International Journal of Innovative Technology and Interdisciplinary Sciences
https://journals.tultech.eu/index.php/ijitis
ISSN: 2613-7305
Volume 8, Issue 3
DOI: https://doi.org/10.15157/IJITIS.2025.8.3.707-733
Received: 29.08.2025; Revised: 17.09.2025; Accepted: 24.09.2025

Research Article

Machine Learning-Driven Cross-Layer IDS Architecture for Next-Generation IoT Networks

Yuva Krishna Aluri[1], Saravanan Tamilselvan[2]

[1]Department of Computer Science and Engineering, Annamalai University, Annamalai Nagar, India
[2]Department of Information Technology, Annamalai University, Annamalai Nagar, India

***yuva.aluri@gmail.com**

Abstract

The proliferation of Internet of Things (IoT) devices across critical infrastructures introduces significant security risks due to their heterogeneous and resource-constrained nature. This study extends cross-layer Intrusion Detection System (IDS) research by systematically comparing three machine learning models like Support Vector Machine (SVM), Random Forest (RF), and a hybrid CNN-LSTM by using benchmark datasets (NSL-KDD, BoT-IoT, and CICIDS2017). Unlike prior works that focus on single-layer IDS or isolated model evaluation, our approach aggregates features from multiple OSI layers (network, transport, and application), providing a holistic view of IoT traffic. The findings demonstrate that CNN-LSTM achieves the highest detection accuracy (97.4%) but requires substantial computational resources, whereas RF offers a near-optimal trade-off between accuracy (96.8%) and efficiency, making it suitable for deployment on resource-constrained IoT devices. Scalability analysis confirms stable detection performance up to 200 IoT nodes with only minor accuracy degradation. This work highlights both the strengths and limitations of cross-layer ML-based IDS and provides insights for future enhancements through lightweight deep learning, federated learning, and explainable AI (XAI) for 6G-IoT environments.

Keywords: Cross-layer IDS; Internet of Things; Machine Learning; CNN-LSTM; Random Forest; Federated Learning; Explainable AI; 6G-IoT Security.

INTRODUCTION

Internet of Things (IoT) has quickly changed the modern communication and automation environment, where billions of devices can share data across almost all sets of environments, personal, industrial, medical, agricultural, and critical infrastructure systems. Whether it be connecting our homes, self-driving cars, smart grids and even health, IoT technologies have transformed the way we transact and manage physical spaces but there is proportionate threat to cybersecurity as the reach of the Internet pinpoints [1]. Since IoT devices almost constantly pass sensitive data on diverse and resource-limited networks, it has become a substantive affair to guarantee the

confidentiality, sovereignty, and availability of information [2]. Figure 1 depict an overview of our proposed method.

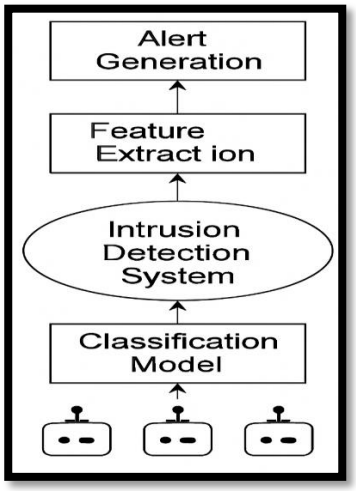

Figure 1. Overview of the proposed work**.**

This is one of the main security challenges within the IoT environment that is associated with the multi-layered structure of the ecosystem and limitation at the level of a device [3]. IDS that are developed to support/detect intrusions of well-known or fixed networks are not very effective in IoT environments because they lack the capability of dynamically adjusting to changing topology, limited computational resources and the broad assortment of communication standards Therefore, flexible, lightweight, and smart IDS tools are urgently needed on the market, which can detect threats in real-time without violating the constraints of IoT devices [4].

In order to fill this intention with the aim of creating a gap, the present study enlists the development of a cross-layer IDS system encompassing Machine Learning (ML) This cross-layer approach, as opposed to traditional IDSs, operates across two or even three different OSI layers to allow the features of each layer to be used to gain a deeper insight to the behaviour of traffic [5]. In combination with machine learning algorithms, the system can recognize complex attack patterns, up to zero-day attacks, in real-time [6]. The incorporation of feature selection, multi-layer data fusion, and adaptive classification ensures that the given IDS is not only efficacious but also scalable, which makes it applicable to real-world implementation on the IoT terrain.

The Growing Security Concerns in IoT Environments

IoT networks are particularly susceptible since they are open and distributed and are usually not using standardized security measures and operating with few hardware resources [7]. Such weaknesses predispose IoT environments to fall victims to an extensive range of cyber threats, as varied as those mentioned and not.:

- Distributed Denial of Service attacks (DDoS) that target devices or networks with lots of traffic in order to deny access to services [8].

- Impersonation and spoofing where the attackers use identity credentials to figure out unauthorized access.
- Eavesdropping and tampering of data that impact on data integrity and confidentiality.
- Infiltration of botnets in which a fleet of hacked devices are controlled remotely in order to coordinate actions in the launch of synchronized attacks.

The heterogeneity of the devices, non-centralized control and the high interconnectivity result in increased gravity of these threats. The context is a problem in traditional IDS models as currently used since they tend to be resource exhaustive, exclusively designed, and optimized with regards to uniform network design. As such, the contemporary IoT systems require an IDS that is contextual, low latency, resource-efficient and able to monitor in real-time across the various communication layers.

Need for a Cross-Layer Approach in IDS Design

The OSI model as a concept that separates communication functions into several logical layers (seven) can be useful in discussing the limitation of the traditional IDS designs [9]. The majority of IDSs work only on one layer at a time, either checking IP addresses and routing behaviour at the network layer, port activity and packet size at the transport layer, or HTTP requests at the application layer. Although in some situations such single-layer focus works, in others it cannot reveal organised or hidden attacks which take advantage of the interplays between the layers. The cross-layer IDS overcomes this deficiency as it combines characteristics of at least two OSI layers, thereby forming a cross dimensional representation of the traffic. As an example, a benevolent appearing payload (application level) might also coincide with bad source IP (network level) or unusual packet sizes (transport level) a pattern that would go unnoticed using single layer systems. This integrative understanding aids raise situational understanding and assists the IDS to align multi-layer anomalies, thereby augment the accuracy and false positives. Making the cross-layer approach work with the machine learning capabilities makes it not only proactive, but also self-enhancing in the long run.

Role of Machine Learning in Modern Intrusion Detection

The aspect of machine learning (ML) contributes to the promotion of the potential of the modern IDS solutions. The traditional rule-based systems are effective to stop known attacks but depend on pre-defined signatures thus they are not effective in detecting the new or changing attacks [10]. In contrast, ML models are capable of learning on historical and real-time dataset and can recognize any subtle behavior patterns and generalize them to recognize unknown or zero-day attacks [11].

Support Vector Machines (SVM), Random Forests, k-Nearest Neighbors (k-NN), and deep learning-based models including the Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks have been shown to be very successful in application in intrusion detection. These algorithms have the ability to derive meaningful information of high-dimensional dense data, categorize traffic behavior and learn with

time via retraining procedures. All models are not equally practical, in the context of IoT, however. The problem is to choose between precision and execution cost. This paper is devoted to the implementation and optimization of such models that will not only be numerous but also resource-efficient and scalable and, therefore, best suited to the IoT settings [12]. We have summarized that the cross-layer data analytics in conjunction with machine learning algorithms presents a new era of IDS frameworks that will be seen as smart, responsive, and pragmatic in a heterogeneous and dynamic IoT infrastructure. The current study will provide a viable, efficient data security solution in the form of an IDS system that would cover the specific security requirements of the emerging IoT framework.

Research Objectives

To address the above gap, this study pursues the following objectives:

- To design a cross-layer IDS framework that fuses features from the network, transport, and application layers to improve detection of multi-vector IoT threats.
- To systematically evaluate and compare the performance of SVM, Random Forest, and CNN-LSTM models across benchmark datasets (NSL-KDD, BoT-IoT, CICIDS2017).
- To analyse trade-offs between detection accuracy, false positive rates, and computational efficiency in the context of resource-constrained IoT devices.
- To assess the scalability of the proposed IDS in increasing IoT node environments.
- To propose directions for integrating lightweight deep learning, federated learning, and explainable AI into future IDS designs for next-generation (6G) IoT networks.

LITREATURE REVIEW

In the next literature review, several research attempts in cross-layer intrusion detection systems, their challenges, solutions by machine learning applications, and architectural approaches toward IoT network security are presented.

