Babylonian Journal of Networking
Vol.2025, **pp**. 116–125
DOI: https://doi.org/10.58496/BJN/2025/010; ISSN: 3006-5372
https://mesopotamian.press/journals/index.php/BJN

Research Article

Network-Based Intrusion Detection in IoT Environments Using Hybrid Machine Learning Techniques

Mansour Obeidat [1,*], Rami Shehab [1]

[1] *Applied College, King Faisal University, 31982, Al-Ahsa, Saudi Arabia*
[1] *Applied College, King Faisal University, 31982, Al-Ahsa, Saudi Arabia*

ARTICLE INFO

Article History
Received 3 Jul. 2025
Revised 20 Aug. 2025
Accepted 12 Sep. 2025
Published 23 Oct. 2025

Keywords
Intrusion Detection System (IDS),
IoT Security,
Hybrid Machine Learning,
NSL-KDD,
DS2OS,
IoT Botnet Datasets,
Support Vector Machine (SVM).

ABSTRACT

The recent proliferation of the Internet of Things (IoT) has emerged many security threats, especially on network-based communication platforms. With the increase of cyber-attacks against critical systems, in particular DDoS, e-fraud type or other, the demand for intelligent, adaptive IDS is clearly important. In this context, this paper proposes a hybrid machine learning model integrating traditional algorithms like Support Vector Machines (SVM) and emerging deep neural networks to improve the precision and robustness of detection in IoT systems. The performance of the proposed framework is tested on various benchmark datasets which includes NSL-KDD, DS2OS, and IoT Botnet using various performance parameters such as Accuracy, Precision, Recall, F1-score. The suggested approach yielded a high detection rate of 96.38%, indicating the capability of our system to pinpoint sophisticated intrusion instances on multi-type IoTNs. Experimental results demonstrate that the hybrid solution has the potential for false positives reduction as well as for enhancing response against the threat in real environment. This study is an attempt to bring cyber-security solutions for the emerging landscape of IoT infrastructures, which are scalable, adaptive networked based and intelligent.

1. INTRODUCTION

Internet of Things (IoT) and its deployment in critical infrastructures have been growing exponentially for the past decade increasing the threat landscape, especially with the increase in complex cyber-attacks against WSNs and WSN based distributed IoT systems [1-5]. Legacy security approaches—encryption, authentication and access control—are inadequate to detect sophisticated attacks, including zero- day attacks, in such dynamic and resource-constrained IoT environments [6-8].Artificial Intelligence (AI), in particular, using Machine Learning (ML) and Deep Learning (DL) techniques, has been recognized as a potential paradigm to strengthen cybersecurity [9]. Hybrid feature selection methods using a combination of entropy based mutual information feature selection with K-Means clustering result in efficient dimensionality reduction leading to computational cost reduction and better performance of intrusion detection models [10]. These methods are then succeeded by the use of classifiers such as Feedforward Deep Neural Networks (DNNs) which are able to learn intricate traffic features specific to intrusions with a good level of accuracy [11].Challenges including IoT scale, low latency, and varied device capability of IoT networks may also make IoT networks prone to attacks such as DDoS (Distributed Denial of Service), botnet spreading, unauthorized access, among others [8]. To tackle these problems, Support Vector Machines (SVMs) are extensively used because they are robust to binary classification tasks. Nevertheless, they are very sensitive to parameter settings, which may be tuned by means of metaheuristics like Particle Swarm Optimization (PSO) [12]. In this study we present a hybrid intrusion detection model based on machine learning and deep learning for protecting the IoT networks. Comparative analysis on several datasets (NSL-KDD, DS2OS, IoT Botnet) demonstrates the performance of the approach in terms of accuracy, precision, recall, and F1-score. By utilizing the intelligent detection mechanisms, the developed system will provide scalable and efficiency defense against IoT cyber threats [13].

*Corresponding author. Email: Mobaydat@kfu.edu.sa

2. LITERATURE REVIEW

Several other works have focused on various methods to improve IoT intrusion detection. In [14] a deep learning intrusion detection system (IDS) combined with explainable artificial intelligence (XAI) was introduced for enhancing model transparency in decision making. While the detection rate of their approach was high, it was computationally quite heavy. At [15] concentrated on IoMT and used machine learning algorithms to enhance IDS performance but could not adapt fast enough to changes in attack scenarios. At [16] proposed an edge-enabled industrial IoT network-specific IDS architecture using federated learning and blockchain, enhancing both security and latency. But scalability still was an issue. In [17] a proposal was made where a hybrid deep Q-network was proposed with optimizations that increased the detection rate and reduced false positives however it was computationally intensive. Study [18] investigated the use of generative AI and large language models in IoT security and summarized the new trends and opportunities it brings as well as the risks of over trusting in automatic decision-making systems. [19] covered the use of CNN and RNN architectures in IoT-IDS, emphasizing their high detection potential, but also noting their difficulty with interpretability and generalization from wide training data. In [20] we proposed DeepLG SecNet, an LSTM-GRU based model that greatly enhanced accuracy as well as detection speed in IoT networks, but it should be further optimized for large-scale deployment. Deep Residual Convolutional Neural Networks Have been applied for Anomaly Detection The studies [21,22] investigated deep residual convolutional neural network for anomaly detection, it has produced robust results but with high computational and preprocessing requirements. In [23], have proposed a hybrid model of VGG19 and 2D-CNN for the detection of intrusions in fog–cloud environments, the results of which were better in terms of robustness and detection rate. However, the model had a trade-off between performance and real time. Last but not the least, [24] introduced the Flow Transformer an transformer based structure for flow-based intrusion detection. Their approach showed better scalability and accuracy, but further validation in heterogeneous IoT environments was suggested.

