ISSN: 2581-3404 (Online) **IF: 5.86 (SJIF)**

IJIRTM, Volume-10, Issue-4, July-2026

Intrusion Detection System based on Machine Learning and Deep Learning Model

Ankit Gupta[1], Dr. Harsh Mathur[2]

Research Scholar[1], Head & Associate Professor[2]

Department of Computer Science & Engineering[1,2]

Rabindranath Tagore University, Raisen, India[1,2]

ankit1989chitrakoot@gmail.com [1], harsh.mathur@rntu.ac.in [2]

Abstract. *The exponential growth of cloud computing, Internet of Things (IoT), Industrial Internet of Things (IIoT), edge computing, and intelligent networking has significantly increased the frequency and complexity of cyber-attacks. Traditional signature-based Intrusion Detection Systems (IDS) are often ineffective against zero-day attacks, polymorphic malware, and sophisticated network intrusions due to their dependence on predefined attack signatures and limited adaptability. Consequently, Machine Learning (ML) and Deep Learning (DL) techniques have emerged as promising solutions for intelligent intrusion detection by automatically learning network traffic patterns and identifying malicious activities. This literature survey critically reviews recent advances in ML- and DL-based intrusion detection systems, compares existing methodologies using standard performance metrics such as Accuracy, Precision, Recall, F1-score, False Positive Rate (FPR), False Negative Rate (FNR), Area Under the Curve (AUC), and Detection Rate (DR), and identifies current research gaps. This research work presents, comparative study for intrusion detection system using ML-DL based approaches, and also provides valuable insights for designing next-generation intelligent, scalable, explainable, and lightweight intrusion detection systems suitable for modern cloud, IoT, and edge computing environments.*

Keywords: Machine learning, Network security, Deep learning, Intrusion detection system, Cyber-attacks.

Introduction

The rapid expansion of digital communication, cloud computing, Internet of Things (IoT), Industrial Internet of Things (IIoT), edge computing, fifth-generation (5G) communication, and artificial intelligence has transformed modern network infrastructures into highly interconnected and intelligent ecosystems. A network intrusion refers to any unauthorized activity that attempts to compromise the confidentiality, integrity, or availability of computer systems, communication networks, or digital resources. Intrusions may involve unauthorized access, privilege escalation, malware installation, data theft, denial-of-service attacks, ransomware deployment, botnet propagation, phishing, reconnaissance, spoofing, or advanced persistent threats (APTs). These attacks are becoming increasingly sophisticated because attackers continuously modify their attack strategies to evade conventional security mechanisms.

Traditional network security mechanisms such as firewalls, antivirus software, and signature-based intrusion detection systems primarily rely on predefined attack signatures and manually crafted security

rules. Although these methods remain effective against previously known attacks, they often fail to identify zero-day attacks, polymorphic malware, encrypted attacks, insider threats, and continuously evolving cyber threats. As network traffic grows exponentially due to cloud services and IoT devices, manually updating signature databases becomes increasingly impractical. These limitations have encouraged researchers to investigate intelligent intrusion detection systems capable of automatically learning network behavior and detecting both known and unknown attacks with high accuracy. Machine Learning (ML) has emerged as a promising solution by enabling computers to identify attack patterns directly from historical network traffic without relying exclusively on predefined rules. Overall, network intrusion detection has evolved from simple rule-based monitoring systems into intelligent, adaptive, explainable, and autonomous security frameworks capable of protecting modern communication infrastructures against highly dynamic cyber threats.

Need of Intrusion Detection System

The continuously increasing sophistication of cyberattacks has made real-time intrusion detection an essential requirement for modern cybersecurity systems. Unlike traditional offline analysis, real-time intrusion detection continuously monitors network traffic as it flows through communication channels and immediately identifies suspicious activities before attackers can compromise critical resources. Modern enterprises, financial institutions, healthcare organizations, government agencies, smart cities, industrial control systems, cloud platforms, and IoT environments require uninterrupted services where even a few seconds of delayed attack detection may result in severe financial losses, operational disruption, privacy violations, or national security risks.

