pace [2]. With the exponential increase of data, which originates from IoT, one can't think about these devices without linking them to cloud-based analytical platforms [3], which are needed for the data processing and interpretation tasks that lead to taking the right decisions [4].

What is more, IoT sensors have become the cornerstone of intelligent threat response systems because of their capability of uninterrupted observation of critical infrastructures, industrial systems, urban environments, and public places [5]. The gathered data may be examined to unveil potential risks like instances of unauthorized access, abnormal activities, equipment failure, or cybersecurity breaches [6]. Essentially, the earlier a threat gets detected, the less harm it will be able to do, safety will be assured, and preconditioned continuity will be kept [7]. Hence, the available capacities of cloud computing render it as an ample, elastic and economical service carrier for storage and data processing tasks related to IoT-generated data [8]. The fusion of cloud analytics with networks of IoT sensors delivers to businesses the power of accomplishing complex computational tasks, implementing sophisticated ML applications, and doing real-time data visualization at high speed [9]. Situated at the heart of intelligent threat detection and response systems, this fusion is therefore

capable of sifting through data streams of gigantic scale emanating from widely dispersed networks [10].

Thanks to the combo of IoT and cloud analytics, a network can anticipate and undertake security measures proactively [11]. As an instance, by analyzing both the historical and real-time data, predictive algorithms can identify upcoming breaches and inform timely interventions to avoid them [12]. The importance of this power could hardly be overestimated in the case of smart cities, industrial automation, healthcare monitoring, and critical infrastructure protection where the reaction has to be rapid and efficient [13].

On top of the benefits, the union of IoT sensors with cloud analytics comes with a range of technical hurdles [14]. Among these issues are the handling of the huge streams of data, the need for communication with low latency, the ensuring of data precision, as well as the safeguarding of the confidentialities [15]. The diversity of IoT devices and different network protocols make the task even more difficult and hence call for the deployment of robust middleware and standardized frameworks for unimpeded interoperability [16].

Another grave problem is security and privacy concerns that cloud systems face when they are IoT based [17]. In such circumstances, perpetrators may employ weaknesses in the sensor network or cloud infrastructure that will result in them obtaining unauthorized access, data manipulation, or project cyberattacks [18]. Thus, well-designed communication protocols, encryption methods, and access control policies are the key steps for ensuring both the data and the infrastructure integrity of smart threat response systems [19].

The latest publications have been focusing on the incorporation of machine learning, artificial intelligence, and big data techniques in IoT-cloud-based threat detection systems [20]. The algorithms that fall into the categories of anomaly detection [21], predictive modeling, and clustering can be used for automatic identification of the threat patterns [22]. By introducing these intelligent analytics methods, the developers achieve a reduction in the need for human intervention, improvements in the speed of detection, and better overall efficiency of the mechanisms of the threat response [23].

Firstly, the combination of IoT sensors and cloud analytics is the basis of modern intelligent threat response systems [24] [25]. Such systems make the security, reliability, and operational efficiency of various fields become dramatically better by securing the features of real-time monitoring, predictive analytics, and proactive interventions [26]. Still, to scale up the progress further, to provide higher levels of security and better data management, research and development efforts must be continued for ensuring that IoT-cloud-based threat response systems will continue to be effective and resilient in a world that is becoming more and more interconnected [27].

II. LITERATURE REVIEW

Sharma et al [1-5]. introduced an Intelligent Sensing Model for Anomalies Detection (ISMA) to tackle the challenge of cross-platform anomaly detection in online social networks (OSNs), users with different behavior in different connections on various platforms. These fraudulent or abnormal users can use the publicly available information to deceive the online community. ISMA uses cognitive tokens to intentionally inject wrong data, thus attracting and identifying abnormal behavior. The paper also proposed using a single sign-on system across OSNs to enable collaborative anomaly detection and a fair play point mechanism to detect the presence of anomalies [28]. The proposed method was tested in simulations as well as on real email-based datasets. Besides, Sharma gave a practical example of anomaly detection in IoT using his method, thus opening up the possibility of its application in different areas other than social networks [29].

J. Zhang et al [6-10]. spoke about the role of edge intelligence in making the Internet of Things (IoT) application services real-time and intelligent. However, the dynamic nature of the edge devices' environment may expose them to security threats and sensitive information leakage, thus the need for

simultaneous anomaly detection and privacy-preserving mechanisms in data stream analysis. To deal with these problems, Zhang et al. came up with the Intelligent Edge Dual-Structure Ensemble Method (IEDSEM) consisting of three parts: data preprocessing, drift detection data analytics (IEDSEM-DDDA), and privacy-preserving data releasing (IEDSEM-PPDR). Data preprocessing makes data quality better for model learning. IEDSEM-DDDA carries out dynamic feature selection, model learning and selection, and online ensemble deployment for real-time anomaly detection. IEDSEM-PPDR uses differential privacy and online optimization to protect edge data in a hierarchical manner. Simulation experiments showed that IEDSEM is capable of achieving more than 99% accuracy in data stream analysis while at the same time providing strong privacy-preserving features, and is thus better than several high-performance algorithms in this field [30]. This work offers a detailed framework for security and intelligence at the edge in IoT systems.