2.1 Super Vector Machine (SVM)

SVM is a very powerful algorithm in supervised learning that was introduced by Vapnik et al. in the late 90's and it has been widely used to learn the general power form. It was a concept which was at the root of the neural Networks and could be regarded as the mathematical generalization of the early neural learning models. It is well-known that SVMs can be employed to solve linear and non-linear classification problems by mapping the input data into a high-dimensional space and finding an optimal separating hyperplane [25-31]. As shown in Figure 1, the decision region (hyperplane) between two classes is decided based on the margin of distance and the SVM determines the decision region (hyperplane) which has the widest distance. This margin-causing optimization technique tends to improve generalization on unseen data. The idea of the algorithm is to find N-dimensional plane as the hyperplane that this is optimal in a sense to split the data points based on the class they belongs to.

Mathematically, this is formulated as a convex optimization problem:

$$\min_w \lambda \|w\|^2 + \sum_{i=1}^{n} (1 - y_i \langle x_i, w \rangle) \quad (1)$$

The partial derivative with respect to the *k*-th component of the weight vector is:

$$\frac{\delta}{\delta w_k} \lambda \|w\|^2 = 2\lambda w_k \quad (2)$$

The hinge loss derivative condition is defined as:

$$\frac{\delta}{\delta w_k} (1 y_i \langle x_i, w \rangle)_+ = \begin{cases} 0, & \text{if} y_i \langle x_i, w \rangle \geq 1 \\ -y_i x_{ik}, & \text{else} \end{cases} \quad (3)$$

The objective is to maximize the margin—the distance between the hyperplane and the closest data points from either class. This ensures not only better separation but also improved reliability when classifying unseen instances.

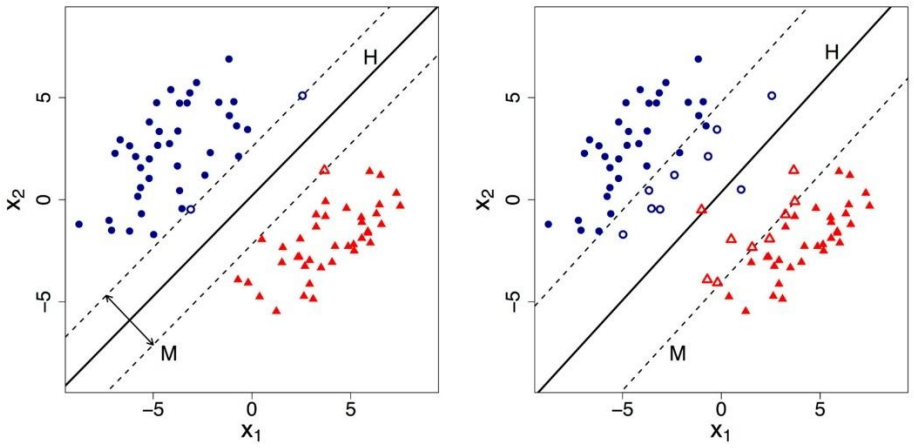

FIG. 1. SVM CONCEPT SHOWING CLASSIFICATION BOUNDARY AND CLASS SEPARATION.

2.2 Hyperplanes and support vectors

SVMs use hyperplanes, the fundamental elements in the mathematics of classifiers, in order to distinguish data into different classes. The hyperplane's dimensionality varies according to the input features. For instance:

a) When we have two features as input, the hyperplane can be represented as a straight line, which is a 2D.
b) with three properties it is reduced to a 2D plane (3D),
c) In coordinate space in the case of higher dimensions, this is a hyperplane which we can't really picture directly; see Figure 2.