The emergence of IoT and IIoT has dramatically increased the number of interconnected devices generating massive volumes of heterogeneous network traffic. These resource-constrained devices often possess limited computational power and minimal built-in security mechanisms, making them attractive targets for attackers. Consequently, intrusion detection systems deployed in such environments must provide rapid detection with low computational overhead while maintaining high detection accuracy. Several recent studies emphasize lightweight deep learning architectures and compressed neural network models specifically designed for edge computing and IoT environments.

Intrusion detection is equally important for mitigating Distributed Denial of Service (DDoS), botnet propagation, ransomware, brute-force attacks, SQL injection, spoofing, phishing, and insider attacks. Early detection allows security administrators to isolate compromised systems, block malicious traffic, update firewall policies, revoke unauthorized access, and initiate automated incident response before significant damage occurs. Energy-efficient deep learning models employing knowledge distillation, quantization, model compression, and adaptive feature selection significantly reduce inference time while preserving high detection accuracy. These approaches enable deployment of intelligent IDS solutions directly on edge devices without requiring continuous communication with centralized cloud servers.

Modern research also recognizes that high detection accuracy alone is insufficient for practical cyber-security applications. Security analysts require transparent and interpretable models capable of explaining why a network flow is classified as malicious. Explainable AI techniques therefore play an increasingly important role by identifying influential features and improving trust in automated intrusion detection decisions. Similarly, optimization algorithms improve feature selection and hyper-parameter tuning, reducing computational complexity while increasing classification performance.

Although considerable progress has been achieved, several research challenges remain unresolved. Existing intrusion detection systems continue to suffer from class imbalance, adversarial attacks, high computational requirements, encrypted traffic analysis, poor generalization to unseen attacks, and scalability issues in large-scale cloud and IoT environments. Therefore, future intrusion detection systems should integrate optimization algorithms, explainable artificial intelligence, lightweight deep learning architectures, ensemble learning, machine learning and adaptive online learning mechanisms to provide highly accurate, scalable, interpretable, and real-time cyber-security solutions suitable for next-generation intelligent networks.

Literature Review

Table 1: comparative study for intrusion detection system suing machine learning and deep learning model.

Year	Author	Technique / Model	Performance Parameters	Major Findings
2024	Mohammed Mynuddin et al.	ML + DL Hybrid IDS	Accuracy, FPR	Improved detection with reduced false alarms
2025	Ramya Chinnasamy et al.	HBO + ANN	Accuracy, Precision, Recall, FAR	Feature optimization improves IDS performance
2025	Mohale et al.	XGBoost + XAI	Accuracy , FPR, FNR	Explainable intrusion detection
2025	Tamara Al-Shurbaji et al.	DL Survey	Review	Identified future DL challenges
2025	Muhanna Ahmed Ali et al.	RF, LSTM, SVM	Accuracy	RF performed best
2025	Farhan et al.	Sequential DNN + Extra Tree	Accuracy, Precision, Recall,	Optimized feature selection
2025	Manivannan et al.	ARNN + FOX	Accuracy, Precision, Recall, Specificity	FOX optimization improved IDS
2025	Dash et al.	SSA-LSTM	Accuracy, ROC, Precision, Recall	SSA optimization superior
2025	Wang et al.	BS-GAT	Accuracy , F1-score	Graph neural network enhanced detection
2025	Umar et al.	DNN-KDQ	Accuracy, Latency	Edge-computing IDS
2025	Yang et al.	BERT + GRU	Accuracy, Precision, Recall	Transformer-based IDS
2025	Hossain	CNN, LSTM, RNN	Accuracy	CNN achieved best performance

2025	Srinivasan et al.	CNN + Blockchain + RL	Accuracy, FPR	Integrated detection and prevention
2025	Ahmed et al.	ML + DL + Fuzzy Clustering	Accuracy, Precision, Recall	Hybrid IDS improved security
2025	Zhao et al.	Improved MLP	F1-score, Accuracy	Improved minority attack detection