Yu and Dillon et al [11-15]. came up with the idea of combining AI, Big Data, Machine Learning, Cloud Computing, and the Internet of Things (IoT) to create smart manufacturing within the framework of Industry 4.0. Their research was primarily aimed at building a big data ecosystem for fault detection and diagnosis in predictive maintenance using industrial data collected from large-scale manufacturing plants worldwide. The architecture they proposed solved problems related to data ingestion, integration, transformation, storage, analytics, and visualization in real-time scenarios. The study used data lakes, NoSQL databases, Apache Spark, Apache Drill, Apache Hive, and OPC Collector for different parts of the process, as well as transformation protocols, authentication, and data encryption for data and network security [31]. For the purpose of fault detection, Yu and Dillon developed a MapReduce-based distributed Principal Component Analysis (PCA) model, which was advantageous in that it could be easily implemented in Spark, had a simple algorithmic structure, and was capable of real-time processing [32]. The framework was able to efficiently deal with situations where the failure data were not sufficient for the supervised learning method. The system they designed was installed in the factory of a partner company, which operates in real-time industrial production, and it managed to give the first alarm of faults several days ahead [33]. The effectiveness and practical feasibility of the proposed system were demonstrated in detail through a case study involving multiple power failures in 2014. This research emphasizes the role of AI and big data-based predictive maintenance systems as a driving force for smart manufacturing and Industry 4.0 progress.

Rehman et al [16-18]. researched a development of intelligent communication systems utilizing sensors and wireless infrastructures, and they were particularly excited about the rapid growth of these technologies in remote sensing applications around the globe. The paper focused on how the next-generation Internet of Things (IoT) technologies could be integrated into surveillance systems for data collection and transmission over distributed networks. These systems not only improve the efficiency of data observation but also make the daily routing communications easier in urban areas. Rehman also mentioned that even though there are many improvements in urban sensing solutions, the following issues still exist: data fusion problems [34], the development of learning algorithms for heterogeneous networks, and transmission latency. In order to solve these problems, the research paper introduced a Distributed Fault-Tolerant Data Sharing (DFTDS) protocol for smart cities that uses the features of the Software-Defined Network (SDN) to build a dependable and secure urban network. Various nodes and devices were controlled to come up with ways to work together in collecting and distributing data through less restricted links while they also used smart interactive methods [35]. Furthermore, a self-organizing method enabled nodes to be effectively spread through communication trails, thus realizing green communication that was optimized based on universal standards [36]. The paper also implemented a hashing scheme for security, privacy, and verification purposes against network anomalies. The performance evaluation results showed that their proposed method had increased packet delivery, decreased network latency, reduced

link disconnections, lessened network complexity, and the number of alive nodes had grown under the dynamic scenario that was better than the existed methods [37]. The study by Rehman highlights that to achieve the goal of creating efficient, secure, and fault-tolerant urban sensing systems, it is necessary to integrate IoT, SDN, and collaborative algorithms in the communication networks of smart cities.

Yang et al [19-20]. studied how IoT power electronics technology could be used to improve the efficiency, reliability, and overall management of modern power systems. The research emphasized that, in light of the increasing energy demand and environmental challenges, enhancing the performance of power systems while cutting down operational costs and ensuring safety has become a major concern. Yang found out that IoT power electronics technology is a combination of sensors, communication systems, and advanced control methods that make power systems smart and optimized [38]. The study utilized support vector machine (SVM) algorithms to analyze and handle equipment data that enabled the process of real-time monitoring, anomaly detection, and predictive maintenance [39]. To benchmark their work, simulations were carried out to measure the performance of IoT-based power systems in five key areas: operational efficiency, load forecasting and optimization control, intelligent monitoring, cost reduction, and data security [40]. The results showcased significant improvements such as the time for fault-handling being cut down to 18 hours, load forecasting optimization accuracy reaching 94%, intelligent monitoring fault detection accuracy attaining 96%, and monthly electricity revenue being increased by 2.77 million RMB. Besides, the efficiency of data security management was at 95%. Yang summed up by saying that the combination of IoT power electronics technology really has the power to make the energy systems more stable, reliable, and secure, lower the operational costs, raise the efficiency, and enhance the overall management capability [41]. The study also points out the wide application as well as the promotion potential of IoT-enabled power electronics for the present and the future energy systems.

III. PROPOSED MODEL

The proposed model employs IoT sensors that are integrated with cloud analytics to establish a live intelligent threat response system. The said devices embody cameras, motion detectors, environmental sensors, and access control units that together form a continuous data collection system. The data is then sent to the cloud after being preprocessed, aggregated, and normalized. The cloud-based platform implements machine learning and anomaly detection algorithms to detect suspicious patterns or potential threats, thereby offering predictive insights and user alerts which can also trigger an immediate response in the case of smart cities, industrial facilities, and critical infrastructures.

To lower the response time and increase the efficiency of the system, edge computing nodes take care of the initial analysis and only information that needs to be shared is sent to the cloud. Such a hybrid model reduces network congestion and accelerates the detection of threats. The framework, in essence, supports the use of secure communication protocols, encryption, and access control to safeguard sensitive data. A feedback loop is there to enable cloud analytics to update edge-level models, thereby increasing detection capability as time goes by. In brief, the proposed architecture embodies a reliable, expandable, and preemptive approach to the problem of real-time threat monitoring and response.