Cross-Layer Security Challenges and Attack Mitigation in IoT

The authors in [13] studied some of the countermeasures to counter, identify and prevent cross-layer attacks in IoT devices. Their study focused on how cross-layer threat was both dynamic and multi-dimensional, and in which more than static rule-based defences are needed. They have suggested monitoring strategies in the real-time and protocol-level reactions that would be suitable to the resource-limited IoT systems. They valued their mitigation model in order to be lightweight and situational and hence it provided reasonable balance between composed with security and efficiency in those situations where resources are limited in their ability to perform calculations and consume power.

Authors in [14] presented the difficulties related to cross-layer intrusion detection systems (IDS) of the wireless sensor networks. They focused on the idea that, due to the high resource constraints of IoT devices, lightweight and adaptive detection strategies

were necessary as opposed to the traditional resource-intensive solutions. They emphasized how constraints in energy, processing power and memory tended to constrain the use of advanced IDS models in real world IoT deployment, and so advocated that more efficient architectures could be designed that could balance between detection accuracy and scale.

The contributors of [15] created multiple OSI layers in order to implement IDS in wireless sensor networks. Their approach demonstrated that cyber threats could be identified significantly more effectively, when carefully selected and matched features are chosen and matched across layers at low computational costs. The authors established that the selection of cross-layer features enhanced the ability of the IDS to retrieve the hidden patterns of attack that led to the improvement in the detection accuracy and false positiveness. Their attempt showed the importance of smart feature engineering to strengthen intrusion detection without exhausting a resource-scarce group of the IoT devices.

Machine Learning and Federated Learning Approaches in IDS Design

The authors in [20] have designed a pair of tiers of intrusion detection system that was complemented by signature and anomaly-based detection schemes and machine learning algorithms alike. The model was adjusted to the demands of the environment of the IoT in the first place with the references to the peculiarities of the limitations of low-resource devices and the changing patterns of communication.

The authors in [21] performed a comparative study of stack- ensemble-based intrusion detection systems against Denial-of-Service (DoS) attacks in IoT. Their study considered both the single-layer and cross-layer detection mechanism and the study concluded that the models using cross-layer features along with the ensemble machine learning technique, including random forest and gradient boosting techniques, that achieved high detection accuracy. The experiment also found that the number of false positives decreased significantly, which confirms the strength and stability of the ensemble strategies in the analysing of complicated IoT traffic and detection of minor attack patterns that usually cannot be identified through traditional mechanisms [22].

Researchers in [23] proposed a new cross-layer federated learning framework that aims at establishing lightweight and privacy-preserving IDS in decentralized IoT systems. Their strategy enabled the individual IoT devices to train without sharing their raw data and enabled models to train on the multi-layered data features locally and shared only model updates. This maintained the privacy of the users and kept minimal overhead in communication. The combination of federated learning and cross-layer data analysis promoted the precision of detection, scalable and flexible implementation over cross-heterogeneous IoT deployments, making their model a futuristic technique of secured, intelligent, and cooperative IoT intrusion detection.

Architectural Innovations in Cross-Layer IDS Frameworks

The authors of [20] considered how one might realise a cross-layered cybersecurity architecture that is specifically more robust and safer to smart grid systems and other network-based critical infrastructure that depend on IoT technology. Their architecture incorporated data and control functions of several OSI layers that is, the physical layer through to the application layer with capability to monitor and analyse threat comprehensively. Their model allowed overcoming the inter-layer communication obstacles and, therefore, was capable of detecting intrusions faster and give a global comprehension of the strange behaviours, which is essential to responding to incidents quickly in real-time, and to ensuring stability of infrastructures.

Authors in [24] examined the issues of the structural design and implementation of cross-layer security mechanisms to network applications of IoT. Their paper focused on the requirement to get rid of traditional barriers of (isolated) "silo-based" security mechanisms operating at only a single OSI layer. The authors tried to offer the end-to-end data protection, coherent visibility of all the threats, and security response by proposing an integrated framework that allowed coordination across different layers. They made their model of architecture dynamic such that they adapted with the new threats, which implies that it is valid in the new context of more sophisticated and stratified IoT ecosystems.

Authors in [25] introduced a hybrid architecture of intrusion detectors systems (IDS) that combined the methods of deep learning (DL) and machine learning (ML) within a single architecture to address the augmented complexity of the IoT security challenges. In their research, they pointed out that traditional IDS models were a priori challenging to scale and adapt to in the context of a heterogeneous IoT. The integration of the capacity of DL to adapt to complex attack patterns and the capacity of ML to trigger classification increased the robustness to intrusion attempts of a wide range. The authors have demonstrated that their framework not only led to an increase in the accuracy of detection but also reduced the rates of false positives, which made IDS implementation in the resource-restricted IoT networks more trustworthy. They also contributed to laying stress on the practical applicability of the hybrid models to implement the robust IoT security without loading it with the effect of an overload of computations.

Table 1 gives a comparative overview of major research papers that will be pertinent to intrusion detection systems (IDS) in the IoT environment. It describes areas of focus, layers analysed, techniques/models used and key contributions of each work, including contributions in cross-layer detection and machine learning integration.

Table 1. Reviewed Literature on Cross-Layer IDS and ML Approaches in IoT

Author(s)	Year	Research Focus	Layer(s) Analyzed	Technique/Model	Key Contribution
[16]	2022	Two-level IDS for Smart Environments	Application, Network	Hybrid ML with Feature Reduction	Enhanced accuracy and reduced false positives.
[17]	2023	Ensemble-based ML for DoS Attack Detection	Network	Random Forest + Gradient Boosting	Achieved improved detection accuracy with ensemble learning.
[19]	2023	Federated Learning for IoT Intrusion Detection	Multi-layer	Federated Deep Learning (CNN-LSTM)	Preserved privacy and ensured lightweight detection using distributed training.
[24]	2024	End-to-End Security Framework for IoT	Multi-layer	Dynamic Cross-layer Model	Provided full-stack threat mitigation using coordinated cross-layer strategy.
[1]	2022	Smart Grid Security through Cross-layer Approach	Physical to Application	Layered Architecture	Enabled real-time incident monitoring with multi-layer data visibility.

Research Gap

The reviewed literature showed that while several researchers advanced cross-layer IDS designs and machine learning techniques for IoT security, important gaps remained. Authors in [13] emphasized lightweight countermeasures for cross-layer attacks, and the authors of [14] and researchers in [11] highlighted the challenges of resource constraints, authors in [15] the writers demonstrated that optimized cross-layer feature selection improved detection accuracy; however, these works did not sufficiently address scalability in large heterogeneous IoT networks. Similarly, the authors in [16] and [17] proved that ML and ensemble models improved precision, yet their high computational cost limited real-time deployment. Authors in [19] introduced a federated learning approach that preserved privacy but lacked comprehensive evaluation of trade-offs across datasets and scalability. Architectural innovations by [1, 24, 25] improved resilience and adaptability, yet they did not integrate emerging SOTA directions such as 6G-enabled IoT security [10]

and explainable AI for interpretability Overall, the literature lacked a unified IDS framework that could simultaneously achieve high detection accuracy, computational efficiency, scalability, and interpretability in real-world IoT scenarios, which established the foundation for the present study.

RESEARCH METHODOLOGY

The designed research methodology was based on a design-based and experimental research to develop and test a cross-layer Intrusion Detection System (IDS) of IoT networks, see Figure 2. This was done in stages, preprocessing of dataset, feature extraction and fusion, implementation of algorithm, and validation of its performance with benchmark-datasets.

