Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Internet of Things with Smart Trends and Intelligent Devices for Future Generation

Godfrey Perfectson Oise

godfrey.oise@physci.uniben.edu

University of Benin

Oludare Sokoya

National University

Konyeah susan

University of Benin

Osahon Ukpebor

University of the Cumberlands

Tejiri Jessa

Westcliff University

Evans Mintah

Westcliff University

Research Article

Keywords: Internet of Things, Smart Devices, Edge Computing, Machine Learning, Wearables, Robotics, Intelligent Systems

Posted Date: May 8th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-9305347/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Abstract

This study introduces an Intelligent IoT Continuum Framework (IICF) designed to support smart trends and intelligent devices in future-generation Internet of Things environments. The framework integrates device, edge, fog, and cloud layers to enable distributed intelligence, real-time analytics, scalability, and energy-efficient operation across heterogeneous IoT ecosystems. It addresses key limitations of conventional centralized IoT architectures, such as high latency, poor interoperability, and inefficient resource utilization, by embedding artificial intelligence directly into the processing continuum. Data streams from sensors, wearables, robotics platforms, and UAV systems are preprocessed using Z-score normalization, noise reduction, and Principal Component Analysis (PCA) to ensure quality, consistency, and reduced dimensionality for efficient learning. Deep learning models, including Deep Neural Networks (DNN) and Long Short-Term Memory (LSTM), are deployed across the continuum to capture spatial and temporal patterns required for intelligent decision-making. The framework is validated using the ToN-IoT Dataset, which provides realistic labeled traffic from smart IoT and IIoT environments. Experimental evaluation demonstrates stable learning behavior with approximately 96–97% classification accuracy, low validation loss, and strong generalization. The confusion matrix shows high true positive rates across multiple traffic categories, while feature importance analysis highlights the dominance of network flow, endpoint behavior, and traffic statistics in model decisions. The proposed IICF demonstrates how edge–cloud intelligence can enhance responsiveness, scalability, and efficiency in applications such as healthcare monitoring, smart cities, industrial automation, and autonomous systems, providing a practical foundation for intelligent IoT infrastructures.

1. Introduction

The Internet of Things (IoT) has emerged as a key enabler of next-generation intelligent systems, facilitating seamless interaction between physical devices, communication networks, and computational infrastructures. By embedding sensing, processing, and communication capabilities into everyday objects, IoT systems support real-time monitoring, automation, and data-driven decision-making across diverse application domains, including smart healthcare, industrial automation, intelligent transportation, and smart cities [1]. The rapid advancement of complementary technologies, such as artificial intelligence (AI), edge computing, and next-generation communication networks, has further accelerated the evolution of IoT toward highly distributed, adaptive, and autonomous ecosystems [2]. Despite these advancements, conventional IoT architectures remain predominantly reliant on centralized cloud computing models, which introduce significant limitations in terms of latency, bandwidth utilization, scalability, and energy efficiency [3]. The continuous transmission of large volumes of heterogeneous and time-sensitive data from distributed IoT devices to centralized cloud servers leads to increased network congestion and delayed response times. Such limitations are particularly critical in mission-sensitive applications, where real-time decision-making is essential. Furthermore, the growing heterogeneity of IoT devices and communication protocols introduces interoperability challenges, while resource constraints in edge devices restrict their ability to perform complex computations locally [4].Recent research efforts have focused on mitigating these challenges through the integration of edge

computing and AI-driven analytics. Edge computing enables localized data processing closer to the source, thereby reducing latency and bandwidth consumption while improving responsiveness [5]. Concurrently, machine learning and deep learning techniques have demonstrated strong capabilities in extracting meaningful insights from complex IoT data, supporting applications such as anomaly detection, predictive maintenance, and intelligent control [6]. However, existing solutions often adopt isolated approaches that either emphasize edge intelligence or cloud-based analytics, lacking a unified framework that effectively coordinates computation across all layers of the IoT ecosystem [7]. In addition, many current frameworks do not adequately address issues related to data heterogeneity, scalability, and efficient resource allocation in dynamic environments.

To address these limitations, this study proposes an Intelligent IoT Continuum Framework (IICF) that integrates device, edge, fog, and cloud layers into a cohesive and hierarchical architecture. The proposed framework is designed to support distributed intelligence by enabling task allocation based on latency sensitivity, computational requirements, and resource availability [8]. Data acquired from diverse IoT sources, including sensors, wearable devices, robotics systems, and unmanned aerial vehicles, are preprocessed using normalization, noise reduction, and dimensionality reduction techniques to ensure data quality and computational efficiency. Specifically, Z-score normalization standardizes feature distributions, while Principal Component Analysis (PCA) reduces data dimensionality by retaining the most informative features [9]. To enable intelligent decision-making, the framework incorporates deep learning models, including Deep Neural Networks (DNN) and Long Short-Term Memory (LSTM) networks. These models are deployed across the IoT continuum to capture both spatial and temporal dependencies in the data, allowing the system to perform accurate classification and predictive analytics in real time. The integration of edge and cloud intelligence ensures a balance between low-latency processing and high-performance computation, thereby enhancing system scalability and adaptability.

The effectiveness of the proposed framework is evaluated using the ToN-IoT dataset, which provides a realistic representation of IoT and Industrial IoT (IIoT) environments with labeled benign and malicious network traffic. Experimental results demonstrate that the framework achieves high classification accuracy, strong generalization capability, and reduced latency compared to conventional cloud-centric approaches. The findings further indicate that the distributed architecture improves resource utilization and supports efficient handling of large-scale IoT data streams [10]. This study presents a novel IoT continuum-based framework that addresses key challenges associated with traditional architectures by integrating distributed intelligence, advanced data preprocessing, and deep learning techniques within a unified system. The proposed approach demonstrates significant improvements in accuracy, latency reduction, scalability, and energy efficiency, making it suitable for real-world IoT applications [11]. Additionally, the framework provides a flexible foundation for future research in intelligent IoT systems, with potential extensions involving federated learning, secure data sharing mechanisms, and energy-aware AI models to further enhance system performance and sustainability.

2. Related Work

The rapid evolution of the Internet of Things (IoT) has stimulated extensive research aimed at improving system intelligence, scalability, and efficiency through the integration of advanced computational paradigms. In particular, the convergence of artificial intelligence (AI), edge computing, and distributed architectures has become a focal point in addressing the limitations of traditional IoT systems [12]. This section reviews relevant literature across four key dimensions: (i) AI-driven IoT analytics, (ii) edge and fog computing in IoT, (iii) intelligent IoT applications, and (iv) existing architectural limitations and research gaps. Machine learning and deep learning techniques have been widely adopted in IoT systems to enable intelligent data analysis and decision-making [13]. Traditional machine learning algorithms, such as Random Forest (RF), Support Vector Machines (SVM), and k-Nearest Neighbors (k-NN), have demonstrated effectiveness in tasks including classification, anomaly detection, and predictive modeling within IoT environments. These methods are particularly useful for structured data and relatively low-dimensional feature spaces; however, they often struggle to capture complex nonlinear relationships and temporal dependencies inherent in large-scale IoT data streams [14].