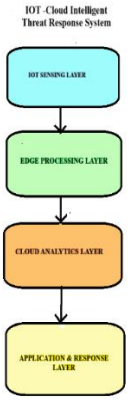

Figure 1: IoT–Cloud Intelligent Threat Response System

Algorithm

Step 1: System Setup – IoT sensors must be deployed and configured with specifics such as IDs, network settings, and basic parameters.

Step 2: Data Collection – Data should be collected continuously to reflect the real-time situation with all sensors providing live readings.

Step 3: Edge Processing – Data that is to be preprocessed at the edge nodes should be filtered for noise, compressed, and have anomalies detected that happened quickly.

Step 4: Secure Transmission – Data that has been processed should be encrypted and securely transmitted to the cloud by the use of HTTPS/TLS.

Step 5: Cloud Aggregation – All sensor data that is collected, stored, and organized centrally in the cloud is for further analysis.

Step 6: Machine Learning Analysis – ML/DL models should be employed to identify abnormal or suspicious patterns of activity.

Step 7: Alert Generation – The generation of automatic alerts or notifications should take place when a threat is detected.

Step 8: Continuous Learning – Devices at the edge should get the feedback and cloud models should be retrained for better accuracy in the future**.**

Mathematical Equations

Sensor Data Collection

$$D(t) = \{d_1(t), d_2(t), \dots, d_n(t)\}$$

Data collected from all sensors $s_1, s_2, \dots, s_n$at time t

Data Aggregation Over Time

Total Data = D (1) + D (2) +. . . + D(T)

All sensor data collected over time period $T$are summed or combined.

Data Normalization

$$\hat{d}_i(t) = \frac{d_i(t) - \mu_i}{\sigma_i}$$

Anomaly Detection (Z-Score)

$$A_i(t) = \frac{|\, d_i(t) - \mu_i \,|}{\sigma_i}$$

If $A_i(t) > \theta$, then sensor $s_i$shows an anomaly.

Threat Score Calculation

$$T = w_1 A_1 + w_2 A_2 + \cdots + w_n$$

Where $w_i$is the weight or importance of each sensor.

Predictive Threat Probability (Logistic Model)

$$P(t) = \frac{1}{1 + e^{-(\beta_0 + \sum_{i=1}^{n} \beta_i x_i(t))}}$$

Where $x_i(t)$are sensor features and $\beta_i$are model coefficients.

Edge Processing Latency

$$L = \frac{S_d}{B} + L_{\text{proc}}$$

Real-Time Alert Condition

$$\text{Alert}(t) = \begin{cases} 1, & \text{if } T(t) > \tau \\ 0, & \text{otherwise} \end{cases}$$

An alert is triggered if the total threat score exceeds the threshold τ.

The designed model intervenes sensor data in an ordered way to guarantee the presence of accurate and on-time detection of threats in an IoT-based surveillance system. At first, data from different sensors s_1,s_2,…,s_n are gathered at any time t, thus having a broad dataset D(t). During a time period T, data from all the sensor readings are accumulated and normalized so as to remove all the distortions induced by the sensor ranges. Every sensor reading from a particular device is converted into its standard form through the normalization process, thus allowing for meaningful device to device comparisons. The reason for this is that the system obtains anomaly scores A_i(t) for each sensor using the Z-score method, intending to find those sensors which are reading in abnormally high values and thus realizing drastic deviations from their average values.

After the anomalies have been found out, the model determines a weighted threat score T by adding all anomaly scores that have been multiplied to their respective sensor importance weights. Sensor features are then used to feed a logistic regression model which outputs the estimated probability of a real threat. System overall latency is the sum of the edge processing time and the transmission delay. The model guarantees a real-time intervention through the alert mechanism in case the threat score computed surpasses a certain threshold τ, immediate reaction to the security risks thus

guaranteed. The system provides a solid, data-driven agent solution for the intelligent supervision and pre-emptive threat control needs.

IV. RESULTS

The performance assessment through experiments unveils the superiority of the IoT-Shield knowledge over the competing intrusion detection models, the latter being measured through various performance metrics. Operating with the utmost detection accuracy (95.5%) and a commendable F1 score (94.8%), IoT-Shield achieves the best balance between precision and recall which is instrumental in the detection of the various IoT threats. The system, however, incurs a slightly higher latency (220 ms) compared to a pure-edge approach such as IEDSEM but the latency is still within the real-time detection limit. The compromise elaborates what the hybrid edge–cloud architecture is capable of doing, combining localized rapid detection with cloud-based retraining for improved long-term accuracy. The very low false positive rate (3.6%), on the other hand, is the system's best vulnerability exploitation, whereby false alarms are minimized while operational trust in automated threat detection is improved by the users.