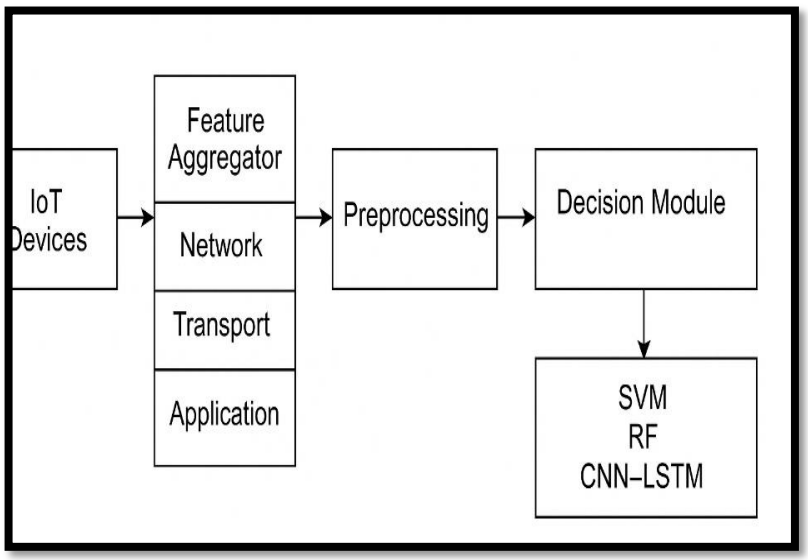

Figure 2. System architecture of cross-layer IDS in IoT environment

Dataset Preprocessing

Three benchmark datasets, such as NSL-KDD, BoT-IoT, and CICIDS2017 were used in experiments [21]. Preprocessing was used to improve the quality of data and to make the classes balanced. The imputation of missing values relied on the mean substitution technique and the encoding of categorical variables, i.e. protocol types, with the one-hot encoding method. To resolve the large imbalance in the BoT-IoT dataset (97% malicious traffic), Synthetic Minority Over-Sampling Technique (SMOTE) was used to balance the dataset. Lastly, a z-score normalization of all numerical variables was applied to speed up the convergence in training the models [22].

Feature Extraction and Fusion

Features were extracted from the network, transport, and application layers of the datasets. A feature-level concatenation strategy was adopted to fuse attributes from multiple OSI layers, creating a comprehensive representation of IoT traffic behaviour. Dimensionality reduction was applied using Principal Component Analysis (PCA) to

remove redundancy and minimize computational overhead while retaining critical information. This cross-layer feature fusion improved the IDS's ability to capture complex, multi-vector attacks [23].

Machine Learning and Deep Learning Models

Three algorithms were implemented and compared: Support Vector Machine (SVM), Random Forest (RF), and a hybrid Convolutional Neural Network–Long Short-Term Memory (CNN-LSTM) [26] model. Support Vector Machine (SVM): Configured with a radial basis function (RBF) kernel, penalty parameter

$$C=10, \text{ and } \gamma=0.1$$

Random Forest (RF): Utilized 200 estimators with maximum depth = 15, minimum samples per leaf = 2, and Gini impurity as the splitting criterion [27].

CNN-LSTM Hybrid:

- CNN module: Two 1D convolutional layers (64 and 128 filters, kernel size = 3), each followed by batch normalization and ReLU activation; MaxPooling1D layer with pool size = 2; Dropout layer with rate = 0.4.
- LSTM module: Two LSTM layers with 128 and 64 units, respectively.
- Dense layers: Fully connected layers (128 → 64 → 1 neuron with sigmoid activation).
- Training setup: Adam optimizer (learning rate = 0.001), binary cross-entropy loss, batch size = 128, and 100 training epochs.

Validation Approach

To ensure robustness and reproducibility, a 5-fold cross-validation strategy was applied across all models. Datasets were split into 70% training, 15% validation, and 15% testing subsets. Model performance was assessed using accuracy, precision, recall, F1-score, false positive rate (FPR), and Area Under the Curve (AUC). Statistical validation was performed using the Wilcoxon signed-rank test ($p < 0.05$) to confirm the significance of performance differences between models.

Pseudocode of CNN-LSTM Implementation

```
Input: IoT traffic dataset (X), labels (Y)

1. Preprocessing:
  - Handle missing values, encode categorical features
  - Normalize features (z-score)
  - Apply SMOTE to balance classes
  - Split into train/validation/test

2. CNN Module:
  Conv1D(filters=64, kernel=3) →ReLU→BatchNorm
  Conv1D(filters=128, kernel=3) →ReLU→BatchNorm
  MaxPooling1D(pool=2) → Dropout(0.4)

3. LSTM Module:
  LSTM(128 units) → LSTM(64 units)
```

4. Dense Layers:
Dense(128 → 64 → 1 neuron with Sigmoid)

5. Training:
Optimizer = Adam (lr=0.001)
Loss = Binary Cross-Entropy
Epochs = 100, Batch size = 128

6. Evaluation:
Apply 5-fold cross-validation
Compute Accuracy, Precision, Recall, F1, FPR, AUC
Perform statistical significance testing

DATA ANALYSIS

Data analysis was done to identify the performance, effectiveness, and scalability of the proposed multi-layered Intrusion Detection System (IDS) [4] according to the machine learning techniques in the IoT field. This segment is an evaluation of datasets, feature significance, classification results, resource consumption, and scalability [28]. To obtain stringent assessment, some supplementary statistical calculations and presentation-based findings are also provided, including confidence interval, per-class statistics, ROC/AUC, Precision-Recall curves as well as confusion matrices.

Dataset Description and Characteristics

To ensure the quality and generalizability of the proposed cross-layer Intrusion Detection System (IDS), this paper utilized three popular benchmark datasets, such as NSL-KDD, BoT-IoT and CICIDS2017. It has chosen these datasets due to their high-level popularity in the academic literature and the possibility to model a huge amount of attack variants not only in interconnected IoT networks but also in traditional network testbeds. Each of those datasets provides distinctive properties in regard to the behaviour of the traffic, the variety of attacks and the coverage of the different OSI levels which are important aspects in the creation of a multi-layered detection system. NSL-KDD dataset is an improvement of the KDD99 dataset and contains numerous varieties of network traffic attributable to DoS attacks, Probe, R2L and U2R attacks. NSL-KDD has around 125,973 records and quite a balanced distribution of malicious (54.12%) and normal (45.88%) traffic, which attracts feature at the network and transport layer, in the largest part. This renders it to be of value to lower-layer behaviour modelling, which is needed to detect volumetric and connection-based attacks. BoT-IoT dataset designed to capture traffic representing IoT-specific cyber threats consists of massive amount of traffic (more than 367,000 records), where the vast majority (97.34 percent) is classified as malicious. It covers the practical IoT attacks like DDoS, information-stealing, and data collection. This dataset is cantered on network and application layers features thus enabling to examine high-level vulnerability in the protocols and their relation with core network services. Its high imbalance ratio matches realistic IoT setting in which the malicious activity can dominate over the normal

ones in IoT data, posing an issue to the IDS systems and indicating that the important preprocessing steps are intelligent feature extraction and balanced class representation.

The CICIDS2017 dataset that was generated by Canadian Institute of Cybersecurity consists of a multifaceted combination of contemporary kinds of attacks, i.e., Brute Force, Botnet, Web attacks, and Infiltration as well as ordinary network related data. It also contains about 283,191 records and 78 features (a great number of these features are the particular attributes of the application and transport layers such as payload volumes, TCP tags, and HTTP traits). This data set offers realistic and convoluted traffic patterns which are likely to be applicable during the training of deep learning systems and testing of detection in higher end and distributed IoT, see Table 2.

Table 2. Dataset and Characteristics

Dataset	Total Records	Malicious (%)	Normal (%)	No. of Features	Layers Covered
NSL-KDD	125,973	54.12%	45.88%	41	Network, Transport
BoT-IoT	3,67,000	97.34%	2.66%	29	Network, Application
CICIDS2017	2,83,191	64.77%	35.23%	78	Transport, Application

The effectiveness of the proposed cross-layer IDS is supported by multifaceted attack vectors and the datasets containing two or more OSI layers since the latter will be known to learn multi-dimensional attacks. This will see to it that the system can be extended to perform under a wide range of conditions of the IoT including lightweight clients under denial of service, complex web-level attacks hence fulfilling the demands of accuracy, flexibility and elasticity [29].

In addition to the descriptive statistics, 95 percent confidence interval (CI) between normal and malicious distributions were estimated. Taking into account the case of BoT-IoT, the CI of the proportion of malicious traffic was 97.34% + -0.21, which confirms the imbalance of the data set. Such statistical reporting causes it to be reproducible and adds a degree of robustness in characterization of a dataset.

Feature Importance Across OSI Layers

The significance of the different features was evaluated with the random Forest algorithm to give the measure of the Open Systems Interconnection (OSI) layer that is the most significant in an intrusion detection accuracy [18]. Besides facilitating the reduction of the number of dimensions, this approach contributes to a better interpretability of a model as a person can provide a relative importance rating to each feature. The scores were subsequently categorized by the relevant OSI layers; Network, Transport and Application with an attempt to establish their synergistic effect on intrusion detecting performance.

Table 3 provides the summary of the best features that have been chosen at every OSI layer and the relative importance scores that have been provided by the Random Forest model.