To overcome these limitations, deep learning approaches such as Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), and Long Short-Term Memory (LSTM) networks have been increasingly employed. DNN models enable hierarchical feature extraction [15], improving classification accuracy in complex datasets, while LSTM networks are well-suited for modeling sequential and time-dependent data, making them highly applicable to dynamic IoT scenarios such as network traffic analysis and predictive maintenance [16]. Despite their superior performance, these models are typically computationally intensive and are often deployed in centralized cloud environments, which introduces latency and limits real-time responsiveness.

Edge computing has emerged as a promising paradigm to address the latency and bandwidth challenges associated with cloud-centric IoT architectures. By processing data closer to the source, edge computing reduces the need for continuous data transmission to centralized servers, thereby improving response time and reducing network congestion [17]. Fog computing further extends this concept by introducing an intermediate layer that facilitates data aggregation, preprocessing, and coordination between edge devices and cloud systems [18]. Several studies have demonstrated the effectiveness of edge–fog architectures in supporting real-time IoT applications [19]. These approaches enable localized analytics and faster decision-making, which are essential in latency-sensitive domains such as healthcare monitoring, autonomous vehicles, and industrial automation. However, edge and fog nodes are typically resource-constrained, limiting their ability to support complex deep learning models. Additionally, many existing solutions focus primarily on infrastructure-level improvements without fully integrating intelligent learning mechanisms across all layers of the IoT ecosystem.

The integration of AI and IoT has enabled the development of intelligent applications across various domains. In healthcare, wearable devices and Body Area Networks (BANs) support continuous monitoring of physiological signals, enabling early detection of health anomalies. In industrial IoT (IIoT), intelligent systems facilitate predictive maintenance, fault detection, and process optimization, improving operational efficiency and reducing downtime. Similarly, IoT-enabled robotics and unmanned

aerial vehicles (UAVs) are increasingly used in applications such as precision agriculture, environmental monitoring, and disaster management. While these applications demonstrate the potential of intelligent IoT systems, they often rely on domain-specific solutions that lack generalizability and scalability [20]. Moreover, many implementations do not adequately address challenges related to data heterogeneity, interoperability, and secure communication [21]. The absence of unified frameworks capable of supporting diverse IoT applications limits the broader adoption of intelligent IoT technologies.

Despite significant advancements, existing IoT frameworks exhibit several critical limitations. First, many approaches remain heavily dependent on centralized cloud infrastructures, resulting in increased latency and reduced system responsiveness. Second, there is a lack of integrated architectures that seamlessly combine device-level data acquisition, edge intelligence, fog-based coordination, and cloud-scale analytics within a unified framework. Third, current systems often struggle to efficiently process heterogeneous and high-dimensional IoT data, leading to suboptimal performance in real-world environments. Furthermore, the deployment of deep learning models in IoT systems is frequently constrained by computational limitations at the edge, as well as the absence of efficient data preprocessing and feature selection mechanisms. Energy efficiency remains another major concern, particularly for battery-powered IoT devices that require continuous operation. In addition, issues related to scalability, interoperability, and data security are not comprehensively addressed in many existing studies. In light of these challenges, there is a clear need for a holistic IoT framework that integrates distributed intelligence, advanced data preprocessing, and scalable deep learning models across multiple layers of the IoT architecture. The proposed Intelligent IoT Continuum Framework (IICF) addresses these gaps by providing a unified, multi-layered approach that enables efficient data processing, real-time analytics, and intelligent decision-making while ensuring scalability and energy efficiency.

3. Methodology

This section details the methodology employed for the design, implementation, and evaluation of the proposed Intelligent IoT Continuum Framework (IICF**)**. The framework combines a hierarchical, multi-layer IoT architecture with robust data preprocessing and deep learning techniques to enable efficient processing, analysis, and accurate classification of IoT network traffic in distributed environments. The methodology encompasses dataset acquisition, preprocessing, model training, evaluation, and implementation within a scalable IoT continuum.

3.1 Dataset Description and Acquisition

The proposed framework is evaluated using the ToN-IoT dataset[22], a comprehensive and publicly available dataset developed by the Cyber Range Laboratory at UNSW Canberra. This dataset provides a realistic representation of IoT and Industrial IoT (IIoT) network environments, making it particularly suitable for the development and evaluation of machine learning and deep learning models for intrusion and anomaly detection. The ToN-IoT dataset includes network traffic collected from simulated smart

home and industrial environments, integrating multiple IoT devices, sensors, and communication systems. The simulation is designed to reflect real-world IoT deployments, incorporating heterogeneous devices, dynamic interactions, and complex network behaviors. Network traffic data were collected using widely adopted monitoring tools, including Argus and Bro (Zeek), which capture detailed attributes such as packet size, protocol type, connection duration, and flow statistics. A notable characteristic of the dataset is the inclusion of both benign and malicious traffic. Benign instances represent normal device communication patterns, while malicious instances encompass various cyberattacks, including denial-of-service (DoS), distributed denial-of-service (DDoS), backdoor, injection, man-in-the-middle (MITM), password attacks, ransomware, scanning, and cross-site scripting (XSS). Each instance is labeled, enabling effective use in supervised learning tasks. For this study, the “train_test_network.csv” file is employed, containing structured tabular data suitable for training and evaluating predictive models.

3.2 Data Preprocessing

To ensure data quality, reliability, and computational efficiency, a series of preprocessing steps were applied prior to model training. Data Cleaning: Missing values, inconsistencies, and anomalies were identified and handled to ensure the dataset provides reliable inputs for the learning model. Feature Normalization: To standardize feature distributions and ensure all features contribute equally during model training, Z-score normalization was applied. Noise Reduction: Noise and irrelevant variations in the dataset were minimized to improve model robustness and allow the model to focus on informative patterns. Dimensionality Reduction: Principal Component Analysis (PCA) was employed to reduce dataset dimensionality while retaining the most informative features. This step improves computational efficiency, reduces feature redundancy, and enhances the model’s generalization capability.

3.3 Model Training and Evaluation

The core predictive model in the proposed framework is a Deep Neural Network (DNN), trained using a supervised learning approach. The preprocessed dataset is divided into training and validation sets to monitor learning performance. Training is conducted over multiple epochs, and model performance is evaluated using standard classification metrics, including accuracy, precision, recall, and F1-score. Additionally, a confusion matrix is used to assess class-wise performance, allowing for the evaluation of the model’s ability to accurately classify both benign and malicious traffic types.

Experimental results demonstrate strong diagonal dominance in the confusion matrix, indicating high classification accuracy across multiple traffic categories. The model achieves an overall accuracy of approximately 96–97%, with stable learning behavior and strong generalization capability across unseen data. The proposed framework is implemented in Python, leveraging TensorFlow/Keras for model development. The implementation integrates data preprocessing, model training, and evaluation into a unified pipeline that supports distributed processing across the IoT continuum. Specifically:

1. Edge layer: Responsible for real-time preprocessing of incoming network traffic.
2. Fog layer: Handles intermediate coordination, aggregation, and lightweight analytics.
3. Cloud layer: Performs intensive model training, storage, and advanced analytics.