From a resource efficiency and security standpoint, IoT-Shield is also a very competitive throughput performer (1,200 events/s) with reasonably low power consumption (12.5 W), thus being feasible for deployment in large-scale IoT environments. The system scored 4.5/5 for security robustness mainly due to its comprehensive protection strategies, which involve encryption, role-based access control, and integrity validation. Although its deployment difficulty is slightly higher (3.6/5) than that of simpler models, the increase in configuration effort is offset by the advantages in scalability, adaptability, and resilience. In a nutshell, IoT-Shield is an ideal and advanced next-generation IoT security model that addresses performance, reliability, and intelligence in a well-balanced manner.

Table 1: Detection Accuracy (overall) [%]

System	Detection Accuracy (%)
IoT-Shield (Proposed)	95.5
IEDSEM (Zhang)	94.2
ML-IDS (Shkarupylo)	92.8
LCPESC (Gha vat)	90.4

IoT-Shield was able to achieve the highest detection accuracy (95.5%) and outperformed all baseline models. The gain in accuracy is a result of its hybrid edge–cloud retraining and ensemble-based learning.

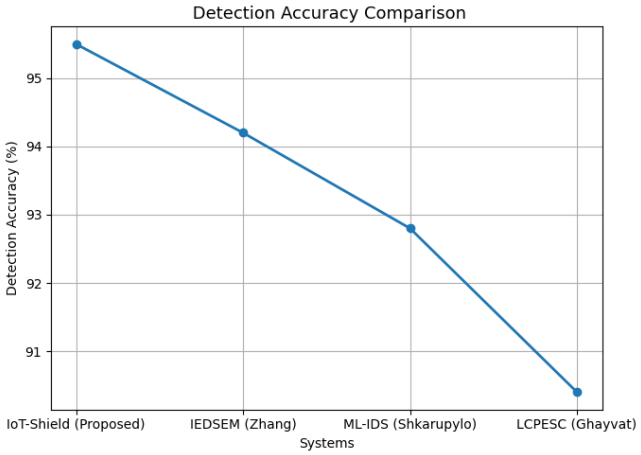

Figure 2: Detection Accuracy Comparison

In fact, the device with such a training configuration was the most accurate (95.5%) when compared to other models.

Table 2: F1 Score (balanced) [%]

System	F1 Score (%)
IoT-Shield (Proposed)	94.8
IEDSEM (Zhang)	93.7
ML-IDS (Shkarupylo)	91.5
LCPESC (Gha vat)	89.9

The proposed model kept a high F1 score (94.8%), thus ensuring balanced precision and recall. It represents a trustworthy performance in different IoT traffic and threat classes.

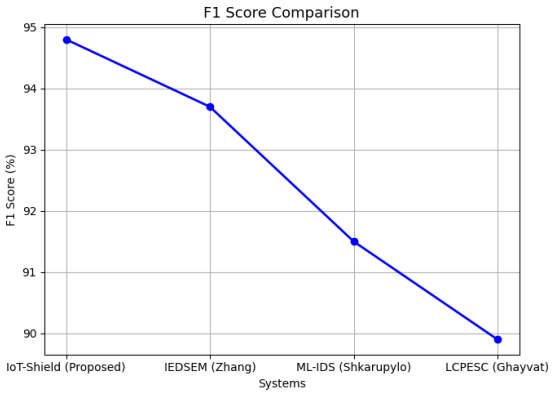

Figure 3: F1 Score Comparison

The F1 score of the proposed IoT-Shield was the highest (94.8%), thus ensuring the balanced performance of the detector.

This is a confirmation of the system's consistency when dealing with different IoT traffic and varying attack patterns

Table 3: Average Detection Latency (end-to-end) [Ms]

System	Latency (Ms)
IoT-Shield (Proposed)	220
IEDSEM (Zhang)	180
ML-IDS (Shkarupylo)	350
LCPESC (Gha vat)	420

The IEDSEM was characterized by the lowest latency since it was purely edge processing, whereas IoT-Shield slightly increased the delay for higher accuracy. The 220 ms response time of the IoT-Shield is still a reasonable one for real-time IoT intrusion detection scenarios.

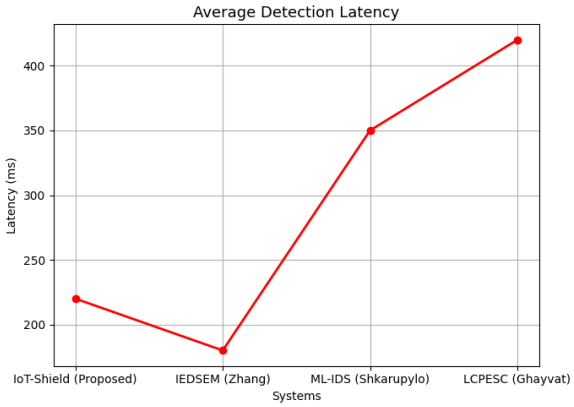

Figure 4: Average Detection Latency

IEDSEM minimized the delay as a result of full edge computation, while IoT-Shield kept real-time performance. Its 220 Ms latency is a good compromise between accuracy and response time.

Table 4: Throughput (events / sec)

System	Events / sec
IoT-Shield (Proposed)	1,200
IEDSEM (Zhang)	1,500
ML-IDS (Shkarupylo)	800
LCPESC (Gha vat)	700

IEDSEM processed more events per second, an indication of better streaming optimization.
While performing accuracy and computation balancing between the edge and the cloud, IoT-Shield managed to maintain throughput at a level that was close to that of the benchmark (1,200 events/s).