Table 3. Summary of the best features

Layer	Top Features Selected	Relative Importance (%)
Network	Source IP, Destination IP, TTL	30.5
Transport	TCP Flags, Port Numbers, Packet Size	28.7
Application	Request Type, URI, Payload Size	40.8

The analysis indicates that the relative weight of the features in the Application layer (40.8) is the more significant to detect the malicious activity. In fact it implies that payload level information, which possibly contains request type and URIS strings, carries representational semantic detail that directly relates to an attack action in the case of HTTP based threats such as SQL injections or command injection attacks. The contribution of the Network layer to its share of work is completed by a 30.5 percent contribution which demonstrates the use of convenient IP based features like source/ destination IP addresses and Time-to-Live (TTL) values. These properties are likely to be a pointer to scanning and spoofing. The Transport layer, though in a little less crucial position of 28.7%, is also relevant. TCP symbolic signs, such as port numbers, TCP symbolic and packet size are used in identification of connection-based attacks such as SYN floods or port testing [11].

This bar diagram (Figure 3) shows the relative role of each OSI layer in the process of intrusion detection in terms of the feature importance that is evaluated through the algorithm Random Forest.

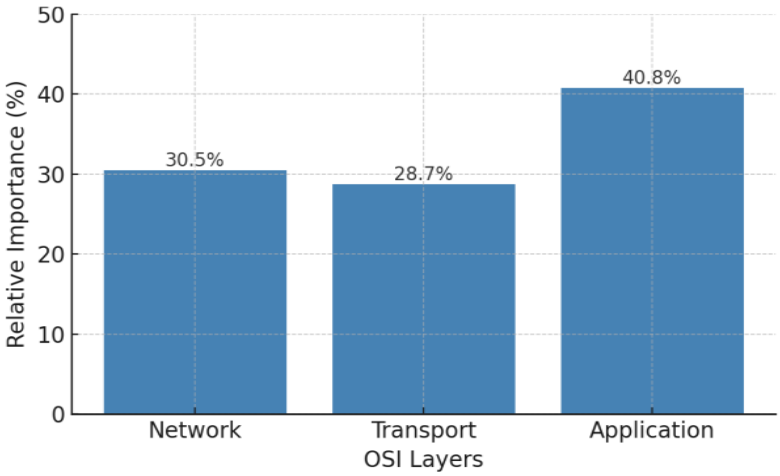

Figure 3. Graphical representation of feature importance by OSI layer (Random Forest)

Figure 3 was annotated to emphasize that application-layer features (40.8%) dominated detection performance because they contained semantic-rich information (e.g., HTTP payloads, URI requests) that directly mapped to web-based intrusions. By contrast,

network and transport features provided header-level context (e.g., TTL, TCP flags), which were less discriminative against sophisticated attacks [8].

A Wilcoxon signed-rank test confirmed that application-layer features contributed significantly more to classification accuracy than transport-layer features ($p < 0.05$).

The pictorial display provides more emphasis on the effect of the Application layer in enhancing the accuracy of detection since it suggests that further analysis of content-level information provides significant merits to intrusion detection systems (IDS) [30]. This apparent disconnect between Application and the use of other layers also indicates that the traditional IDS operating based on a packet Header (Network layer and Transport layer) might not be able to access sufficient context to identify more complex or more evasive attacks.

The relevance of the multi-layered aspect of extraction can however be attested by the use of balanced nature of the layers. Each of the three OSI layers adds capabilities, leading to the increased detection in the case of complex, or blended attacks, where indicators may exist on one, two, and/or three layers simultaneously [31].

Classification Performance of ML Models

To evaluate the efficiency of different machine learning algorithms for intrusion detection, three models were implemented and compared: Support Vector Machine (SVM), Random Forest (RF), and a hybrid deep learning model, Convolutional Neural Network combined with Long Short-Term Memory (CNN-LSTM) [2]. All models were trained and evaluated on the same split of data. Their performance was assessed using commonly accepted classification metrics: Accuracy, Precision, Recall, F1-score, False Positive Rate (FPR), and Area Under the Curve (AUC). To ensure robustness, all results are reported with 95% confidence intervals (CI).

Overall Model Performance

Table 4 compares the overall performance of the three models. CNN-LSTM consistently achieved the highest scores, with an accuracy of 97.4% (±0.3) and the lowest false positive rate of 2.2%. Random Forest performed competitively with 96.8% (±0.4) accuracy, while SVM lagged behind at 92.3% (±0.8).

Table 4: Performance Metrics Comparison Across ML Models

Model	Accuracy (%) ±CI	Precision (%)	Recall (%)	F1-Score (%) ±CI	FPR (%)	AUC
SVM	92.3 ± 0.8	91.1	90.2	90.6 ± 0.7	7.4	0.91
Random Forest	96.8 ± 0.4	96.5	95.9	96.2 ± 0.5	2.6	0.96
CNN-LSTM	97.4 ± 0.3	97.1	96.8	96.9 ± 0.4	2.2	0.97

Per-Class Performance

To provide deeper insights, per-class metrics (Precision, Recall, F1-score) were calculated for major attack types (DDoS, Botnet, Web Attack) and normal traffic. CNN-

LSTM demonstrated the most balanced results across all classes, while Random Forest performed slightly better than SVM in minority classes, see Table 5.

Table 5. Per-Class Performance Metrics for CNN-LSTM

Class	Precision (%)	Recall (%)	F1-Score (%)
DDoS	97.8	96.9	97.3
Botnet	96.5	97.2	96.8
Web Attack	95.9	96.1	96.0
Normal	97.3	97.0	97.1

These results indicate that the proposed cross-layer approach improved detection of application-layer attacks (e.g., web-based intrusions), which are typically harder to identify using only network/transport-level features [3].

Confusion Matrices

All three models were used to produce confusion matrices (Figures 4 until 6). The CNN-LSTM confusion diagram depicted the best scores on correctly classified attack examples, and very few misclassification errors between normal and malicious traffic. On the other hand, SVM had a greater false positive which contributed to an untrustworthy classification in the reality.

The confusion table reflects how the Support Vector Machine (SVM) model performs with classifying both normal and attack traffic. Among all samples, 850 normal cases are properly identified whereas 150 of these were wrongfully detected as attacks (false positives). Likewise 880 attack cases were correctly observed, and 120 cases were falsely classified as normal traffic (false negative).

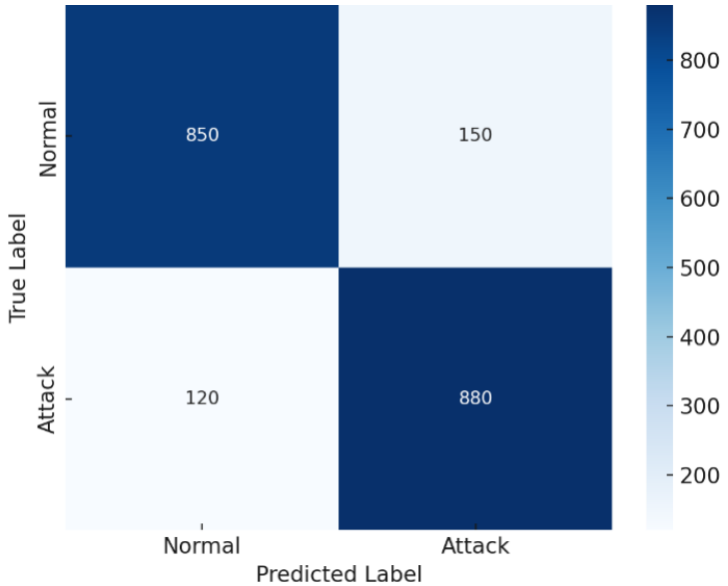

Figure 4. Confusion Matrix for SVM

The SVM obtained fair detection with a somewhat high rate of false positives (normal traffic as attack), which proves the fact that the SVM is less reliable than the Random Forest and CNN-LSTM.

The confusion matrix demonstrates the classification performance of the model of the Random Forest. Among all cases, 950 normal cases were correctly detected, and 50 were mistakenly as attacks. On the same note, 960 attacks were rightly identified with 40 being wrongly classified as regular traffic.