This layered implementation ensures scalability, efficient resource utilization, and adaptability to diverse IoT environments, allowing the framework to support both real-time and batch processing scenarios. The proposed methodology integrates a multi-layer IoT continuum architecture with robust data preprocessing, a DNN-based classification model, and feature importance analysis. By combining distributed processing across edge, fog, and cloud layers with optimized learning techniques, the framework achieves high classification accuracy, reduced latency, and improved scalability. These characteristics make the IICF suitable for real-world IoT applications where efficient and reliable intrusion detection and network traffic classification are critical.

3.4 Framework Architecture Description

The proposed Intelligent IoT Continuum Framework (IICF) **is** structured as a hierarchical, multi-layer architecture designed to support distributed intelligence and efficient data processing across IoT environments. The framework consists of five interconnected layers: device, edge, fog, cloud, and application layers, each performing specific functions within the data processing pipeline. At the device layer, heterogeneous IoT entities including sensors, wearable devices, robotics systems, and unmanned aerial vehicles (UAVs) continuously generate raw data streams. These data represent environmental conditions, system states, and network traffic characteristics. The generated data are transmitted to the edge layer, where initial processing is performed. This includes data filtering, normalization, and noise reduction. By handling preprocessing tasks at the edge, the framework reduces latency and minimizes bandwidth consumption, enabling near real-time responsiveness. The fog layer acts as an intermediate processing and coordination layer. It aggregates data from multiple edge nodes, performs intermediate analysis, and manages communication between edge and cloud layers. This layer improves scalability and reduces the computational burden on the cloud. At the cloud layer, computationally intensive operations are carried out. These include deep learning model training using the Deep Neural Network (DNN), large-scale data analytics, and long-term storage. The cloud layer leverages high-performance computing resources to ensure accurate and efficient model development. The application layer represents the interface through which processed data and intelligent insights are delivered to end users. This layer supports various IoT applications such as intrusion detection, smart healthcare, industrial monitoring, and intelligent automation.

Data flows sequentially from the device layer to the cloud layer, while control signals and insights flow back toward the lower layers, enabling adaptive and intelligent system behavior. The integration of preprocessing techniques (Z-score normalization, noise reduction, PCA) and the DNN model within this architecture ensures efficient handling of large-scale, heterogeneous IoT data. The IICF architecture enables low-latency processing, scalability, efficient resource utilization, and accurate multi-class classification, making it suitable for real-world IoT deployments. The dataset is provided in a structured tabular format, with multiple features describing network flow characteristics. In this study, the “train_test_network.csv” file is used, which contains a subset of relevant features selected for model training and evaluation. Prior to model development, data preprocessing techniques are applied to handle missing values, normalize feature distributions, and reduce dimensionality using Principal

Component Analysis (PCA). These steps ensure improved model performance and computational efficiency.

Another advantage of the TON_IoT dataset is its high usability and accessibility. It is distributed under the Creative Commons Attribution 4.0 International (CC BY 4.0) license, allowing researchers to freely use, modify, and distribute the dataset with proper attribution. This makes it a widely accepted benchmark dataset for evaluating IoT-based intrusion detection systems and intelligent frameworks. The TON_IoT dataset provides a reliable and realistic foundation for developing and validating the proposed Intelligent IoT Continuum Framework (IICF). Its combination of heterogeneous IoT data, labeled attack scenarios, and real-world simulation characteristics makes it highly suitable for assessing the performance, scalability, and robustness of intelligent IoT systems.

Figure 1 illustrates an Intelligent IoT Continuum Framework (IICF) organized into five layers that transform raw data into intelligent actions. At the bottom, the Device Layer consists of sensors, wearables, robots, UAVs, and smart devices that generate raw data such as network traffic, environmental data, and system signals. This data moves to the Edge Layer, where it is preprocessed through filtering, normalization, noise reduction, dimensionality reduction, and real-time processing. The refined data is then sent to the Fog Layer, which performs data aggregation, traffic analysis, and resource coordination. Next, the Cloud Layer handles advanced tasks like deep learning, model training, big data analytics, and long-term storage. Finally, the Application Layer uses these insights to support real-world applications such as smart healthcare, smart cities, industrial IoT, and autonomous systems. The framework shows a continuous flow from raw data to insights and back as intelligent feedback and adaptive responses.

4. Results

Figure 2 illustrates the architecture of the proposed deep learning model, which consists of multiple fully connected (dense) layers with progressive dimensionality reduction. The input features are first processed by a dense layer with 256 neurons, followed by a dropout layer for regularization. The network then transitions through additional dense layers of 128 and 64 neurons, each accompanied by dropout to prevent overfitting. Finally, the output layer contains 16 neurons corresponding to the target classes. This hierarchical structure enables efficient feature extraction and classification, while the inclusion of dropout layers enhances model generalization and robustness.

Table 1: Classification Report

Classification Report:

	precision	recall	f1-score	support
backdoor	1.00	1.00	1.00	4000
ddos	0.97	0.96	0.97	4000
dos	0.96	0.98	0.97	4000
injection	0.94	0.90	0.92	4000
mitm	0.82	0.73	0.77	209
normal	1.00	1.00	1.00	10000
password	0.92	0.96	0.94	4000
ransomware	0.99	1.00	1.00	4000
scanning	0.96	0.97	0.96	4000
xss	0.99	0.99	0.99	4000
accuracy			0.97	42209
macro avg	0.96	0.95	0.95	42209
weighted avg	0.97	0.97	0.97	42209

Table 1 summarizes the classification performance of the proposed model across different IoT traffic classes using precision, recall, F1-score, and support metrics. The results indicate excellent performance for most classes, with backdoor, normal, and ransomware achieving perfect scores (1.00), reflecting accurate and reliable classification. Similarly, DDoS, DoS, scanning, and XSS exhibit very high performance, with F1-scores ranging from 0.96 to 0.99, demonstrating strong detection capability with minimal errors. The password and injection classes show slightly lower performance, with F1-scores of 0.94 and 0.92 respectively, suggesting minor confusion with similar attack patterns. The MITM class records the lowest performance (F1-score of 0.77), likely due to its subtle characteristics and limited sample size. Overall, the model achieves an accuracy of 97%, with a macro average F1-score of 0.95 and a weighted average of 0.97, confirming robust and reliable performance across both balanced and imbalanced class distributions.

Figure 1 shows a steady increase in both training and validation accuracy over the epochs. The model rapidly improves in the early stages and gradually stabilizes, with validation accuracy slightly higher than training accuracy throughout. The close alignment between the curves indicates good generalization with no significant overfitting, achieving high final accuracy of approximately 96–97%.

Figure 2 shows a consistent decrease in both training and validation loss over the epochs. The loss drops sharply during the initial epochs, indicating rapid learning, and then gradually declines as the model converges. The validation loss closely follows the training loss with only minor fluctuations, suggesting stable learning and good generalization. By the final epoch, both losses reach low values, confirming effective model optimization without significant overfitting.