Recent advancements in cybersecurity have accelerated the development of intelligent Intrusion Detection Systems (IDS) capable of identifying increasingly sophisticated cyber threats. Mohammed Mynuddin et al. (2024) proposed an automatic Network Intrusion Detection System using machine learning and deep learning algorithms to improve detection accuracy while reducing false positive rates. Their work demonstrated that combining feature engineering with deep neural networks significantly enhances intrusion detection performance compared to conventional machine learning models. Ramya Chinnasamy et al. (2025) introduced a hybrid Honey Badger Optimization-Artificial Neural Network (HBO-ANN) framework for intrusion detection. Honey Badger Optimization was employed for optimal feature selection, while ANN performed attack classification using the CIC-IDS2017 dataset. Their model achieved 97.66% accuracy with a false alarm rate of only 1.97%, outperforming several optimization-based machine learning models. Mohale and Obagbuwa (2025) investigated Explainable Artificial Intelligence (XAI) techniques for network intrusion detection. They integrated SHAP, LIME, and ELI5 with machine learning models including XGBoost, CatBoost, Random Forest, and Logistic Regression using the UNSW-NB15 dataset. Their results indicated that XGBoost and CatBoost achieved 87% accuracy while substantially improving model interpretability for cybersecurity analysts. Tamara Al-Shurbaji et al. (2025) comprehensively reviewed deep learning-based intrusion detection methods for IoT botnet attacks. Their survey highlighted CNN, RNN, LSTM, Autoencoders, and ensemble deep learning approaches while emphasizing challenges such as class imbalance, dynamic attack evolution, and computational overhead in IoT environments. Muhanna Ahmed Ali and colleagues (2025) evaluated Random Forest, Support Vector Machine, and Long Short-Term Memory for detecting Man-in-the-Middle (MitM) attacks in IoT networks. Random Forest achieved the highest detection accuracy of approximately 94%, demonstrating better robustness and lower false alarm rates than SVM and LSTM. Farhan et al. (2025) proposed a Sequential Deep Neural Network integrated with an Extra Tree Classifier for feature selection. Using the UNSW-NB15 dataset, their model reduced feature dimensionality while achieving 97.93% classification accuracy and excellent precision, recall, and F1-score. Manivannan and Senthil kumar (2025) developed an Adaptive Recurrent Neural Network optimized by the Fox Optimization algorithm (ARNN-FOX). Their optimization-based IDS significantly improved accuracy, sensitivity, specificity, precision, recall, and F1-score compared with traditional CNN-LSTM and RNN-based methods. Dash et al. (2025) optimized LSTM using Particle Swarm Optimization, JAYA, and Salp Swarm Optimization for anomaly detection across NSL-KDD, CICIDS, and BoT-IoT datasets. Their SSA-LSTM model consistently produced superior accuracy, reduced false positives, and improved generalization capability across multiple datasets. Several recent studies have also investigated Graph Neural Networks, Transformer-based BERT models, energy-efficient deep learning, reinforcement learning, blockchain-assisted IDS, fuzzy clustering, ensemble learning, and adversarially robust intrusion

detection. These methods consistently demonstrate improved detection performance while highlighting remaining challenges related to computational complexity, explainability, adversarial robustness, minority-class detection, and real-time deployment in resource-constrained environments.

Problem Statement

Although recent Machine Learning (ML) and Deep Learning (DL) approaches have significantly improved intrusion detection accuracy, several practical limitations remain unresolved. Many existing models require extensive feature engineering, suffer from class imbalance, generate high false positive rates, require considerable computational resources, and struggle with real-time deployment in resource-constrained IoT and edge computing environments. Furthermore, many deep learning models operate as black-box systems, providing limited interpretability and making it difficult for cybersecurity analysts to understand prediction decisions. Optimization algorithms such as Honey Badger Optimization, Particle Swarm Optimization, Fox Optimization, and Salp Swarm Optimization have improved feature selection and hyperparameter tuning; however, achieving an optimal balance among detection accuracy, computational efficiency, model interpretability, scalability, adversarial robustness, and real-time performance remains an open research challenge. Therefore, there is a need to develop an intelligent, lightweight, explainable, optimization-driven intrusion detection framework capable of accurately identifying both known and unknown attacks while supporting real-time deployment in modern cloud, IoT, IIoT, and edge computing environments.