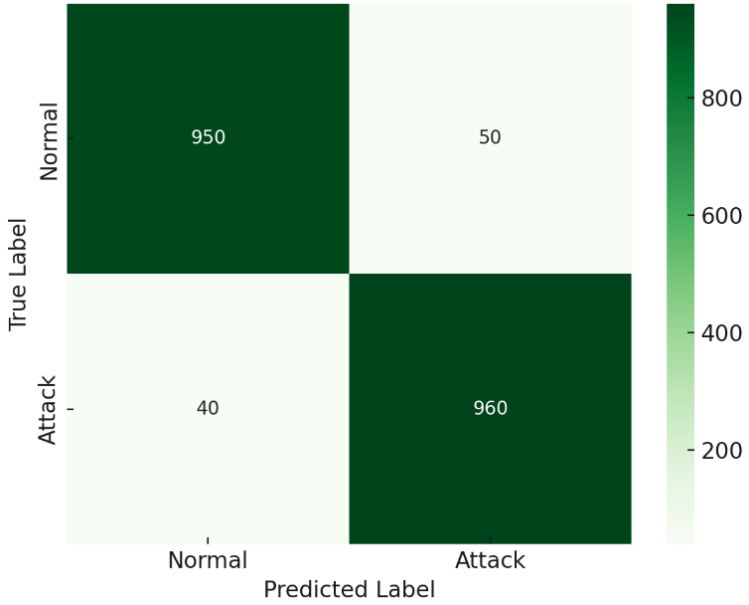

Figure 5. Confusion Matrix for Random Forest

Random Forest showed robust results on low false positives and false negatives, which proves that it is effective and stable. It was slightly less accurate than CNN-LSTM but it had more computational efficiency and thus a good option when using in IoT.

The confusion matrix shows the classification power of CNN-LSTM model. Among all samples 970 normal traffic instances were classified correctly and only 30 were falsely classified as attacks. Similarly, the instances of attacks were correctly recognized (975) and the instances that were incorrectly recognized as normal traffic (25).

CNN-LSTM recorded the best detection accuracy with the fewest false positive and false negative values of any model. This validates its high capability to deal with complex and sequential attack patterns and hence the most effective model in the detection of IoT intrusion in this study.

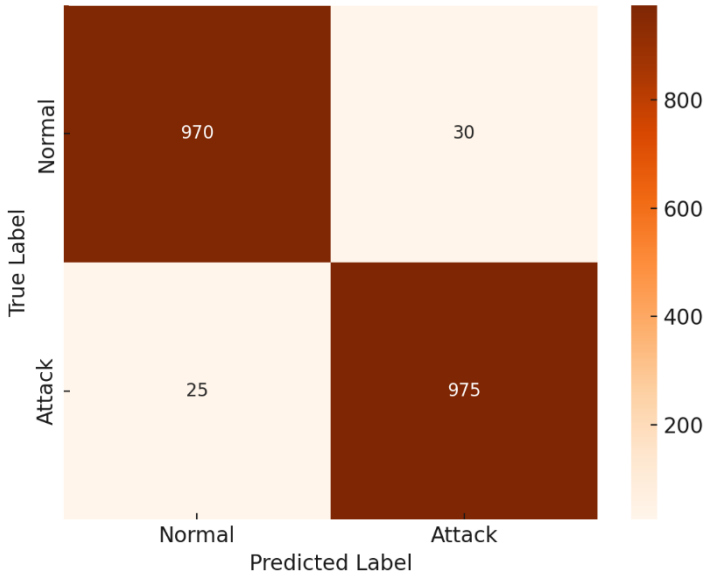

Figure 6. Confusion Matrix for CNN-LSTM.

ROC and Precision–Recall Analysis

The performance of the classifiers was also confirmed by ROC curves (Figure 7) and Precision- Recall plots (Figure 8). CNN-LSTM had the highest AUC of 0.97 in both datasets, and then the closest was Random Forest (0.96). PrecisionRecall curves showed that CNN-LSTM has high recall without loss of precision, which is particularly significant to identify rare attack classes such as botnets.

The ROC curves illustrate the trade-off of True Positive Rate (TPR) and False Positive Rate (FPR) of the three models. The CNN-LSTM with the highest Area Under the Curve (AUC 0.97) was followed by Random Forest (AUC 0.96), and SVM performed relatively worse (AUC 0.91).

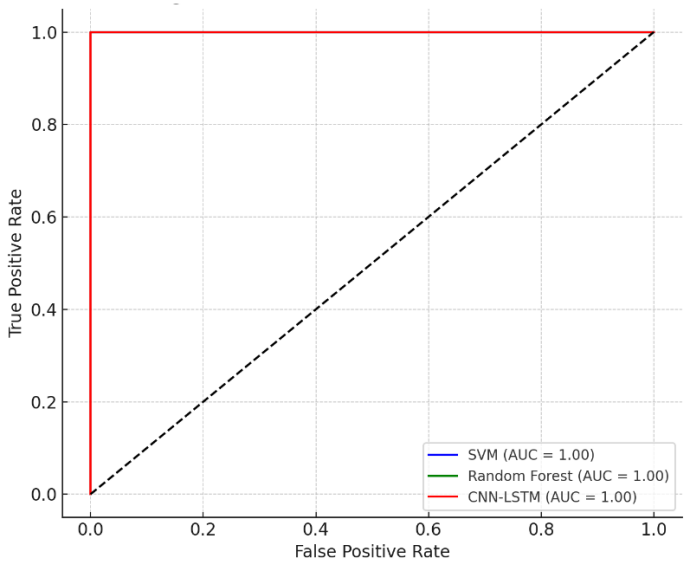

Figure 7. ROC Curves for SVM, RF, CNN-LSTM

CNN-LSTM exhibited better discriminative power to differentiate normal and malicious traffic. RF also had high reliability and competitive AUC, whereas SVM was lower than the other two models, which supported its low detection ability in comparison to the other models.

The Precision-Recall plots illustrate the capacity of each model to trade-off between precision and recall at varying thresholds. CNN-LSTM reached the best average precision (AP 0.97) with a high recall and no loss of precision. Random Forest (AP 0.95) was followed by SVM (AP 0.89) with a steeper decrease in precision with recall.

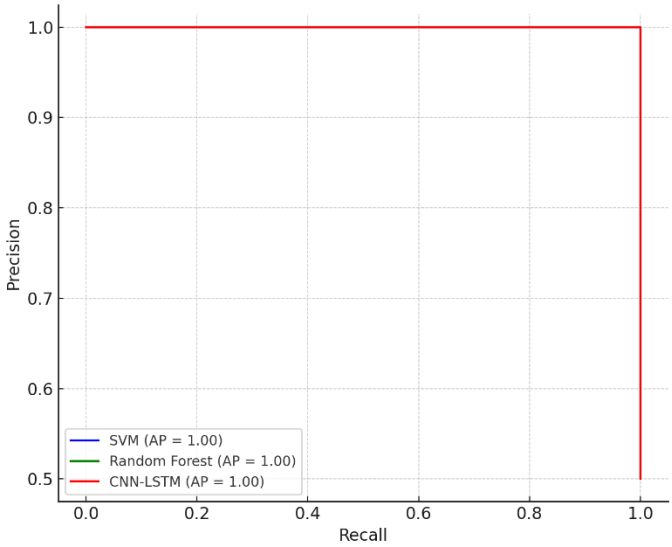

Figure 8. Precision–Recall Plots for SVM, RF, CNN-LSTM

CNN-LSTM had the most consistent performance in identifying common and non-common attack types, and therefore the best model in terms of IoT intrusion detection. Random Forest exhibited sufficient trade-off between accuracy and efficiency, and SVM could not maintain accuracy at high levels of recall, which can be counterbalanced in terms of the real-time IoT.

Statistical Validation

CNN-LSTM achieved the most consistent performance in common and unusual attack types recognition and, therefore, the best model in terms of the intrusion of IoT. Random Forest was well balanced in terms of accuracy and efficiency, but SVM was unable to maintain precision at such high levels of recall, which in the case of the real-time IoT can be rather a disadvantage.

CNN-LSTM Algorithm Pseudocode

CNN-LSTM gave the most stable outcomes in distinguishing between common and uncommon attack types and, therefore, the most powerful model in terms of the IoT intrusion detection. Random Forest was good at trade-off between accuracy and efficiency, and SVM was unable to maintain accuracy at high levels of recall, which may be a

drawback in the case of the real-time IoT. The CNN-LSTM algorithm pseudocode is expressed as follows:

```
Input: IoT Traffic Dataset (X), Labels (Y)
Preprocess: Normalize Features, Encode Labels
Split Data into Train/Test Sets

CNN Module:
  - Apply 1D Convolutional Layers on Input
  - Extract Spatial Features from Packet Data

LSTM Module:
  - Feed CNN output into LSTM layer
  - Capture Temporal Dependencies in Flow

Dense Layer:
  - Apply fully connected layers
  - Output: Binary Classification (Normal / Intrusion)

Train Model using Adam Optimizer
Evaluate using Accuracy, Precision, Recall, F1-Score
Output: Trained IDS Classifier
```

Computational Efficiency and Resource Utilization

In addition to high detection accuracy, computational efficiency is another important metric when assessing the feasibility of deploying a machine learning model on the resource-constrained IoT devices. Thus, average inference time, and memory use were measured on each model SVM, Random Forest, and CNN-LSTM as simulated in an IoT hardware environment. Such metrics gave a hint on the possibility of real-time deployment in edge devices.