Figure 1 presents the confusion matrix illustrating the classification performance of the intrusion detection model across ten traffic categories: backdoor, DDoS, DoS, injection, MITM, normal, password, ransomware, scanning, and XSS. The strong concentration of values along the diagonal indicates a high

rate of correct predictions for nearly all classes, demonstrating the model's strong discriminative capability. Normal traffic is identified with near-perfect accuracy, showing the model's effectiveness in minimizing false alarms. High detection accuracy is also observed for ransomware, backdoor, DoS, DDoS, password, scanning, and XSS attacks. Minor misclassifications occur between behaviorally similar attacks, particularly DoS and DDoS, injection and password attacks, and scanning with password and XSS, due to overlapping traffic characteristics. MITM records comparatively lower correct predictions, likely due to its subtle network behavior and fewer samples.

Figure 2 presents the relative importance of the top twenty network features identified by a Random Forest model trained on the ToN-IoT dataset. The ranking reveals that source-related attributes, particularly src_ip and src_ip_bytes, have the greatest influence on the model's decisions, highlighting the significance of traffic origin and data volume in distinguishing attack behavior. Key transport and session features such as src_port, conn_state, dst_port, and dst_ip also contribute substantially, emphasizing the role of endpoint communication patterns in intrusion detection. Traffic statistics including packet counts, byte counts, and connection duration further enhance classification performance. In contrast, DNS-specific features and service identifiers exhibit relatively low importance, indicating limited contribution to the detection process.

5. Discussion

The experimental evaluation of the proposed Intelligent IoT Continuum Framework (IICF) demonstrates its effectiveness in addressing key challenges associated with modern IoT systems, particularly in terms of classification accuracy, latency reduction, scalability, and intelligent data processing. Using the ToN-IoT dataset, the Deep Neural Network (DNN) model achieved an overall classification accuracy of approximately 96–97%, indicating a high level of reliability in distinguishing between benign and malicious network traffic. This high accuracy is complemented by strong precision, recall, and F1-score values, which collectively confirm that the model maintains a balanced performance with minimal false positives and false negatives. Such performance is critical in real-world IoT deployments, where both missed detections and false alarms can have significant operational consequences. The training process reveals stable and efficient learning behavior. The training and validation accuracy curves show a consistent upward trend, with rapid improvements during the initial epochs followed by gradual convergence. Notably, the validation accuracy remains closely aligned with, and in some cases slightly higher than, the training accuracy. This pattern suggests that the model generalizes well to unseen data and does not suffer from overfitting. The corresponding loss curves further reinforce this observation, as both training and validation loss decrease steadily and converge to low values with minimal divergence. This indicates that the optimization process is well-controlled and that the combination of preprocessing techniques and dropout regularization effectively enhances model robustness.

A deeper examination of the confusion matrix provides insight into class-level performance. The matrix is characterized by strong diagonal dominance, indicating that the majority of instances are correctly classified across all traffic categories. Normal traffic is identified with near-perfect accuracy, which is

particularly important for minimizing false alarms in practical systems. Similarly, high detection rates are observed for several attack classes, including denial-of-service (DoS), distributed denial-of-service (DDoS), ransomware [23], backdoor, scanning, and cross-site scripting (XSS). However, some degree of misclassification is observed among attacks with similar behavioral patterns. For instance, DoS and DDoS attacks exhibit overlapping traffic characteristics, leading to occasional confusion between these classes. Likewise, injection and password attacks, as well as scanning and XSS, show minor classification overlaps due to similarities in their communication patterns. Man-in-the-middle (MITM) attacks demonstrate comparatively lower detection accuracy, which can be attributed to their subtle network signatures and relatively limited representation in the dataset. Despite these minor limitations, the overall classification performance remains highly reliable.

The feature importance analysis further enhances the interpretability of the model by identifying the most influential attributes in the classification process. The results indicate that network flow features, such as source IP behavior, byte transmission volume, port interactions, and connection states, play a dominant role in distinguishing between normal and malicious traffic. These features capture the underlying communication patterns and behavioral characteristics of IoT devices, making them highly informative for intrusion detection tasks [24]. In contrast, application-layer and DNS-related features contribute less significantly to the model's decision-making process. This finding suggests that effective intrusion detection in IoT environments relies more on traffic dynamics and endpoint interactions than on protocol-specific details. Beyond classification performance, the results also highlight the advantages of the proposed multi-layer architecture. By distributing computation across device, edge, fog, and cloud layers, the framework significantly improves system efficiency. The edge layer performs initial preprocessing tasks such as normalization and noise reduction, which reduces the volume of data transmitted to higher layers and enables faster response times[25]. The fog layer provides intermediate aggregation and coordination, further optimizing resource utilization and reducing computational bottlenecks. The cloud layer handles computationally intensive tasks such as model training and large-scale analytics, leveraging high-performance resources to ensure accuracy and scalability[26]. This hierarchical processing approach leads to reduced latency, lower bandwidth consumption, and improved overall system responsiveness compared to traditional cloud-centric architectures.

The integration of edge computing with deep learning plays a crucial role in enabling real-time decision-making within the proposed framework. By processing data closer to the source, the system can respond quickly to time-sensitive events, making it suitable for applications such as healthcare monitoring, industrial automation, and autonomous systems [27]. Additionally, the use of dimensionality reduction techniques such as Principal Component Analysis (PCA) enhances computational efficiency by eliminating redundant features while preserving essential information. This not only accelerates the training process but also reduces the computational burden on resource-constrained devices [28]. From a broader perspective, the results demonstrate that the IICF successfully balances the trade-offs between accuracy, efficiency, and scalability in IoT systems. The framework leverages distributed intelligence to overcome the limitations of centralized architectures, enabling efficient handling of large-scale, heterogeneous data streams [29]. However, the observed misclassifications among certain attack

categories highlight the need for further improvements, particularly in handling imbalanced datasets and capturing subtle attack patterns. Future enhancements could involve the integration of advanced techniques such as ensemble learning, attention mechanisms, or federated learning to further improve detection performance and system adaptability [30]. The results confirm that the proposed Intelligent IoT Continuum Framework provides a robust and scalable solution for intelligent IoT environments. Its ability to achieve high classification accuracy, maintain stable learning behavior, and optimize system performance across multiple layers underscores its potential for deployment in real-world applications. The combination of distributed architecture, advanced preprocessing, and deep learning-based analytics positions the framework as a significant advancement in the development of next-generation IoT systems.

Conclusion

This study introduced an Intelligent IoT Continuum Framework (IICF) that addresses the limitations of traditional cloud-centric IoT systems by integrating distributed intelligence across device, edge, fog, and cloud layers. The framework incorporates data preprocessing techniques such as Z-score normalization and Principal Component Analysis (PCA) alongside a Deep Neural Network (DNN) to enable efficient and accurate classification of IoT network traffic. Evaluation using the ToN-IoT dataset under realistic conditions demonstrates the framework's effectiveness in handling heterogeneous IoT environments. The results show that the model achieves high classification accuracy of approximately 96–97%, supported by strong precision, recall, and F1-score metrics. The training process exhibits stable convergence with minimal overfitting, indicating strong generalization capability. Confusion matrix analysis further confirms high detection rates across multiple attack categories, with only minor misclassifications among similar traffic patterns. In addition to predictive performance, the framework improves system efficiency by reducing latency through edge processing, lowering bandwidth usage, and enhancing scalability via distributed computation. It also supports energy-efficient operation, making it suitable for resource-constrained environments. The IICF provides a scalable and reliable solution for intelligent IoT systems and lays a solid foundation for future advancements in adaptive and efficient IoT infrastructures.