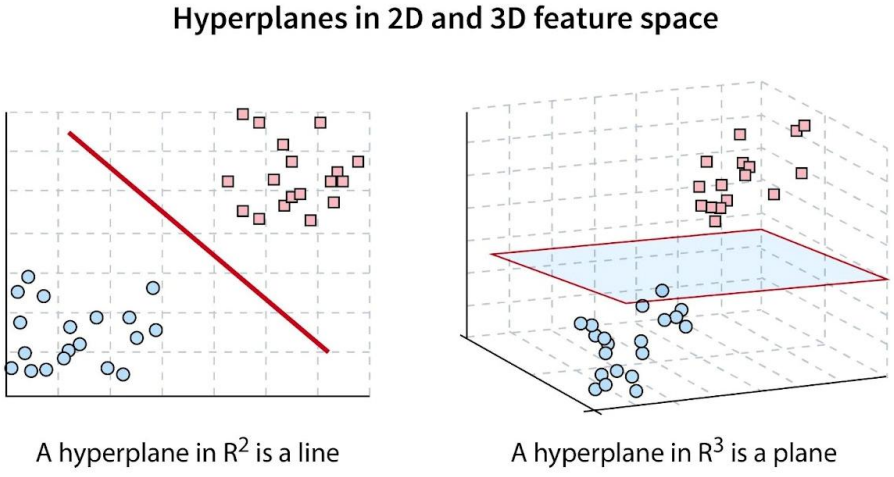

FIG. 2. GEOMETRIC REPRESENTATION OF SVM HYPERPLANES IN 2D AND 3D.

Support vectors are the important subset of the points closest to the decision boundary. They are very important to determine the position and rotation of the hyperplane. If we delete those points, we will move the hyperplane and directly assert their impact to model. Support vector can be accounted as arguments to the delta function (Class II functions, which is in the margin of the corresponding hyperplane). This is a generalization of the maximal margin criterion is shown in Figure 3.

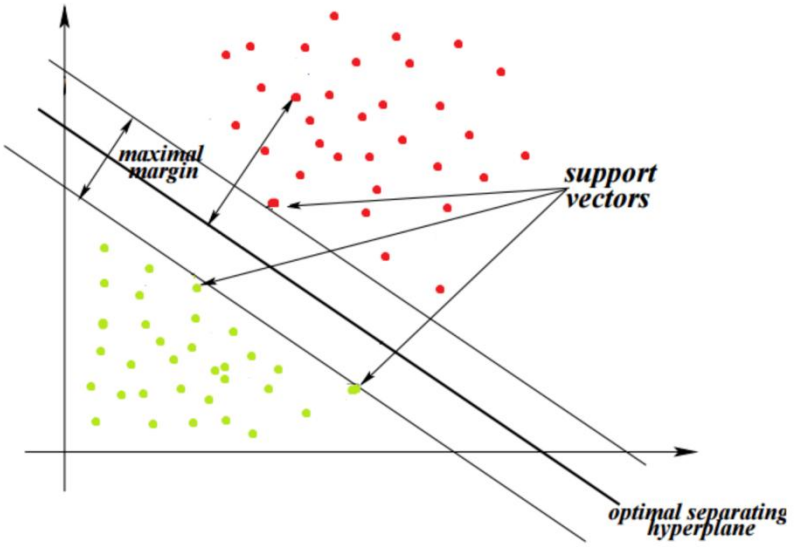

FIG. 3. SUPPORT VECTORS AND THEIR RELATIONSHIP TO THE HYPERPLANE.

These mathematical and geometric principles form the basis for deploying SVM in various intrusion detection scenarios, particularly in Internet of Things (IoT) networks, where distinguishing between normal and malicious traffic is essential.

3. METHODOLOGY

We propose a hybrid and dual-layered IDS specifically designed for the characteristic aspect of IoT network environment. This hybrid approach consists of signature detection in the first layer in combination with anomaly detection, implemented through supervised machine learning in a second layer, and aims to provide both fast and adjustable protection mechanisms against known and novel threats. A schematic of the proposed structure is shown in Figure 4.

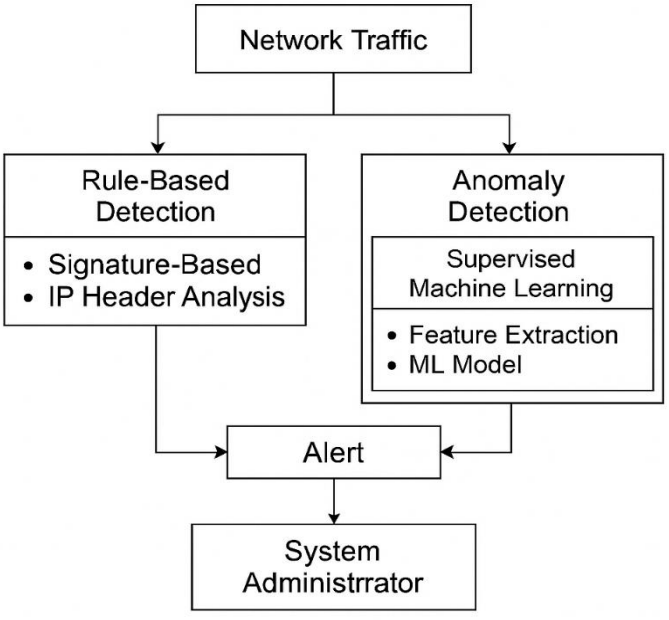

FIG. 4. PROPOSED HYBRID IDS ARCHITECTURE WITH MACHINE LEARNING.