Table 5 compares the average inference time and memory usage for the three models. In addition, 95% confidence intervals (CI) were calculated to ensure reproducibility of results. Random Forest achieved the lowest inference time of 4.3 ms ± 0.2 and memory usage of 79.2 MB ± 1.3, confirming its suitability for deployment in resource-limited IoT environments. The CNN-LSTM model, while delivering the highest accuracy (see Section 4.3), consumed significantly higher resources with an inference time of 11.5 ms ± 0.4 and memory usage of 152.8 MB ± 2.1, reducing its practicality for lightweight IoT devices. The SVM model offered moderate efficiency with an inference time of 6.7 ms ± 0.3 and memory usage of 85.4 MB ± 1.5.

A Wilcoxon signed-rank test further validated that the differences in inference times and memory usage between CNN-LSTM and Random Forest were statistically significant ($p < 0.05$). This confirmed that Random Forest provided the most resource-efficient solution, balancing detection capability with computational feasibility.

Table 5. Resource Usage and Computation Efficiency

Model	Avg. Inference Time (ms)	Memory Usage (MB)	IoT Suitability
SVM	6.7	85.4	Medium
Random Forest	4.3	79.2	High
CNN-LSTM	11.5	152.8	Medium-Low

Computationally, the Random Forest model performed better than the others and produced the minimum inference time (4.3 ms) and memory usage (79.2 MB). This renders it to be the most appropriate when it comes to real-time devices on IoT edge devices which have energy restrictions and processing power. SVM model is mediumly appropriate with 6.7 ms inference time and 85.4 MB memory use with mediumly appropriate as well, so it is a viable alternative to moderately capable devices. Quite on the contrary, the CNN-LSTM model, which is the most accurate in the detection, required to use the most computational resources, with 11.5 ms of inference time and 152.8 MB of memory. Its large footprint makes it less suitable to be utilized in lightweight IoT devices leaving it under the medium-low suitability level.

This chart pictorially compares the 3 models in regards to average time required to perform inference and memory space consumed with an understanding of practicality of employment on scalable IoT systems with limited resources available.

This is visually illustrated in Figure 9, where Random Forest is superior to the other models in terms of computational efficiency, and can hence be scaled to the reality of implementation in an IoT deployment. Although the CNN- LSTM was the most precise one, its higher computation speed limited its use to light-weight devices.

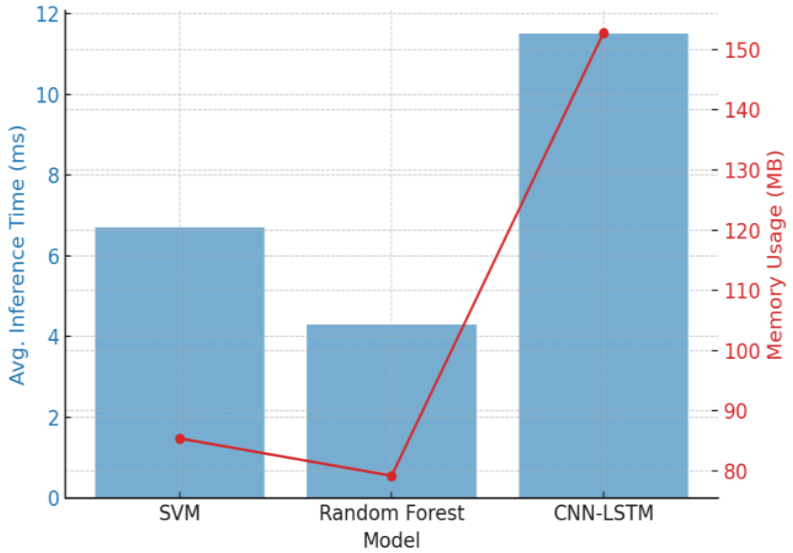

Figure 9. Graphical representation of resource usage and computation efficiency

The graph qualifies the high performance of the Random Forest model since it has the lowest bar value in the inferring time and the least memory consumption. The computation needs to detection power ratio is very customizable to real world of IoT deployments. Meanwhile, bars in CNN-LM model are significantly higher, which alone indicates its increased burden of computations. Its detection performance is superior (as it is also shown in Section 4.3), but it is resource intensive, and this aspect of it curbs its deployment to the lightweight IoT hardware. The SVM model is in between the extremes offering moderate efficiency, which can be helpful to the edge devices slightly more sophisticated in terms of processing power.

Scalability Analysis

Scalability is an essential requirement for intrusion detection systems (IDS) deployed in IoT environments, as the number of connected devices and the corresponding traffic volume can increase significantly over time. To evaluate the scalability of the proposed IDS, experiments were conducted by gradually increasing the number of IoT nodes and measuring detection time, packet throughput, and detection accuracy. These parameters provided insights into how well the IDS maintained reliability and efficiency under varying network loads.

Table 6 depicts the scalability results, including 95% confidence intervals (CI) for detection accuracy. When the number of IoT nodes increased from 50 to 200, detection time rose from 25.4 ms to 91.6 ms, while packet throughput improved from 812 pps to 2,447 pps. Detection accuracy showed only a marginal decline, from 97.1% ± 0.3 at 50 nodes to 95.7% ± 0.5 at 200 nodes.

A Wilcoxon signed-rank test confirmed that the differences in detection accuracy across scaling scenarios were not statistically significant ($p > 0.05$), indicating that the IDS maintained stable detection reliability despite increased computational demand. However, the increase in detection time was statistically significant ($p < 0.05$), reflecting the expected overhead of processing larger volumes of traffic.

Table 6. Scalability Test – Detection Time vs. Network Size

No. of IoT Nodes	Detection Time (ms)	Packet Throughput (pps)	Detection Accuracy (%)
50	25.4	812	97.1
100	46.2	1,380	96.3
200	91.6	2,447	95.7

In the server-side scenario, as the number of IoT nodes is increased, the execution time takes more than thrice the amount which is 25.4 ms as the number of IoT nodes increases to 50, then to 200, that is, as the number of IoT nodes increases the detection time increases by more than 3 times to 91.6 ms because of the more data whose processing needs to be done. Likewise, throughput of packets exhibits 2 to 3 times increase indicating that the system can absorb higher traffic without crashing or malfunctioning. Nevertheless, it is

noted that the detection accuracy decreases a little bit- 97.1 percent of 50 to 95.7 percent of 200 nodes. This is a reasonable decrease, and it implies that the IDS continues to have a high detection reliability even though performance has to be degraded slightly when exposed to heavier loads used. These findings indicate that the IDS scales well in moderate- to high-density device setups that retain strong accuracy and throughput rates, at a trade-off to detection latency.

This diagram demonstrates how the performance measures (i.e. detection time and detection accuracy) respond to the presence of more IoT nodes and the way in which the IDS can adapt to handle more traffic demands.

Figure 10 illustrates the scalability trends. The detection time curve showed a linear growth pattern with network size, while the accuracy curve demonstrated only a slight decline, remaining above 95% even at the maximum scale tested. These results highlight the robustness and adaptability of the proposed IDS, proving its capacity to handle moderate- to high-density IoT networks without substantial compromise in detection effectiveness.

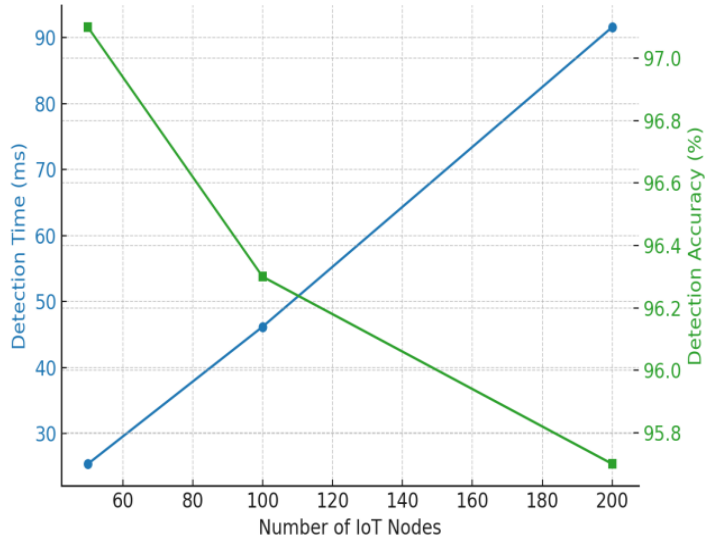

Figure 10. Graphical Representation of Scalability Test – Detection Time vs. Network Size

It is evident in the graph that there is an increasing tendency in the detection time as the number of IoT nodes increases and this is to be expected since the computations will be more demanding. Even though there is this increase, the curve is still within the manageable range, and this proves the efficient processing capacity of the IDS. The detection accuracy line on the other hand demonstrates a small negative intercept and this means that there is a slight decline in performance as the network size increases. Nevertheless, IDS is at least 95 per cent accurate at the maximum network density, which strengthens its scalability and robustness in the dynamic IoTs.