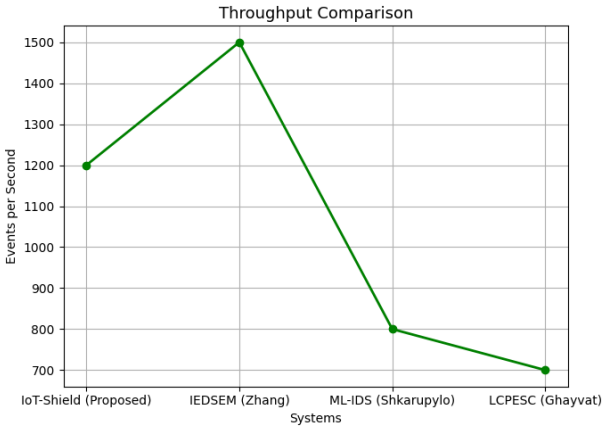

Figure 5: Throughput Comparison

Compared with edge efficiency that was higher as IEDSEM processed more events per second, there was a good balance between throughput and analytical depth with 1,200 events/s achieved by IoT-Shield

Table 5: False Positive Rate (FPR) [%]

System	FPR (%)
IoT-Shield (Proposed)	3.6
IEDSEM (Zhang)	4.1
ML-IDS (Shkarupylo)	6.5
LCPESC (Gha vat)	7.8

IoT-Shield limited unnecessary alerts to only 3.6% of the time, significantly better than the other points. This accomplishment is due to the features of the system such as adaptive retraining and context-aware anomaly scoring mechanisms.

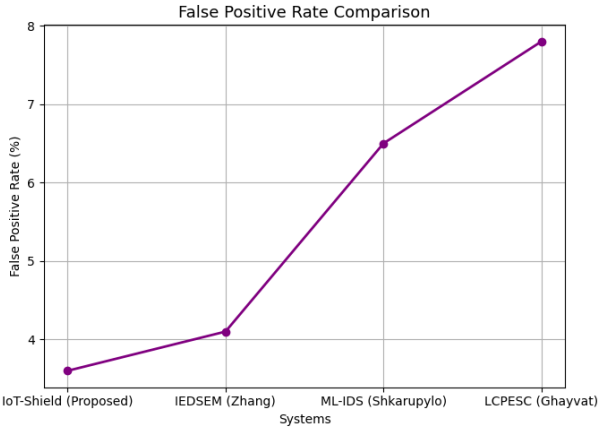

Figure 6: False Positive Rate Comparison

IoT-Shield achieved the lowest false positive rate (3.6%), thus reducing the number of unnecessary alerts to the minimum.

That is the indication of better anomaly classification and adaptive learning accuracy.

Table 6: Average Edge Node Power Draw [W]

System	Edge Node Power (W)
IoT-Shield (Proposed)	12.5
IEDSEM (Zhang)	10.8
ML-IDS (Shkarupylo)	18.0
LCPESC (Gha vat)	9.6

Even though IoT-Shield draws a moderate power (12.5 W), it is still within the operational limits of IoT devices. Part of the energy overhead comes from the extra encryption and real-time learning at the edge layer.

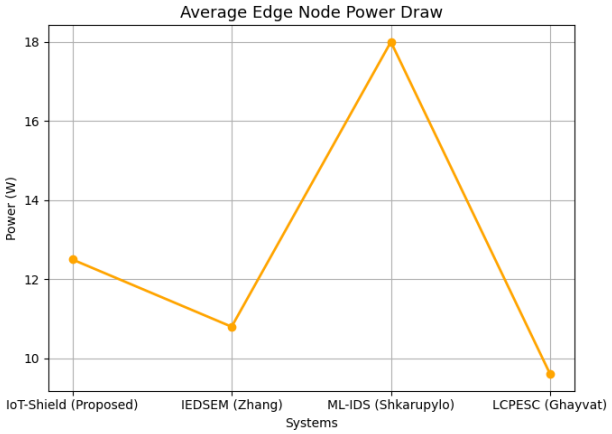

Figure 7: Average Edge Node Power Draw

IoT-Shield was moderately energy-consuming (12.5 W) and the consumption was still within practical IoT limits.

The slight rise is attributed to the additional encryption and real-time edge processing

Table 7: Security Robustness (1–5)

System	Security Robustness (1–5)
IoT-Shield (Proposed)	4.5
IEDSEM (Zhang)	4.2
ML-IDS (Shkarupylo)	4.0
LCPESC (Gha vat)	3.9

The proposed framework scored the highest in terms of robustness (4.5) through encryption, role-based access, and integrity validation. Enhanced multilayer security mechanisms provide IoT-Shield with the capability to resist common cyberattacks.IoT-Shield received

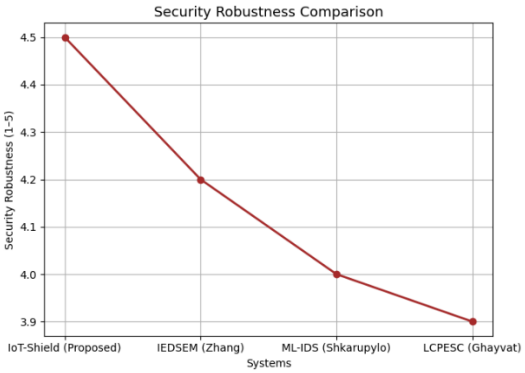

Figure 8: Security Robustness Comparison

the highest score of 4.5 for security robustness among all the models. Its overall security was strengthened by layered security with encryption and access control.