3.1 Signature-Based Detection Layer

The first one acts as RB-IDS. It utilizes a database of known bad IP addresses, domain generation algorithms (DGAs), spam patterns and malware signatures from trusted sources such as the DShield Block List, ATLAS (Arbor Networks), and the Spam Haus DROP (Don't Route or Peer) list. ndb, foxhole. cdb, and junk. db. The incoming traffic packets are divided into IP headers and content payloads. These are checked against the signature repositories. Upon matching, an alert is raised, the packet is flagged as malicious and the user is notified in real time. Non-malicious traffic is sent to tier 2 for additional processing. The packet filtering is done in promiscuous mode where all packets are captured on the network interface by jNetPcap or cascading/httpcap. It dissects them to retrieve issues such as addresses, ports, protocol and content. This is described in Figure 5. As shown here Figure 6 After the header is removed from it, it is compared with known attack signatures.

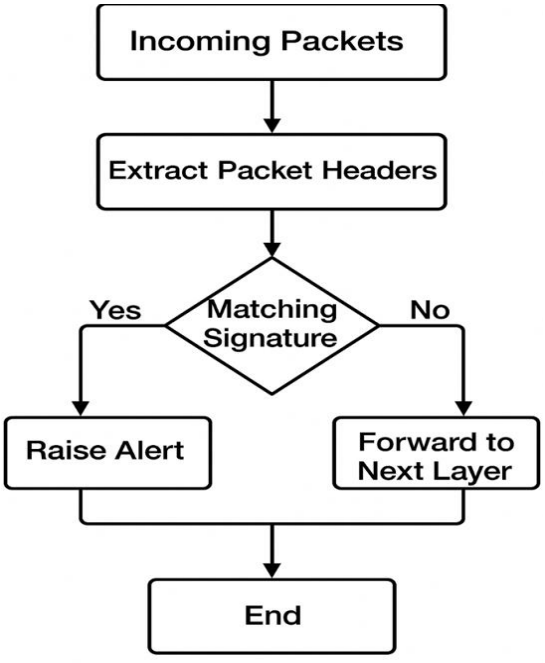

FIG. 5. PACKET FILTERING MODULE FOR SIGNATURE MATCHING.

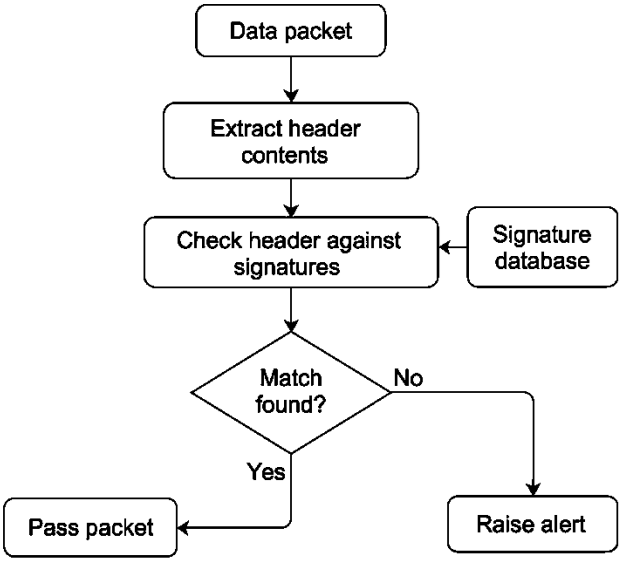

FIG. 6. SIGNATURE-BASED INTRUSION DETECTION LOGIC.

3.2 Anomaly-Based Detection Layer

The next detection layer uses machine learning (ML) to recognize network traffic irregularities, which are inconsistent with predefined signatures. This layer improves zero-day and novel attack detection by taking advantage of trained models.Training is performed on labeled packet data sets. Data is preprocessed in feature vectors, and then models are trained with algorithms such as Support Vector Machine (SVM) that make a decision according to whether data exceeds a threshold value. After the hidden layer we also employ a sigmoid function to map the predictions to a value between -1 and 1:

a) If output ≥ 0.5 that means the packet is an anomaly (attack).
b) If the output < 0.5 we consider the packet benign.

Threshold tuning is critical:

a) A small threshold of 0.3 decreases false positives but could also lead to worse missed attack.
b) A high threshold (e.g., 0.7) is prone to produce more false alarms as it captures more threats.

The anomaly detection process is illustrated in Fig 7.

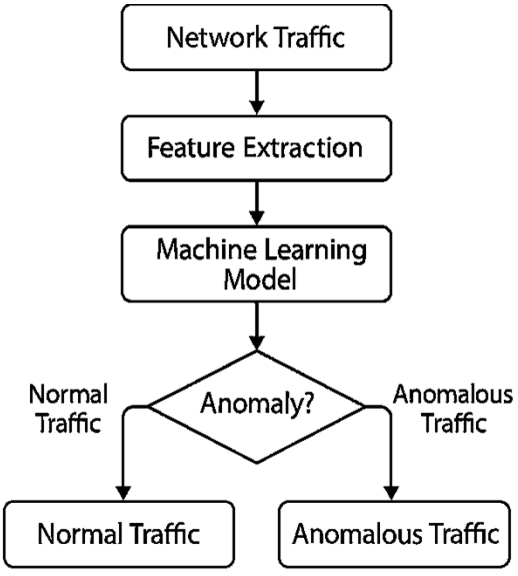

FIG. 7 ANOMALY-BASED INTRUSION DETECTION USING MACHINE LEARNING.