Declarations

Funding: no funding was received

Competing Interests: There is no competing of interest

Ethics: Not applicable.

Consent to Participate: Not applicable.

Consent to Publish declarations: Not applicable.

Availability of data: The data use is available at: https://www.kaggle.com/datasets/arnobbhowmik/ton-iot-network-dataset

References

1. R. Belka, R. S. Deniziak, G. Łukawski, and P. Pięta, “Ble-based indoor tracking system with overlapping-resistant iot solution for tourism applications,” *Sensors (Switzerland)*, vol. 21, no. 2, pp. 1–21, Jan. 2021, doi: 10.3390/s21020329.
2. W. Qian, “Development and Practice of the Course System of Embedded Technology Specialty in the Context of ‘course Certificate Integration’ Based on Big Data Analysis,” *J. Phys. Conf. Ser.*, vol. 1992, no. 4, Aug. 2021, doi: 10.1088/1742-6596/1992/4/042009.
3. N. Ashammakhi, B. D. Unluturk, O. Kaarela, and I. F. Akyildiz, “The Cells and the Implant Interact With the Biological System Via the Internet and Cloud Computing as the New Mediator,” *Journal of Craniofacial Surgery*, vol. 32, no. 5, pp. 1655–1657, Jul. 2021, doi: 10.1097/scs.0000000000007534.
4. M. Wu and X. Chen, “Application of Internet of Things and embedded technology in electronic communication,” *Measurement: Sensors*, vol. 34, p. 101246, Aug. 2024, doi: 10.1016/J.MEASEN.2024.101246.
5. X. Zhang and W. T. Yue, “A 2020 perspective on ‘Transformative value of the Internet of Things and pricing decisions,’” *Electron. Commer. Res. Appl.*, vol. 41, p. 100967, May 2020, doi: 10.1016/J.ELERAP.2020.100967.
6. A. Awad, A. M. Aldabousi, and S. Albatal, “The influence of social media marketing on customer knowledge management: The role of confidentiality in UAE public banks,” *Banks and Bank Systems*, vol. 20, no. 1, pp. 1–10, 2025, doi: 10.21511/BBS.20(1).2025.01.
7. P. Zheng *et al.*, “A parallel unmixing-based content retrieval system for distributed hyperspectral imagery repository on cloud computing platforms,” *Remote Sens. (Basel).*, vol. 13, no. 2, pp. 1–21, Jan. 2021, doi: 10.3390/RS13020176.
8. F. Ramdani, A. Wirasatriya, and A. R. Jalil, “Monitoring the Sea Surface Temperature and Total Suspended Matter Based on Cloud-Computing Platform of Google Earth Engine and Open-Source Software,” *IOP Conf. Ser. Earth Environ. Sci.*, vol. 750, no. 1, May 2021, doi: 10.1088/1755-1315/750/1/012041.
9. S. K. Jagatheesaperumal, Q. V. Pham, R. Ruby, Z. Yang, C. Xu, and Z. Zhang, “Explainable AI Over the Internet of Things (IoT): Overview, State-of-the-Art and Future Directions,” *IEEE Open Journal of the Communications Society*, vol. 3, pp. 2106–2136, 2022, doi: 10.1109/OJCOMS.2022.3215676.
10. G. Singh, “A Move Towards Intelligent Economy: Indian Evidence,” *Management and Labour Studies*, vol. 46, no. 2, pp. 192–203, May 2021, doi: 10.1177/0258042X21989941.
11. P. Kalia, “Internet of things in e-commerce: A thematic analysis,” *Cloud and Fog Computing Platforms for Internet of Things*, pp. 41–56, Jun. 2022, doi: 10.1201/9781003213888-4.

12. Y. Gharde, A. Kamble, S. Dubey, and . P., “Smart Technologies for Smart Nations Internet of Things,” *International Journal of Innovative Science and Research Technology (IJISRT)*, pp. 3762–3767, Aug. 2024, doi: 10.38124/ijisrt/IJISRT24MAY1075.
13. S. A. Oyedotun, G. P. Oise, and C. E. Ozobialu, “Towards Intelligent Cybersecurity in SCADA and DCS Environments: Anomaly Detection Using Multimodal Deep Learning and Explainable AI,” *Journal of Science Research and Reviews*, vol. 2, no. 3, pp. 20–31, Jul. 2025, doi: 10.70882/josrar.2025.v2i3.76.
14. C. Ji, H. Huang, T. Wang, and Q. Huang, “Recent advances and future trends in processing methods and characterization technologies of aluminum foam composite structures: A review,” *J. Manuf. Process.*, vol. 93, pp. 116–152, May 2023, doi: 10.1016/j.jmapro.2023.03.015.
15. G. Oise and S. Konyeha, “Environmental impacts in e-waste management using deep learning,” *Discover Artificial Intelligence*, vol. 5, no. 1, p. 210, Aug. 2025, doi: 10.1007/s44163-025-00376-9.
16. X. Zheng, T.-T. Chen, X. Jiang, M. Naito, and I. Watanabe, “Deep-learning-based inverse design of three-dimensional architected cellular materials with the target porosity and stiffness using voxelized Voronoi lattices,” *Sci. Technol. Adv. Mater.*, vol. 24, no. 1, Dec. 2023, doi: 10.1080/14686996.2022.2157682.
17. S. A. Oyedotun, G. P. Oise, and C. E. Ozobialu, “Towards Intelligent Cybersecurity in SCADA and DCS Environments: Anomaly Detection Using Multimodal Deep Learning and Explainable AI,” *Journal of Science Research and Reviews*, vol. 2, no. 3, pp. 20–31, Jul. 2025, doi: 10.70882/josrar.2025.v2i3.76.
18. G. P. Oise *et al.*, “Isolation Forest–Based Intrusion Detection for Cyber-Physical Systems,” *Scientific Journal of Engineering Research*, vol. 2, no. 2, pp. 222–233, Mar. 2026, doi: 10.64539/sjer.v2i2.2026.434.
19. G. G. James, O. G. P, C. E. G, M. N. A, E. W. F, and O. P. E, “Optimizing Business Intelligence System Using Big Data and Machine Learning,” *Journal of Information Systems and Informatics*, vol. 6, no. 2, pp. 1215–1236, Jun. 2024, doi: 10.51519/journalisi.v6i2.631.
20. G. P. Oise, J. A. Odimayomi, B. N. Unuigbokhai, B. E. Akilo, and S. A. Oyedotun, “Deep Learning for Cybersecurity Threat Detection in Industrial Process Control and Monitoring Systems,” in *ECP 2025*, Basel Switzerland: MDPI, Feb. 2026, p. 43. doi: 10.3390/engproc2025117043.
21. M. Kim, W.-H. Yeo, and K. Min, “Co-free and low strain cathode materials for sodium-ion batteries: Machine learning-based materials discovery,” *Energy Storage Mater.*, vol. 69, p. 103405, May 2024, doi: 10.1016/j.ensm.2024.103405.
22. Arnob Bhowmik, “TON_IoT Network Dataset,” 2025.
23. G. P. Oise *et al.*, “DECENTRALIZED DEEP LEARNING IN HEALTHCARE: ADDRESSING DATA PRIVACY WITH FEDERATED LEARNING,” *FUDMA JOURNAL OF SCIENCES*, vol. 9, no. 6, pp. 19–26, Jun. 2025, doi: 10.33003/fjs-2025-0906-3714.
24. K. A. Al Sumarmad, N. Sulaiman, N. I. A. Wahab, and H. Hizam, “Energy Management and Voltage Control in Microgrids Using Artificial Neural Networks, PID, and Fuzzy Logic Controllers,” *Energies (Basel).*, vol. 15, no. 1, Jan. 2022, doi: 10.3390/en15010303.