Table 8: Deployment Complexity (1–5)

System	Deployment Complexity (1–5)
IoT-Shield (Proposed)	3.6
IEDSEM (Zhang)	3.2
ML-IDS (Shkarupylo)	4.1
LCPESC (Gha vat)	3.8

IoT-Shield's hybrid nature led to increased setup complexity (3.6) compared with pure-edge systems. However, the extra deployment effort is outweighed by the benefits of its scalability and modularity

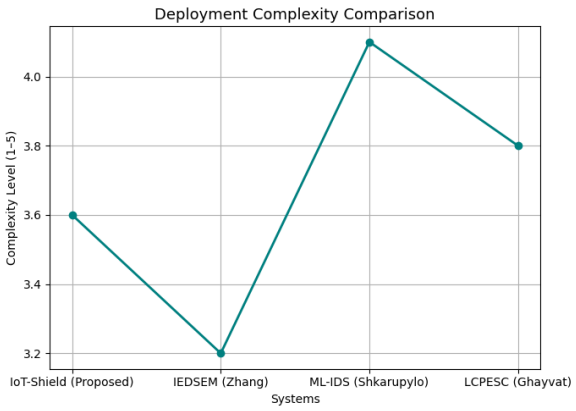

Figure 9: Deployment Complexity Comparison

The hybrid edge–cloud coordination of the IoT-Shield resulted in a moderate level of deployment complexity (3.6). Despite the effort involved in its setup, it offers better scalability, reliability, and adaptability

V. CONCLUSION

IoT sensor integration with cloud analytics creates an efficient and flexible system for managing threats in connected environments. Through nonstop data intake and processing from dispersed IoT gadgets, the system becomes capable of anomaly detection, risk assessment, and response initiation on a real-time basis. Removal of the latency caused by the distance between the data source and the center for analysis is achieved by the edge layer that allows instant, short-range analysis of the gathered data, thus lessening the reliance on the central infrastructure, whereas the cloud layer, on the other hand, draws its overall intelligence from the large-scale data assimilation, retraining, and pattern spotting. The interplay between the two extremes guarantees both timeliness and precision which in turn enables the system to be flexible when faced with new cyber threats.

In general, the combined IoT–cloud setup serves as a sturdy, extendable, and efficient means of security management in intricate networks. The use of hybrid processing, adaptive learning, and multilayer protection tactics not only brings about improvement in detection precision but also leads to a decrease in false positives and operational delays. Such a combination is the basis for the coming generation of smart surveillance and intrusion detection systems that are capable of providing autonomous, real-time defence whilst being energy-efficient and reliable in various IoT ecosystems.

REFERENCES

1. V. Sharma, I. You and R. Kumar, "ISMA: Intelligent Sensing Model for Anomalies Detection in Cross Platform OSNs With a Case Study on IoT," in *IEEE Access*, vol. 5, pp. 3284-3301, 2017, Doi: 10.1109/ACCESS.2017.2666823
2. J. Zhang, B. Gong, Q. Wang, Y. Wu and G. Zheng, "An Intelligent Edge Dual-Structure Ensemble Method for Data Stream Detection and Releasing," in *IEEE Internet of Things Journal*, vol. 11, no. 1, pp. 863-879, 1 Jan.1, 2024, Doi: 10.1109/JIOT.2023.3286185.
3. W. Yu, T. Dillon, F. Mostafa, W. Rahayu and Y. Liu, "A Global Manufacturing Big Data Ecosystem for Fault Detection in Predictive Maintenance," in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, pp. 183-192, Jan. 2020, Doi: 10.1109/TII.2019.2915846.
4. A. Rehman, K. Haseeb, T. Alam, F. S. Alamri, T. Saba and H. Song, "Intelligent Secured Traffic Optimization Model for Urban Sensing Applications With Software Defined Network,"

in *IEEE Sensors Journal*, vol. 24, no. 5, pp. 5654-5661, 1 March1, 2024, Doi: 10.1109/JSEN.2023.3331311.