3.3 IOT Network Model

The IDS deployment in IoT environments faces constraints such as limited battery life, low processing power, and intermittent node activity. To address these, the proposed system integrates lightweight detection agents on edge devices that monitor both local and neighbor traffic. These agents report anomalies to a base station, which consolidates and alerts the administrator. This model ensures adaptive, energy-efficient, and distributed intrusion detection. Table 1 present summary of IoT network constraints and IDS design solutions.

TABLE I: SUMMARY OF IOT NETWORK CONSTRAINTS AND IDS DESIGN SOLUTIONS

Constraint	Impact	IDS Design Solution
Limited battery capacity	Restricts continuous processing	Energy-aware adaptive IDS operation
Low processing power	Hinders real-time deep analytics	Lightweight detection at the edge
Intermittent node availability	Nodes may sleep or disconnect	Dynamic monitoring based on node status
Decentralized environment	Hard to track distributed threats	Local detection agents with central alert aggregation
Need for contextual awareness	Incomplete view of threats	Use of neighbor knowledge and internal alert metadata

Using a dynamic Intrusion Detection System (IDS) deployed on the IoT network edge-devices. A Detection Agent is deployed at each edge node to monitor local traffic and detect anomalies. If anomalies exist, indicated by "#" alerts are sent to both Base Station and the End-Edge Anomaly Detection Center and the End-Edge Anomaly Detection Center sends these alerts to the System Administrator. For power consumption savings, all the idle nodes go to sleep mode and to wake-up mode during traffic flow. This distributed and adaptive model helps lowering the communication overhead and enables

timely containment and local detection of malicious security threats in resource limited IoT environments. In the figure 8 effect of energy aware node behavior, centralized alert detection and edge-based anomaly monitoring in lightweight detection architecture is depicted.

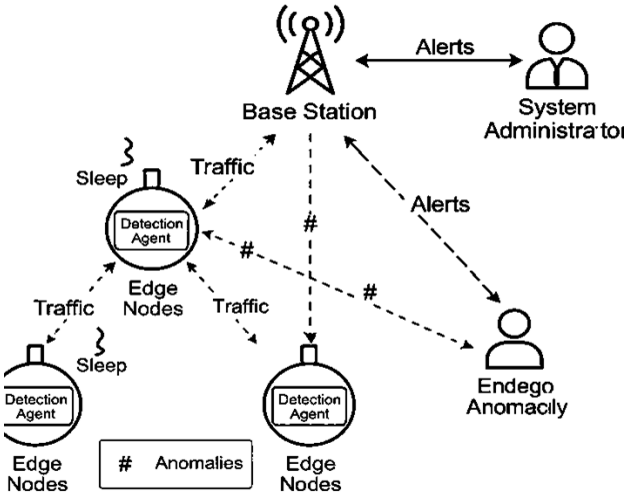

FIG. 8. ADAPTIVE IDS DEPLOYMENT IN IOT NETWORK.

4. EXPERIMENTAL RESULT

Experiments MDSymblo'18 [82] proposed the AI-based hybrid intrusion detection system which combines the machine learning model and the neural network to detect the intrusion on the IoT environment was validated by extensive experimental studies on the NSL-KDD dataset. Various performance metrics, including accuracy, detection rate, false positive rate, and system scalability, were used to evaluate the performance of the presented IDS. This section describes the details of the dataset, the features employed, the evaluation measures, and the compared methods.

4.1 NSL-KDD Dataset

The NSL-KDD dataset is the popular dataset for IDS benchmark, which includes 42 features in each connection record, including the label for either an attack or normal. Types of attack are divided according to the protocol they exploit (ICMP, UDP, TCP).

Table 2: Classification of the attack types included in the NSLKDD dataset, given upon the underlying transport protocol (ICMP, UDP, TCP). The classification contributes to the understanding of the distribution of threats and protocol related vulnerabilities underlying the dataset.

TABLE II. CATEGORIZED ATTACK TYPES IN NSL-KDD DATASET

Protocol	Attack Types
ICMP	Normal, Smurf, Satan, Pod, Ipsweep, Nmap, Portsweep
UDP	Teardrop, Rootkit, Nmap, Satan
TCP	Neptune, Guess Passwd, Perl, Land, Ipsweep, Buffer Overflow, FTP Write, etc.

The dataset features are categorized into different sets, summarized in the tables below to reflect connection, content, and time-based characteristics.

4.2 Feature Set Description

Table 3 summarizes the basic connection-level features extracted from each record in the dataset. These features represent general information about the network connection such as protocol type and connection duration.