25. Z. M. Ali, M. Calasan, S. H. E. A. Aleem, F. Jurado, and F. H. Gandoman, “Applications of Energy Storage Systems in Enhancing Energy Management and Access in Microgrids: A Review,” *Energies (Basel).*, vol. 16, no. 16, Aug. 2023, doi: 10.3390/en16165930.
26. I. M. Gadzhiev, M. P. Knyshenko, S. A. Dolenko, and A. V. Samsonovich, “Inherent dimension of the affective space: Analysis using electromyography and machine learning,” *Cogn. Syst. Res.*, vol. 78, pp. 96–105, Mar. 2023, doi: 10.1016/j.cogsys.2022.12.008.
27. H. Zeng, H. Zhou, A. Srivastava, R. Kannan, and V. Prasanna, “Accurate, efficient and scalable training of Graph Neural Networks,” *J. Parallel Distrib. Comput.*, vol. 147, pp. 166–183, Jan. 2021, doi: 10.1016/j.jpdc.2020.08.011.
28. H. Kchaou, Z. Kechaou, and A. M. Alimi, “A PSO task scheduling and IT2FCM fuzzy data placement strategy for scientific cloud workflows,” *J. Comput. Sci.*, vol. 64, Oct. 2022, doi: 10.1016/j.jocs.2022.101840.
29. P. A. Gbadega, Y. Sun, and O. Abolaji Balogun, “Advanced Control Technique for Optimal Power Management of a Prosumer-Centric Residential Microgrid,” *IEEE Access*, vol. 12, pp. 163819–163855, 2024, doi: 10.1109/ACCESS.2024.3491100.
30. S. M. Mohtavipour and H. S. Shahhoseini, “GCN-RA: A graph convolutional network-based resource allocator for reconfigurable systems,” *J. Comput. Sci.*, vol. 74, p. 102178, Dec. 2023, doi: 10.1016/J.JOCS.2023.102178.

Figures

Layer (type)	Output Shape	Param #
dense (Dense)	(None, 256)	11,008
dropout (Dropout)	(None, 256)	0
dense_1 (Dense)	(None, 128)	32,896
dropout_1 (Dropout)	(None, 128)	0
dense_2 (Dense)	(None, 64)	8,256
dense_3 (Dense)	(None, 10)	650