Machine Learning

Machine Learning (ML) is a branch of Artificial Intelligence (AI) that enables computer systems to learn patterns, relationships, and decision rules directly from historical data without being explicitly programmed for every scenario. Instead of relying on predefined instructions, ML algorithms continuously improve their performance by analyzing data and adapting their predictive models over time. The ability of machine learning to identify hidden patterns within massive datasets has made it one of the most widely adopted technologies in cybersecurity, healthcare, finance, smart manufacturing, transportation, and intelligent communication systems.

In network security, machine learning has become an essential technology for Intrusion Detection Systems (IDS) because modern cyberattacks continuously evolve and frequently bypass traditional signature-based security mechanisms. ML-based IDS automatically analyze network traffic, identify abnormal communication patterns, classify malicious activities, and detect previously unseen attacks with significantly higher accuracy than conventional rule-based systems. Recent research demonstrates that machine learning algorithms such as Decision Tree, Random Forest, Support Vector Machine (SVM), Logistic Regression, Naïve Bayes, K-Nearest Neighbor (KNN), Gradient Boosting, XGBoost, and ensemble learning models substantially improve intrusion detection performance while reducing false positive rates. Although traditional machine learning algorithms have achieved remarkable success, their performance heavily depends on feature engineering, feature selection, dataset quality, and parameter optimization. Consequently, many recent studies integrate optimization algorithms and deep learning architectures to automatically extract informative features and improve classification accuracy for increasingly complex cyber threats.

Types of Machine Learning

Machine Learning can be broadly categorized into four major types depending on the nature of available training data and the learning methodology.

Supervised Learning

Supervised Learning is the most commonly used machine learning approach for network intrusion detection. In this technique, the model is trained using labeled datasets where each network traffic record is associated with a known output label, such as "Normal" or "Attack." During training, the algorithm learns the relationship between input features and output classes and later predicts the class of unseen network traffic.

Popular supervised learning algorithms include:

- Logistic Regression
- Decision Tree
- Random Forest
- Support Vector Machine (SVM)
- Naïve Bayes
- K-Nearest Neighbor (KNN)
- Gradient Boosting
- XGBoost
- Extra Trees Classifier

Unsupervised Learning

Unsupervised Learning operates on unlabeled datasets where the algorithm attempts to discover hidden structures or clusters within network traffic without prior knowledge of attack labels. This approach is particularly useful for detecting unknown attacks and zero-day threats because it identifies deviations from normal network behavior.

Common unsupervised learning algorithms include:

- K-Means Clustering
- DBSCAN
- Hierarchical Clustering
- Gaussian Mixture Models
- Autoencoders
- Principal Component Analysis (PCA)

Semi-Supervised Learning

Semi-supervised learning combines a small amount of labeled data with a large quantity of unlabeled network traffic. Since labeling cybersecurity datasets is expensive and time-consuming, semi-supervised learning has gained considerable attention in modern IDS research.

Its major advantages include:

- Reduced labeling cost
- Better utilization of real-world network traffic
- Improved generalization capability
- Better zero-day attack detection

Reinforcement Learning

Reinforcement Learning (RL) enables an intelligent agent to learn optimal actions through continuous interaction with the network environment. Instead of relying on labeled examples, the agent receives rewards or penalties based on its actions and gradually improves its decision-making policy.

In cybersecurity, reinforcement learning is increasingly used for:

- Dynamic intrusion prevention
- Automated firewall configuration
- Intelligent routing
- Adaptive threat response
- Resource allocation

Proposed Work

The rapid increase in cyberattacks against cloud computing, IoT, Industrial IoT (IIoT), edge computing, and enterprise networks demands intrusion detection systems that are highly accurate, computationally efficient, interpretable, and capable of real-time operation. Although recent deep learning approaches achieve excellent classification accuracy, they often require expensive computational resources, extensive training time, and large memory requirements, making them unsuitable for deployment in resource-constrained environments. Moreover, many existing deep learning models operate as black-box systems, limiting the ability of cybersecurity analysts to understand attack predictions and increasing operational complexity. To overcome these limitations, this research proposes an Explainable Machine Learning-Based Network Intrusion Detection System (EML-NIDS) that combines advanced data preprocessing, optimized feature selection, ensemble machine learning classification, and explainable artificial intelligence (XAI). Unlike conventional IDS approaches that rely solely on deep learning, the proposed framework emphasizes lightweight yet highly accurate machine learning models capable of real-time deployment. Initially, the collected network traffic dataset will undergo comprehensive preprocessing including missing value handling, duplicate removal, categorical encoding, normalization, feature scaling, and class balancing using techniques such as SMOTE. Subsequently, an optimization-based feature selection mechanism will identify the most informative traffic attributes, reducing feature redundancy and computational complexity while preserving classification performance.