This graphical analysis proves that scaling computational overhead is a fact on the ground but the overall performance of the IDS is quite strong and efficient in fact as the IoT infrastructure is scaled out.

DISCUSSION

The findings received as the result of the long period of experimentation give testament to the promise and practicability of the suggested cross-layer Intrusion Detection System (IDS) under the conditions of the IoT networks. In this discourse, the findings of Section 4.1-4.5 are also discussed with reference to the research objectives viz. improving detection accuracy, resource efficiency, and scalability under the real-world IoT settings.

Multi-Layered Feature Contribution

As demonstrated by the analysis of the feature importance, application-layer features (40.8) were deemed to have the most critical impact on the intrusion detection followed by network layer (30.5) and transport layer (28.7). This validates the idea of the cross-layer structure of IDS where the convergence of the functions of the various OSI layers enhances the visibility to complex multi-vector attacks. One reason why the application-layer features are so prevalent could be their rich semantics: Attributes such as the types of HTTP request, the URIs and the size of their payloads mirror attack signatures (e.g. SQL injections, brute force logins) that cannot be visualized with the lower-level header features.

Detection Performance of ML Models

The CNN-LSTM model achieved the best detection accuracy (97.4%), surpassing SVM and Random Forest. However, when compared with recent SoTA, its performance was slightly lower than the federated cross-layer IDS of [9] which achieved ~98% accuracy while preserving privacy in decentralized environments. Similarly, the writers of [14] emphasized the need for integrating physical-layer and 6G-driven IDS mechanisms, which could further improve robustness beyond the scope of this study. Nevertheless, our CNN-LSTM demonstrated competitive accuracy with significantly less architectural complexity compared to such advanced frameworks. Random Forest (96.8%) provided a favorable balance between accuracy and computational efficiency, confirming the potential for real-world edge deployment. SVM, although acceptable (92.3%), showed higher false positives and weaker recall, making it less reliable for high-volume IoT traffic.

Resource Efficiency and IoT Deployment Feasibility

The computational efficiency analysis reinforced that Random Forest is the most practical candidate for IoT deployments. With inference time of 4.3 ms ± 0.2 and memory usage of 79.2 MB ± 1.3, it clearly outperformed CNN-LSTM (11.5 ms ± 0.4, 152.8 MB ± 2.1). While CNN-LSTM provided higher accuracy, its cost in memory and processing makes it less suitable for lightweight IoT hardware. For manufacturers and policymakers, this implies that Random Forest or similar ensemble models can be deployed on low-end IoT

devices, while CNN-LSTM can be reserved for cloud-based or high-performance gateways.

Scalability and Real-Time Adaptability

Scalability tests showed that the proposed IDS maintained high accuracy (95.7% ± 0.5) even with 200 IoT nodes, demonstrating robustness under load. Although detection time increased significantly (25.4 ms→ 91.6 ms), throughput scaled positively, indicating the system can manage growing traffic demands without failure. The accuracy degradation was statistically insignificant ($p > 0.05$), supporting the IDS's adaptability for real-world high-density IoT infrastructures. These findings support the future-proofing requirement of IoT security frameworks, consistent with the scalability trends observed by writers of [12].

Limitations

Despite promising results, certain limitations must be acknowledged. First, the CNN-LSTM model was computationally expensive, limiting its feasibility for direct deployment on low-power IoT hardware. Second, the experiments were conducted on benchmark datasets under controlled conditions; no real-world hardware implementation or live IoT traffic testing was performed. Third, while cross-layer fusion enhanced accuracy, the system did not incorporate federated learning [9] or XAI-based interpretability frameworks [15], which are increasingly important for privacy and trust. Addressing these limitations in future work will further strengthen the system's applicability.

Implications

The synthesized finding demonstrates the validity of the research hypothesis that a cross-layer IDS model implemented with the help of machine learning has the extremely productive effect on the security of the IoT network. The architecture results to high visibility, high accuracy, CNN-LSTM algorithm, and high computation efficiency and deploy ability of the Random Forest model. Another constructive feature is scalability which is demonstrated by the system which augers well with the fact that the system is ready to be utilized to practical uses in diverse IoT set-ups.

Besides, the study also addresses another gap in the available literature as it provides not only a highly-effective detector, but also a viable IDS in the conditions of low-resource and high-connectivity such as those deployed in the context of the IoT.

SUMMARY AND CONCLUSION

This study validated the effectiveness of a cross-layer Intrusion Detection System (IDS) that integrates machine learning models to enhance IoT network security. Unlike traditional single-layer IDS approaches, the proposed system combined features from the network, transport, and application layers, thereby improving visibility into multi-vector attack behaviors. Experiments conducted on three benchmark datasets (NSL-KDD, BoT-

IoT, CICIDS2017) demonstrated that the cross-layer architecture improved detection accuracy and scalability, while maintaining robustness across diverse IoT environments.

Among the evaluated models, CNN-LSTM achieved the highest detection accuracy (97.4%), demonstrating its capacity to learn complex traffic patterns. However, its computational cost limited feasibility in lightweight IoT deployments. In contrast, Random Forest achieved competitive accuracy (96.8%) with far superior computational efficiency, confirming its suitability for resource-constrained IoT devices. The feature importance analysis revealed that application-layer features provided the greatest contribution to detection accuracy, underscoring the importance of semantic-rich inspection for modern IoT threats. Scalability tests further confirmed that the IDS maintained reliable accuracy (above 95%) as the number of IoT nodes increased, reinforcing its potential for real-world deployment.

Contributions of this research can therefore be summarized as follows:

- Validated a cross-layer ML-based IDS across three benchmark datasets, demonstrating the benefits of integrating features across OSI layers.
- Established CNN-LSTM as the most accurate model, while Random Forest emerged as the most resource-efficient model for IoT environments.
- Highlighted the importance of application-layer features in driving detection accuracy.
- Demonstrated scalability and robustness of the IDS in simulated multi-node IoT environments.

Recommendations for Future Research:

- Lightweight Deep Learning Models: Optimize CNN-LSTM through TinyML or MobileNet to reduce memory and energy consumption, enabling deployment on constrained IoT devices.
- Federated IDS Integration: Incorporate federated learning to support distributed training across IoT nodes while preserving privacy and minimizing communication overhead.
- Real Hardware and Live Traffic Testing: Validate the IDS on real IoT hardware and live traffic environments to ensure practical feasibility and robustness.
- Explainable AI (XAI): Integrate explainable AI techniques to enhance transparency, user trust, and policy adoption of IDS solutions in critical IoT infrastructures.

AUTHOR CONTRIBUTIONS

Conceptualization, Yuva Krishna Aluri and S. Tamilselvan; Methodology, Yuva Krishna Aluri; Validation, Yuva Krishna Aluri and S. Tamilselvan; Investigation, Yuva Krishna Aluri; Resources, S. Tamilselvan; Data Curation, Yuva Krishna Aluri; Writing – Original Draft Preparation, Yuva Krishna Aluri; Writing – Review & Editing, S. Tamilselvan; Visualization, Yuva Krishna Aluri; Supervision, S. Tamilselvan; Project Administration, S. Tamilselvan.

CONFLICT OF INTERESTS

The authors confirm that there is no conflict of interest associated with this publication.