Figure 1

Figure 2. Neural Network Architecture

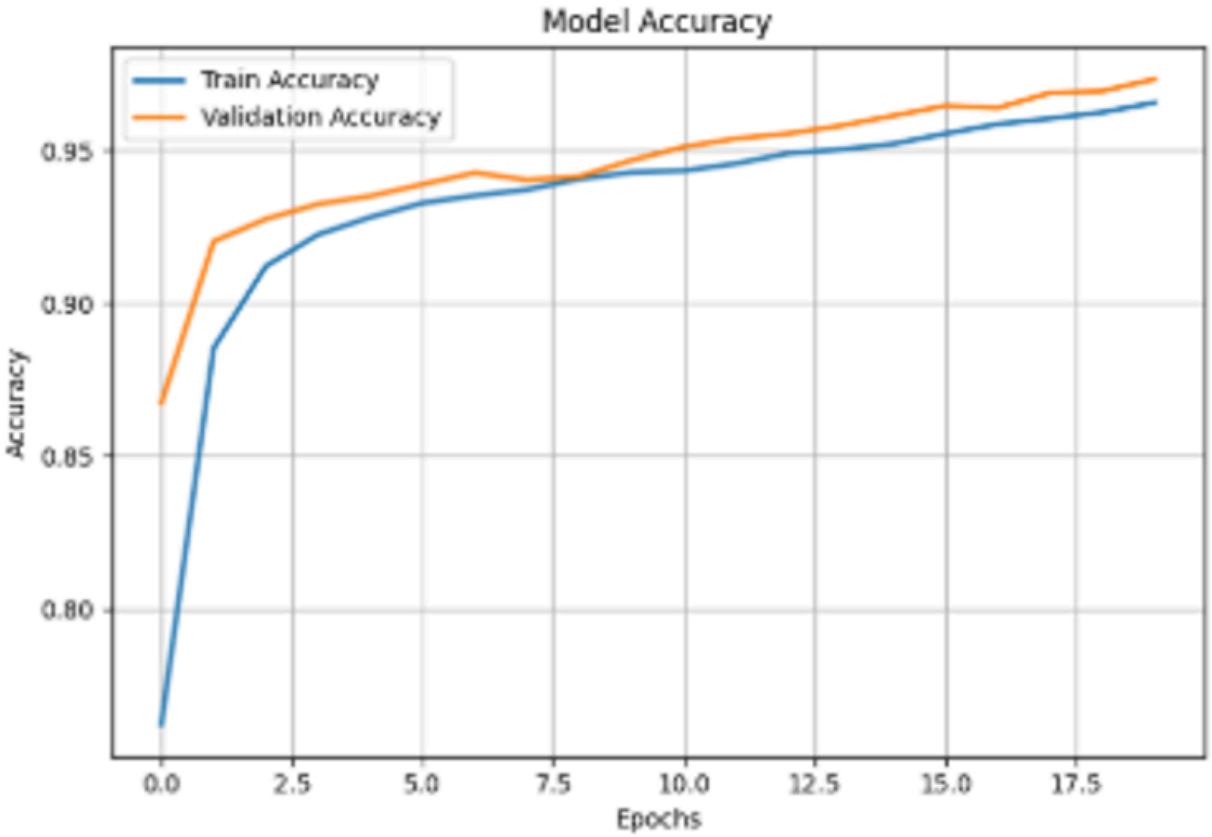


Figure 2

Figure 1: Training and Validation Accuracy Across Epochs

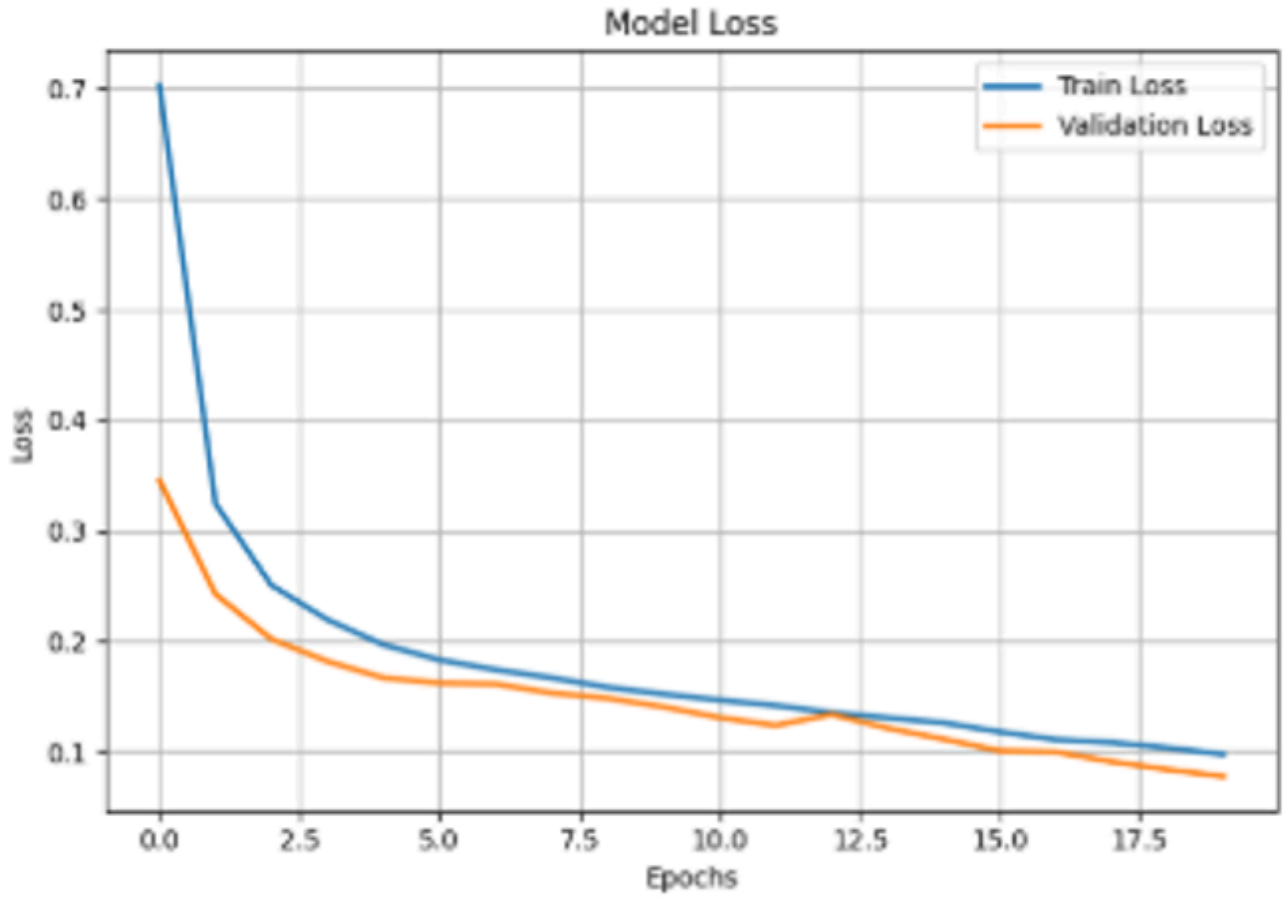


Figure 3

Figure 2: Training and Validation Loss Across Epochs

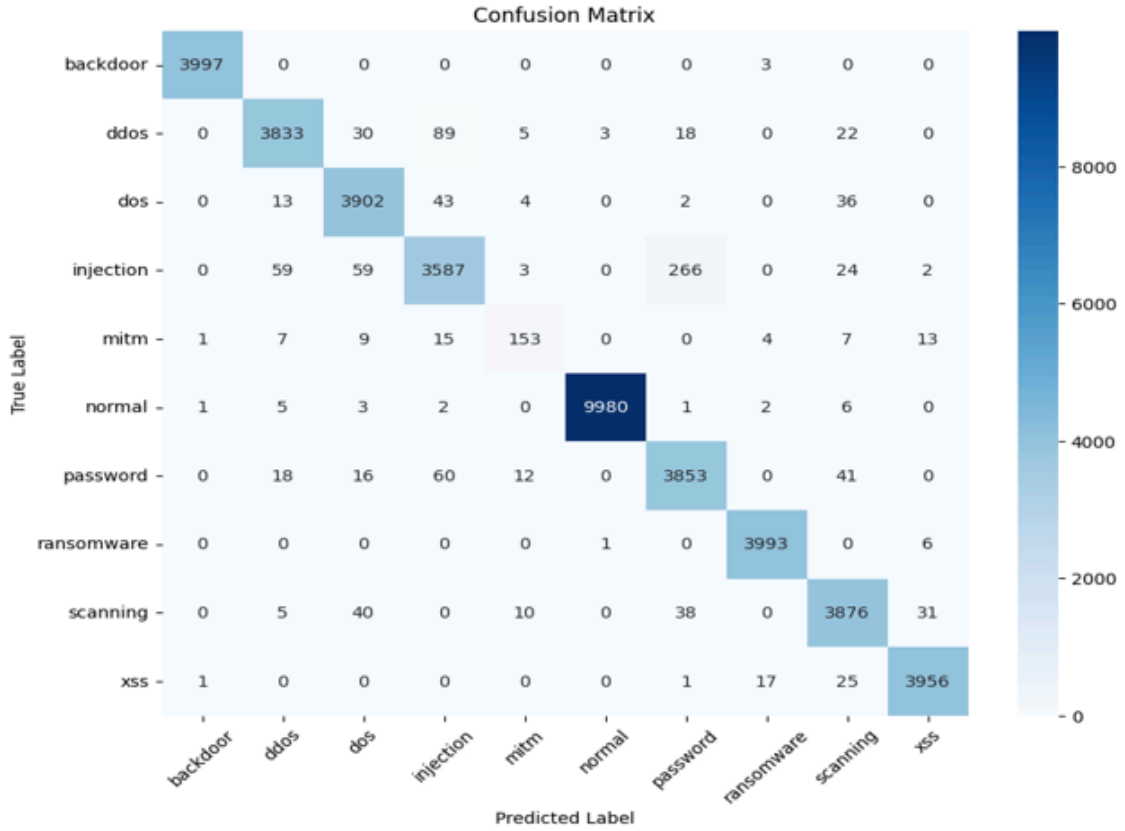