TABLE III. BASIC CONNECTION FEATURES

Feature No.	Feature Name	Description	Sample
1	Duration	Connection length	0
2	Protocol Type	Type of network protocol (e.g., TCP/UDP)	UDP
3	Service	Network service accessed	data
4	Flag	Connection status flag	SF

Table 4 highlights features related to traffic volume and packet structure. These features are essential for identifying unusual patterns in data transmission, which could indicate network misuse or DoS attacks.

TABLE IV. TRAFFIC VOLUME FEATURES

Feature No.	Feature Name	Description	Sample
5	Source Bytes	Bytes sent from source	700
6	Destination Bytes	Bytes sent to destination	30
7	Land Attack Flag	1 if land attack; else 0	1
8	Wrong Fragment Count	Invalid or broken fragments	0
9	Urgent Packets	Urgent control flags	0

Table 5 presents content-based features that examine the payload of connections, such as login attempts and shell accesses. These indicators are particularly useful for identifying application-layer attacks or unauthorized system access.

TABLE V. CONTENT-BASED FEATURES

Feature No.	Feature Name	Description	Sample
10	Hot Indicators	Number of "hot" indicators	0
11	Failed Logins	Count of failed login attempts	1
12	Logged In	1 if successfully logged in; else 0	0

Table 6 outlines time-based statistical features that describe host behavior over short time windows. These attributes are crucial for detecting scanning, probing, or brute-force attempts across time-dependent patterns.

TABLE VI. TIME-BASED FEATURES

Feature No.	Feature Name	Description	Sample
32	Host Count	Count of connections from same destination IP	400
33	Destination Host Port Count	Number of connections from same port	64
36	Same Service Rate	Percentage using same service	0.36
40	Rerror Rate	Error rate triggered by REJ flag	1.07

4.3 Evaluation Metrics for IDS

The following descriptive indicators were used in lieu to assess the IDS performance. Table 7 shows the primary evaluation metrics for testing IDS performance. These are — cost, detection rate, the ability to scale, and robustness —Which are holistic with respect to feasibility and performance of the system in the real-world IoT scenarios.

TABLE VII. KEY IDS PERFORMANCE METRICS

Metric	Description
Cost	Evaluated based on detection resource usage, system response, and downtime
Detection Rate	Measures correct identification of attacks vs. missed threats
Scalability	Ability to handle growing traffic and user load
Resilience	Adaptability to evolving attack patterns and signature updates

4.4 Comparative Performance Evaluation

The proposed hybrid AI-based IDS was compared with the recent studies. In Figure 9 we compare the accuracy of our proposed IDS with a few recent state-of-the-art intrusion detection models. These results present the effectiveness of hybrid method over IoT networks.