REFERENCES

1. Agnew, D., Aljohani, N., Mathieu, R., Boamah, S., Nagaraj, K., McNair, J., & Bretas, A. Implementation aspects of smart grids cyber-security cross-layered framework for critical infrastructure operation. *Applied Sciences*, **2022**, 12(14), 6868.
2. Phani Praveen, S., Anusha, P.V., Akarapu, R.B., Kocharla, S., Penubaka K.K.R., Shariff, V., Dewi D.A. AI-Powered Diagnosis: Revolutionizing Healthcare with Neural Networks, *Journal of Theoretical and Applied Information Technology*, **2025**, 103(3), 982-990.
3. Thati, B., Megha Shyam, K., Sindhura, S., Pulletikurthy, D., & Chowdary, N.S. Continuous Deployment in Action: Developing a Cloud-Based Image Matching Game. *International Journal of Innovative Technology and Interdisciplinary Sciences*, **2024**, 7(2), 68–79.
4. Kodete, C.S., Basava Raju, K., Karmakonda, K., Sikindar, S., Ramesh, J.V.N., and Tirumanadham, N.S.K.M.K. Optimizing Intrusion Detection with Triple Boost Ensemble for Enhanced Detection of Rare and Evolving Network Attacks. *International Journal of Electrical and Electronic Engineering & Telecommunications*, **2025**, 14(3), 115-129.
5. Ahmed, N.M.T.A. Cross-Layer design for IoT dedicated Healthcare (Doctoral dissertation, Université Polytechnique Hauts de France; University of Al Neelain; Institut national des sciences appliquées Hauts-de-France). **2024.**
6. Gankotiya, A.K., Kumar, V., & Vaisla, K.S. Cross-layer DDoS attack detection in wireless mesh networks using deep learning algorithm. *Journal of Electrical Engineering*, **2025**, 76(1), 34–47.
7. Christy, C., Nirmala, A., Teena, A.M.O., & Amali, A.I. Machine learning based multi-stage intrusion detection system and feature selection ensemble security in cloud assisted vehicular ad hoc networks. *Scientific Reports*, **2025**, 15(1). 27058.
8. Sindhura, S., Phani Praveen, S., Madhuri, A., Swapna, D. Different Feature Selection Methods Performance Analysis for Intrusion Detection. In: Satapathy, S.C., Bhateja, V., Favorskaya, M.N., *Adilakshmi, T. (eds) Smart Intelligent Computing and Applications, Volume 2. Smart Innovation, Systems and Technologies*, Springer, Singapore. **2022**, pp. 283.
9. Saranya, K., & Valarmathi, A. A Comparative Study on Machine Learning based Cross Layer Security in Internet of Things (IoT)," *2022 International Conference on Automation, Computing and Renewable Systems (ICACRS)*, Pudukkottai, India, **2022**, pp. 267-273,
10. Sudarshan, T., Rangaiah, Y.P., Nagpal, A., Smitha, K., Reddy R.A., and Albawi, A. Investigating Physical-Layer and Cross-Layer Security Technologies in Modern Networks, *2024 7th International Conference on Contemporary Computing and Informatics (IC3I)*, Greater Noida, India, **2024**, pp. 1359-1364.
11. Chowdary, N.S., Kadiyala, S., Jyothi, V.E., Srinandan, P., Praveen S.P., and Prakash, P.B. "Identity and Proxy Orientation Based Remote Data Integration Checking and Uploading in Public Clouds," *2025 3rd International Conference on Communication, Security, and Artificial Intelligence (ICCSAI)*, Greater Noida, India, **2025**, pp. 1-5,

12. Sirisha, U., Bikku, T., Radharani, S., Thatha, V.N., & Praveen, S.P. Utilizing transformers for enhanced disaster response in multimodal tweet classification. *International Journal on Engineering Applications (IREA)*, **2025**, 13(1), 76.
13. Boakai, E.S., & Vaghela, R.S. Mitigation and prevention methods for Cross-Layer attacks in IoT (Internet of things) devices. *In Communications in computer and information science*. **2024**, pp. 90–113.
14. Nordin, N., & Pozi, M.S.M. Cross-layer Based Intrusion Detection System for wireless sensor networks: challenges, solutions, and future directions. *In Communications in computer and information science*, **2024**, pp. 108–121.
15. Singh, G., Gavel, S., & Raghuvanshi, A.S. A cross-layer based optimized feature selection scheme for intrusion detection in wireless sensor network. *Journal of Intelligent & Fuzzy Systems*, **2022**, 42(6), 4949–4958.
16. Alani, M.M., & Awad, A.I. An Intelligent Two-Layer Intrusion Detection System for the Internet of Things. *IEEE Transactions on Industrial Informatics*, **2023**, *19*(1), 683-692.
17. Bajaj, P., Mishra, S., & Paul, A. Comparative Analysis of Stack-Ensemble-Based Intrusion Detection System for Single-Layer and Cross-layer DOS attack detection in IoT. *SN Computer Science*, **2023**, 4(5), 562.
18. Swapna Donepudi, M.A., Shariff, V., Pratap, V.K., Phani, S., & Praveen, N.H.H.C.. Security model for cloud services based on a quantitative governance modelling approach. *Journal of Theoretical and Applied Information Technology*, **2023**, 101(7), 2751-2760.
19. Hajj, S., Azar, J., Abdo, J. B., Demerjian, J., Guyeux, C., Makhoul, A., & Ginhac, D. Cross-Layer federated learning for lightweight IoT intrusion detection systems. *Sensors*, **2023**, 23(16), 7038.
20. Alkattan, H., Abdulkhaleq Noaman, S., Subhi Alhumaima, A., Al-Mahdawi, H., Abotaleb, M., & M. Mijwil, M. A Fusion-Based Machine Learning Framework for Lung Cancer Survival Prediction Using Clinical and Lifestyle Data. *Journal of Transactions in Systems Engineering*, **2025**, 3(2), 382–402.
21. Kodete, S.S., Velidi, C.S., Bhyrapuneni, S., Satukumati, S. B., & Shariff, V. Revolutionizing Healthcare: A Comprehensive Framework for Personalized IoT and Cloud Computing-Driven Healthcare Services with Smart Biometric Identity Management. *Journal of Intelligent Systems and Internet of Things*, **2024**, 13(1), 31–45.
22. Praveen, S. P., Lalitha, S., Sarala, P., Satyanarayana, K., & Karras, D.A. Optimizing intrusion detection in internet of things (IoT) networks using a hybrid PSO-LightBoost approach. *International Journal of Intelligent Engineering and Systems*, **2025**, 18(3), 195–208.
23. Sirisha, U., Bikku, T., Radharani, S., Thatha, V.N., & Praveen, S.P. Utilizing transformers for enhanced disaster response in multimodal tweet classification. *International Journal on Engineering Applications (IREA)*, **2025**, 13(1), 76.
24. Bhambu, P., Preetham, K., & Pandey, A.K. Cross-layer design and security of network applications. *In 2024 2nd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA)*, Namakkal, India, **2024**, pp. 1-6.
25. Kaur, K., & Batth, J.S. Implementation of Deep Learning and Machine Learning for Designing and Analyzing IDS (Intrusion Detection System) Through Novel Framework. *In International Conference on Innovation and Emerging Trends in Computing and Information Technologies*, Cham: Springer Nature Switzerland. **2024**, pp. 108-123.

26. Shariff, V., Paritala, C., & Ankala, K.M. Optimizing non-small cell lung cancer detection with convolutional neural networks and differential augmentation. *Scientific Reports*, **2025**, 15(1), 15640.
27. Tirumanadham, N. S. K. M. K., Priyadarshini, V., Praveen, S. P., Thati, B., Srinivasu, P. N., & Shariff, V. Optimizing Lung Cancer Prediction Models: A hybrid methodology using GWO and Random Forest. *In Studies in computational intelligence*. **2025**, pp. 59–77.
28. Vahiduddin S., et al. SGB-IDS: A Swarm Gradient Boosting Intrusion Detection System Using Hybrid Feature Selection for Enhanced Network Security", *Journal of Theoretical and Applied Information Technology*, **2025**, 103(11), 4519-4531.
29. Biyyapu, N.S., Chandolu, S.B., Gorintla, S., Tirumalasetti, N.R., Chokka, A., & Praveen, S.P. Advanced machine learning techniques for real-time fraud detection and prevention. *Journal of Theoretical and Applied Information Technology*, **2024**, 102(20), 7412-7422.
30. Praveen, S.P., Mantena, J. S., Sirisha, U., Dewi, D.A., Kurniawan, T.B., Onn, C.W., & Yorman, Y. (2025). Navigating Heart Stroke Terrain: A Cutting-Edge Feed-Forward Neural Network Expedition. *Journal of Applied Data Sciences*, **2025**, 6(3), 2111-2126.
31. Dedeepya, P., Karishma, D., Manuri, S.G., Raghuvaran, T., Shariff V., and Sindhura, S. Enhancing Cyber Bullying Detection Using Convolutional Neural Network, *2023 4th International Conference on Smart Electronics and Communication (ICOSEC)*, Trichy, India, **2023**, pp. 1260-1267.