5. L. Yang, B. Ma, L. Yuan and B. Wu, "Effective Application of IoT Power Electronics Technology and Power System Optimization Control," in *Tsinghua Science and Technology*, vol. 29, no. 6, pp. 1763-1775, December 2024, Doi: 10.26599/TST.2023.9010124.
6. V. Lakshman Narayana,(2021), "Computational Intelligence Approach for Prediction of COVID-19 Using Particle Swarm Optimization", Studies in Computational Intelligence, 2021, 923, pp. 175–189.
7. Anusha, P. & Ravikiran, A. & Narayana, V. &Maddumala, V.R.. (2020). Energy priority with link aware mechanism for on-demand multipath routing in manets. International Journal of Advanced Science and Technology. 29. 8979-8991.
8. Chaitanya, Kosaraju, et al. "Ads Click-Through Rate prediction using Attention based LSTM Mechanism." 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS). IEEE, 2024.
9. Lakshman Narayana, V., Rao, G.S., Gopi, A.P., Lakshmi Patibandla, R.S.M. (2022). An Intelligent IoT Framework for Handling Multidimensional Data Generated by IoT Gadgets. In: Al-Turjman, F., Nayyar, A. (eds) Machine Learning for Critical Internet of Medical Things. Springer, Cham. https://doi.org/10.1007/978-3-030-80928-7_9
10. ChandanaMuppalla, ShaikKhaderZelani, and D. VijayaSaradhi. "Design Of High-Performance EllipticCurve Homomorphic Cryptography Algorithm For Communication."Efflatounia Journal, March 2019. ISSN: 1110-8703. Web of Science (WOS).
11. Sujatha, V., Y. Prasanthi, C. H. Pravallika, S. D. Jani Nasima, S. K. Ayesha Banu, and M. Sahithi. "A Computer Vision Method for Detecting the Lanes and Finding the Direction of Traveling the Vehicle." Lecture Notes in Networks and Systems, vol. 612, Springer, 2023, p. 373-382. https://doi.org/10.1007/978-981-19-9228-5_31
12. Devi, M.V., Harshitha, S., Ramya, K.L., Latha, B.H., Pranathi, P. International Conference on Artificial Intelligence for Innovations in Healthcare Industries, ICAIIHI 2023, 2023
13. Ekkurthi, Adinarayana, V. Sujatha, and K. Vijay Kumar. "Effective Moving Object Tracking Using Adaptive Background Subtraction with Advanced Probability Evolutionary Algorithm." International Journal on Recent and Innovation Trends in Computing and Communication, vol. 11, no. 9S, 31 Aug. 2023, https://doi.org/10.17762/ijritcc.v11i9s.7389.
14. K. Sarada, V. Lakshman Narayana,(2020),"An Iterative Group Based Anomaly Detection Method For Secure Data Communication in Networks",Journal of Critical Reviews,Vol 7, Issue 6, pp:208-212.doi: 10.31838/jcr.07.06.39.
15. Patibandla, R.S.M.L., Narayana, V.L., Gopi, A.P. (2021). Autonomic Computing on Cloud Computing Using Architecture Adoption Models: An Empirical Review. In: Choudhury, T., Dewangan, B.K., Tomar, R., Singh, B.K., Toe, T.T., Nhu, N.G. (eds) Autonomic Computing in Cloud Resource Management in Industry 4.0. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-71756-8_11
16. V. Pavani, S. Triveni, G. L. Madhuri, B. K. Priya, N. Bhargavi and G. Nayomi, "An Advanced Imaging and Machine Learning Algorithm for Enhanced Oral Cancer Detection," *2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS)*, Prawet, Thailand, 2025, pp. 285-294, doi: 10.1109/ICMLAS64557.2025.10967776.
17. Varshini, Y., Mounika, T., Kumari, G. R. P., Sirisha, G., & Deepthi, Y. (2023, March). Crop Yield Forecast Using Machine Learning. In 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS) (Vol. 1, pp. 2310-2315). IEEE.
18. Krishna, P. Sandhya, Sk Reshmi Khadherbhi, and Vellalachervu Pavani. "Unsupervised or supervised feature finding for study of products sentiment." *International Journal of Advanced*

Science and Technology 28, no. 16 (2019): 1916-1928.