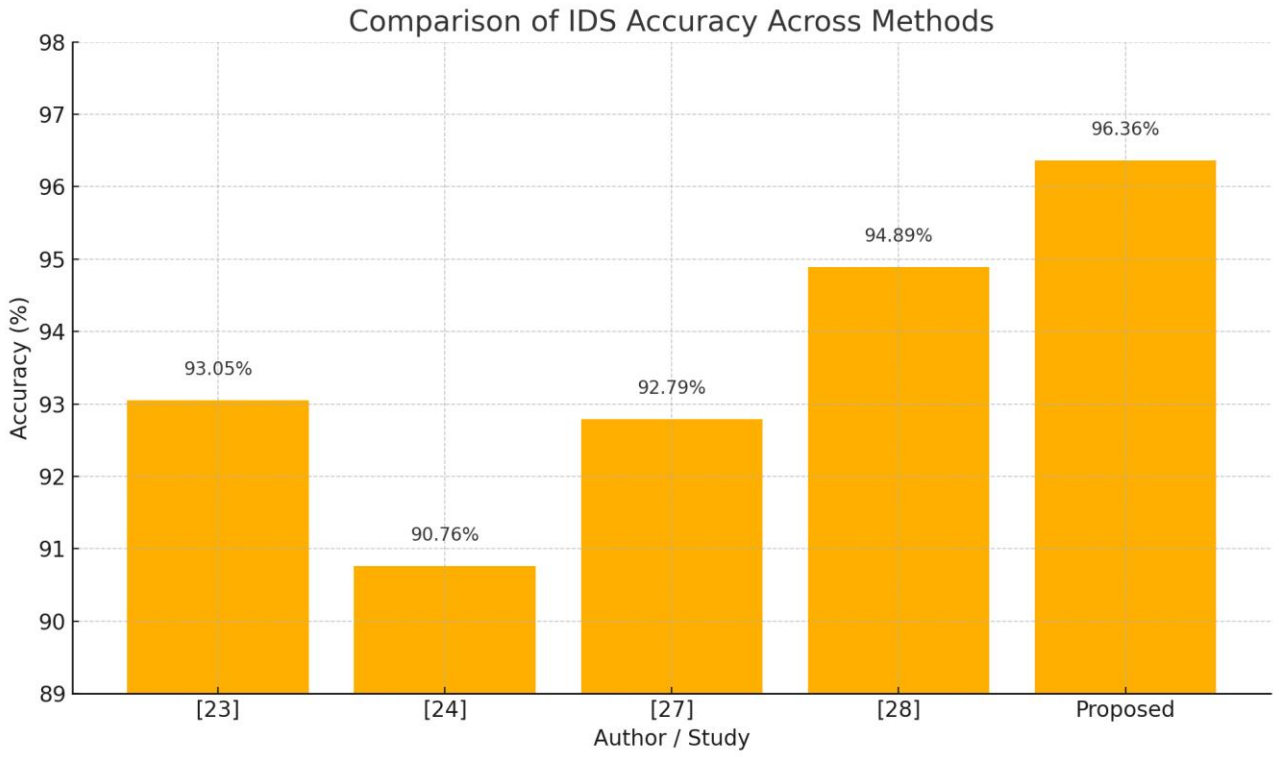

FIG. 9. ACCURACY COMPARISON WITH EXISTING APPROACHES

The proposed Intrusion Detection System (IDS) achieved a high detection accuracy of 96.36%, surpassing the performance of other state-of-the-art systems. It maintained a low false positive rate while ensuring comprehensive detection coverage, which is essential for minimizing alert fatigue and enhancing system reliability. Furthermore, the system demonstrated adaptability and energy efficiency, making it particularly suitable for deployment in resource-constrained IoT environments. The hybrid design, which integrates both signature-based and anomaly-based detection techniques, contributed to improved robustness and the ability to detect both known and emerging threats effectively.

5 CONCLUSION

While the fields of computer science and information technology have been growing rapidly, there has been growing interest in the security aspects of interconnected devices (IoT devices in particular). The growing dependence of business, society and everyday life on network systems creates a demand for effective and flexible Intrusion Detection Systems (IDS). This research has suggested a hybrid IDS model for higher detection and prevention of cyber-attacks in IoT networks by blending Edgar C. Merwyn based Machine learning and Long-term short-term memory based convolutional neural network methodology. Experiment results from NSL-KDD data set show that the proposed method can achieve a high detection accuracy of 96.36% with a low false positive rate and has good adaptability to dynamic IoT environments. It was particularly the combination of SVMs and optimization schemes like PSO that allowed for effective tuning parameters to enhance classification. Secondly, incremental SVM training provided the model with the capability to accommodate ongoing variations in network patterns through the incremental update of support vectors according to the KKT conditions. The advantage of the hybrid model is that it combines the advantages of signature-based and anomaly-based detection, and can detect known and new attacks. Its distributed nature and energy-aware design also facilitate rollout in resource-constrained IoT environments. In summary, the AI-based IDS architecture to IoT security considerations is a powerful and scalable memory model and logical method, which would be a promising route in the future real-world implementation for deployment in emerging smart networks.

Conflicts of Interest

Author declare no conflicts of interest.

Funding

Author, declare they have received no funding for this paper.

Acknowledgment

Non.