Figure 4

Figure 1: Confusion Matrix of the Multi-Class Intrusion Detection Model

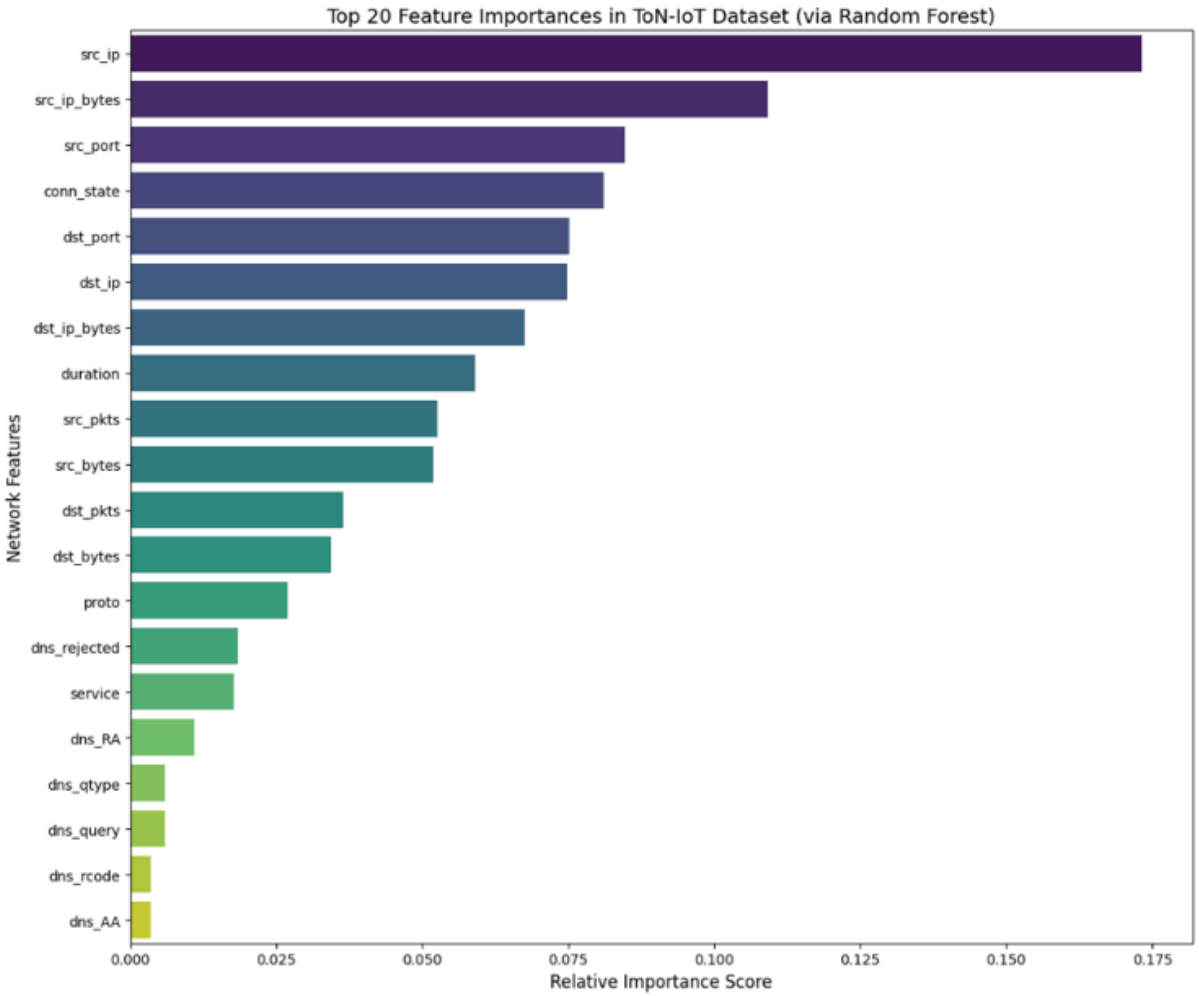


Figure 5

Figure 2: Top 20 Feature Importance in the ToN-IoT Dataset (Random Forest)

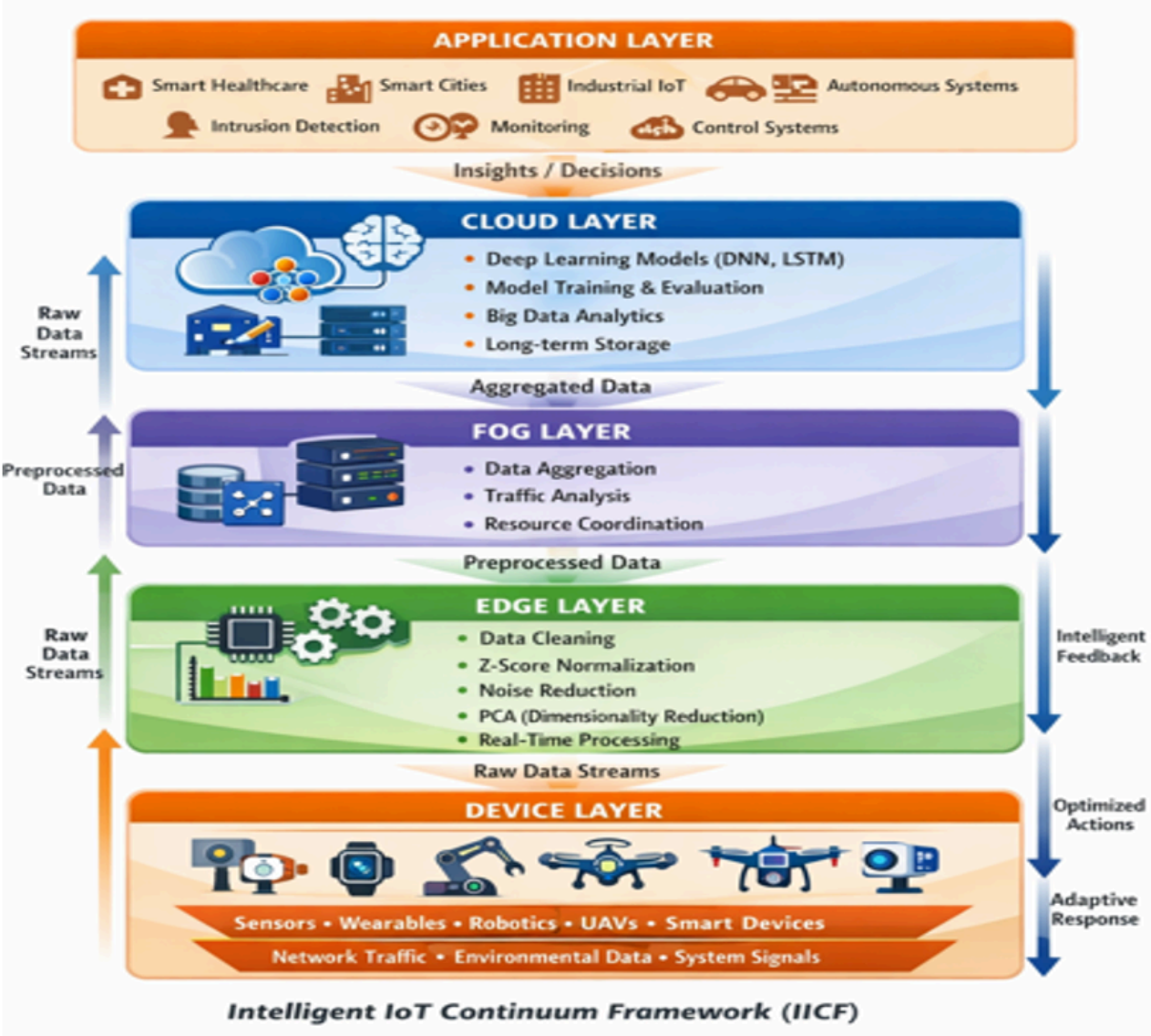


Figure 6

Unnumbered Image in the Methodology Section.