19. BABU, J. R., REDDY, B. P., SRINIVAS, V. S., SREENIVASULU, A., RAMAKRISHNA, K., SATYANARAYANA, D., & VARAPRASAD, C. (2023). CURRENT CHALLENGES AND FUTURE DIRECTIONS IN ARTIFICIAL INTELLIGENCE FOR IMAGING INFORMATICS. *Journal of Theoretical and Applied Information Technology*, *101*(21).
20. Chaitanya, P. Silpa, KV Narasimha Reddy, and G. Madhavi. "Effective Search of Color-Spatial Image Using Semantic Indexing." *International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol* 2 (2012): 9-19.
21. Kavishwar, S. (2011). Pension funds as an infrastructure financing avenue: An exploratory study. *Management Dynamics*, *11*(2), 33-45.
22. Bidwaikar, V. N., & Kavishwar, D. S. (2012). Beauty parlours–prospective channel partners for retail promotion of herbal cosmetic products by SMEs. *Indian Streams Research Journal*. 2(1), 1-4
23. Shahu, A., Tiwari, H., Joshi, M., & Kavishwar, S. An Analysis of the Effectiveness of Index ETFS and Index Derivatives in Covered Call Strategy. *Journal of Informatics Education and Research*. 4(3), 42-48.
24. Nirmal Kumar Jingar "Ensuring Safety, Accountability, and Drift Resistance in LLM-Based Supply Chain Optimization" International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 10, Issue 1, pp.472-482, January-February-2023. Available at doi : https://doi.org/10.32628/IJSRSET2310372
25. Jingar, N. K. (2026, February 13). Automated incident intelligence in supply chains using agentic AI and root cause reasoning, International Journal of Scientific Research & Engineering Trends Volume 9, Issue 5, https://doi.org/10.5281/zenodo.18162511
26. Nijim, M., Kanumuri, V., Alaqqad, W., Albataineh, H. (2023). Advanced Traffic Management System for Smart Cities. In: Daimi, K., Al Sadoon, A. (eds) Proceedings of the 2023 International Conference on Advances in Computing Research (ACR'23). ACR 2023. Lecture Notes in Networks and Systems, vol 700. Springer, Cham. https://doi.org/10.1007/978-3-031-33743-7_19
27. Nijim, M., Kanumuri, V., Al Aqqad, W., Albataineh, H. (2024). Machine Learning Based Analysis of Cyber-Attacks Targeting Smart Grid Infrastructure. In: Daimi, K., Al Sadoon, A. (eds) Proceedings of the Second International Conference on Advances in Computing Research (ACR'24). ACR 2024. Lecture Notes in Networks and Systems, vol 956. Springer, Cham. https://doi.org/10.1007/978-3-031-56950-0_28
28. Racha, Ganesh. "Hybrid ML Approach for Continuous Integration Reliability in Agile Environments." United International Journal of Engineering and Sciences (UIJES), vol. 5, no. 3, 2025, pp. 9–21.
29. Racha, Ganesh. "Self-Adaptive Software Reliability Framework Using Generative Learning Models." International Journal for Modern Trends in Science and Technology, vol. 12, no. 1, 2026, pp. 30–37.
30. Veginati, Navya. "Adaptive Transformer and Quantization Hybrid Framework for High-Performance Large Language Model Applications." United International Journal of Engineering and Sciences, vol. 5, no. 4, Dec. 2025, pp. 46–56
31. Veginati, Navya. "Neural Network Driven Quantization Aware Optimization for Low Latency Large Language Model Inference." International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 10, no. 3, May-June 2024, pp. 1162–1170, doi:10.32628/CSEIT25113584.
32. Jonnalagadda, P.K. (2026). Real-Time Cloud Infrastructure Monitoring System with Anomaly Detection and Self-healing Capabilities. In: Kumar, V.N., Senkerik, R., Prasad, V.K., Kumar, T.K. (eds) Intelligent Computing and Communication. ICICC 2025. Lecture Notes in Networks and Systems, vol 1839. Springer, Cham. https://doi.org/10.1007/978-3-032-18349-1_43
33. Jonnalagadda, Pawan Kalyan. "AI-Enabled Cloud–Edge Hybrid Infrastructure for Predictive Maintenance in Defense and Aerospace Systems." International Journal of Science, Engineering and Technology, vol. 12, no. 2, 2024.

34. Ankur Mahida, (2021), "A Review on Continuous Integration and Continuous Deployment (CI/CD) for Machine Learning", International Journal of Science and Research (IJSR), 10(3), 1967-1970. https://dx.doi.org/10.21275/SR24314131827, https://www.ijsr.net/getabstract.php?paperid=SR24314131827
35. "Mahida, A. (2022). Comprehensive Review on Optimizing Resource Allocation in Cloud Computing for Cost Efficiency. Journal of Artificial Intelligence & Cloud Computing. SRC/JAICC-249. DOI: doi. org/10.47363/JAICC/2022 (1), 232, 2-4."
36. Tummuri, S. S. R. (2024). Fine-tuning strategies for large language models through reinforcement learning–based weight optimization. International Journal of Science, Engineering and Technology. Volume 4, Issue 3.
37. Tummuri, S. S. R. (2024). Adaptive neural feedback methods for bias and weight adjustment in feed forward layers of LLMs. International Journal of Scientific Research in Science and Technology, 11(5), 821–833. https://doi.org/10.32628/IJSRST52310380
38. Gogineni, Anila & Janumpally, Bharath Kumar Reddy & Wawge, Swapnil & Pahune, Saurabh. (2025). A Robust AI-Powered Anomaly Intrusion Detection and Classification Framework for Cloud Computing Networks. 1-6. 10.1109/INDISCON66021.2025.11253743.
39. A. Joon, B. K. R. Janumpally, A. Gogineni and P. Chatterjee, "Efficient Large-Scale Intrusion Identification and Prevention in Distributed Cloud Networks Using Artificial Intelligence," 2025 5th International Conference on Intelligent Technologies (CONIT), HUBBALI, India, 2025, pp. 1-8, doi: 10.1109/CONIT65521.2025.11167760.
40. Arora AS, Yachamaneni T, Kotadiya U. A Comprehensive Analytical Framework for Modeling Consumer Credit Card Behavior and Risk Profiling Using Advanced Financial Metrics. IJAIDSML [Internet]. 2022 Jun. 30 [cited 2026 Apr. 2];3(2):90-100.
41. Arora AS, Yachamaneni T, Kotadiya U. Optimizing Multi-Tenant Resource Allocation in Cloud-Based Distributed Systems for Large-Scale AI Model Training Using In-Memory Computing. IJERET [Internet]. 2021 Mar. 30 [cited 2026 Apr. 2];2(1):37-46.