References

[1] A. A. Megantara and T. Ahmad, 'A hybrid machine learning method for increasing the performance of network intrusion detection systems,' Journal of Big Data, vol. 8, no. 1, pp. 1–19, 2023.
[2] G. Perumal, G. Subburayalu, Q. Abbas, S. M. Naqi, and I. Qureshi, 'VBQ-Net: A novel vectorization-based boost quantized network model for maximizing the security level of IoT system to prevent intrusions,' Systems, vol. 11, no. 8, p. 436, 2023.
[3] A. Mahalingam, G. Perumal, G. Subburayalu, M. Albathan, A. Altameem, R. S. Almakki, and Q. Abbas, 'ROAST-IoT: A novel range-optimized attention convolutional scattered technique for intrusion detection in IoT networks,' Sensors, vol. 23, no. 19, p. 8044, 2023.
[4] H. Liao et al., 'A survey of deep learning technologies for intrusion detection in Internet of Things,' IEEE Access, 2024.
[5] K. DeMedeiros, A. Hendawi, and M. Alvarez, 'A survey of AI-based anomaly detection in IoT and sensor networks,' Sensors, vol. 23, no. 3, p. 1352, 2023.
[6] M. Markevych and M. Dawson, 'A review of enhancing intrusion detection systems for cybersecurity using artificial intelligence (AI),' in Proc. Int. Conf. Knowledge-Based Organization, vol. 29, no. 3, pp. 30–37, 2023.
[7] M. Amin et al., 'Cyber security and beyond: Detecting malware and concept drift in AI-based sensor data streams using statistical techniques,' Computers and Electrical Engineering, vol. 108, p. 108702, 2023.
[8] A. Kathirvel and C. P. Maheswaran, 'Enhanced AI-based intrusion detection and response system for WSN,' in Artificial Intelligence for Intrusion Detection Systems, pp. 155–177, Chapman and Hall/CRC, 2023.
[9] R. L. D. Moura, V. N. Franqueira, and G. Pessin, 'Cybersecurity in industrial networks: Artificial intelligence techniques applied to intrusion detection systems,' 2023.
[10] M. Tubishat, F. Al-Obeidat, A. S. Sadiq, and S. Mirjalili, 'An improved dandelion optimizer algorithm for spam detection: Next-generation email filtering system,' Computers, vol. 12, no. 10, p. 196, 2023.
[11] H. J. Shiu, C. T. Yang, Y. R. Tsai, W. C. Lin, and C. M. Lai, 'Maintaining secure level on symmetric encryption under quantum attack,' Applied Sciences, vol. 13, no. 11, p. 6734, 2023.
[12] F. Gatica-Neira, P. Galdames-Sepulveda, and M. Ramos-Maldonado, 'Adoption of cybersecurity in the Chilean manufacturing sector: A first analytical proposal,' IEEE Access, vol. 11, pp. 133475–133489, 2023.
[13] E. Debas, N. Alhumam, and K. Riad, 'Unveiling the dynamic landscape of malware sandboxing: A comprehensive review,' 2023.
[14] K. N. H. De Silva et al., 'Realtime network-based anomaly detection and malware analysis for SMEs and smart homes,' Int. Res. J. Innovations Eng. Technol., vol. 7, no. 10, pp. 249–255, 2023.
[15] M. M. Saeed et al., 'Machine learning techniques for detecting DDoS attacks,' in Proc. 3rd Int. Conf. Emerging Smart Technologies and Applications (eSmarTA), pp. 1–6, IEEE, Oct. 2023.
[16] S. Sheeja and J. Joseph, 'A three-layer convolution neural network approach for intrusion detection in IoT,' in Proc. 11th Int. Conf. Intelligent Computing and Information Systems (ICICIS), pp. 261–268, IEEE, Nov. 2023.
[17] O. G. Abdulateef, A. Joudah, M. G. Abdulsahib, and H. Alrammahi, 'Designing a robust machine learning-based framework for secure data transmission in Internet of Things (IoT) environments: A multifaceted approach to security challenges,' J. Cyber Security and Risk Auditing, vol. 2025, no. 4, pp. 266–275, 2025.
[18] S. A. M. Al-Rubaye, 'Intrusion detection system in IoT networks using SVM-PSO classification,' M.S. thesis, Altınbaş Univ., Inst. of Graduate Studies, 2022.
[19] B. Sharma, L. Sharma, C. Lal, and S. Roy, 'Anomaly based network intrusion detection for IoT attacks using deep learning technique,' Computers and Electrical Engineering, vol. 107, p. 108626, 2023.
[20] A. Verma and V. Ranga, 'On evaluation of network intrusion detection systems: Statistical analysis of KDDS-001 dataset using machine learning techniques,' Authorea Preprints, 2023.
[21] M. Al-Olaqi, A. Al-Gailani, and M. M. H. Rahman, 'Comprehensive study of SQL injection attacks mitigation methods and future directions,' J. Cyber Security and Risk Auditing, vol. 2025, no. 4, pp. 347–365, 2025.
[22] B. Sharma, L. Sharma, C. Lal, and S. Roy, 'Explainable artificial intelligence for intrusion detection in IoT networks: A deep learning based approach,' Expert Systems with Applications, vol. 238, p. 121751, 2024.
[23] M. A. Al-Shareeda, L. B. Najm, A. A. Hassan, S. Mushtaq, and H. A. Ali, 'Secure IoT-based smart agriculture system using wireless sensor networks for remote environmental monitoring,' STAP J. Security Risk Management, vol. 2024, no. 1, pp. 56–66, 2024.
[24] Z. Sun, G. An, Y. Yang, and Y. Liu, 'Optimized machine learning enabled intrusion detection system for Internet of Medical Things,' Franklin Open, vol. 6, p. 100056, 2024.

[25] S. Alsahaim and M. Maayah, 'Analyzing cybersecurity threats on mobile phones,' STAP J. Security Risk Management, vol. 2023, no. 1, pp. 3–19, 2023.
[26] S. Ali, Q. Li, and A. Yousafzai, 'Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: A survey,' Ad Hoc Networks, vol. 152, p. 103320, 2024.
[27] M. Alshinwan, A. G. Memon, M. C. Ghanem, and M. Almaayah, 'Unsupervised text feature selection approach based on improved Prairie Dog algorithm for text clustering,' Jordanian Journal of Informatics and Computing, vol. 2025, no. 1, pp. 27–36, 2025.
[28] G. S. R. Emil Selvan, T. Daniya, J. P. Ananth, and K. S. Kumar, 'Network intrusion detection and mitigation using hybrid optimization integrated deep Q network,' Cybernetics and Systems, vol. 55, no. 1, pp. 107–123, 2024.
[29] F. Alwahedi, A. Aldhaheri, M. A. Ferrag, A. Battah, and N. Tihanyi, 'Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models,' Internet of Things and Cyber-Physical Systems, 2024.
[30] S. R. Addula, S. Norozpour, and M. Amin, 'Risk assessment for identifying threats, vulnerabilities and countermeasures in cloud computing,' Jordanian Journal of Informatics and Computing, vol. 2025, no. 1, pp. 38–48, 2025.