The optimized feature subset will then be utilized to train multiple supervised machine learning classifiers including Decision Tree, Logistic Regression, Support Vector Machine (SVM), Random Forest, Extra Trees Classifier, Gradient Boosting, XGBoost, LightGBM, CatBoost, and AdaBoost. Hyperparameter optimization using Grid Search Cross Validation or Bayesian Optimization will further enhance model performance. The best-performing classifier will be selected based on multiple evaluation metrics including Accuracy, Precision, Recall, F1-score, ROC-AUC, Detection Rate, False Positive Rate, and False Negative Rate.

Outcomeof the Proposed Work

Compared with existing research, the proposed framework contributes by:

- Developing a machine learning-based IDS.
- Remove redundant network traffic features.
- Evaluating a comprehensive suite of state-of-the-art machine learning classifiers and selecting the best model among them.

- Addressing class imbalance, reducing false positives, and maintaining high detection accuracy for attacks.

Conclusion

The comprehensive review of the uploaded literature demonstrates that machine learning algorithms such as Decision Tree, Random Forest, Support Vector Machine (SVM), Logistic Regression, Gradient Boosting, XGBoost, and ensemble classifiers have significantly improved intrusion detection performance compared to conventional security systems. Furthermore, deep learning architectures including Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), Graph Neural Networks (GNN), Transformer-based BERT models, and hybrid CNN-LSTM frameworks have achieved remarkable detection accuracies on benchmark datasets. Optimization algorithms including Honey Badger Optimization, Particle Swarm Optimization, Fox Optimization, Salp Swarm Algorithm, and Knowledge Distillation have further enhanced feature selection, hyperparameter optimization, computational efficiency, and model generalization. Overall, this research aims to develop a scalable, efficient, explainable, and real-time intrusion detection framework capable of protecting modern cloud, enterprise, IoT, IIoT, and edge computing environments from both known and unknown cyber threats. The findings of this review provide a strong theoretical foundation for the proposed methodology and highlight the importance of combining optimization techniques, ensemble machine learning, and explainable artificial intelligence to build the next generation of intelligent Network Intrusion Detection Systems (NIDS). Such a framework has the potential to significantly improve cyber-security resilience by providing accurate, interpretable, and low-latency intrusion detection while addressing the limitations identified in existing research.

References

[1] M. Mynuddin et al., "Automatic Network Intrusion Detection System Using Machine Learning and Deep Learning," TechRxiv, 2024.

[2] R. Chinnasamy et al., "Empowering Intrusion Detection Systems: A Synergistic Hybrid Approach with Optimization and Deep Learning Techniques," International Arab Journal of Information Technology, vol. 22, no. 1, 2025.

[3] V. Z. Mohale and I. C. Obagbuwa, "Evaluating Machine Learning-Based Intrusion Detection Systems with Explainable AI," Frontiers in Computer Science, 2025.

[4] T. Al-Shurbaji et al., "Deep Learning-Based Intrusion Detection System for Detecting IoT Botnet Attacks: A Review," IEEE Access, 2025.

[5] M. A. Ali et al., "Intrusion Detection in IoT Networks Using Machine Learning and Deep Learning Approaches," Discover Internet of Things, 2025.

[6] M. Farhan et al., "Network-Based Intrusion Detection Using Deep Learning Technique," 2025.

[7] R. Manivannan and S. Senthilkumar, "Intrusion Detection System Using Novel Adaptive Recurrent Neural Network-Based Fox Optimizer," International Journal of Computational Intelligence Systems, 2025.

[8] N. Dash et al., "An Optimized LSTM-Based Deep Learning Model for Anomaly Network Intrusion Detection," 2025.

[9] Y. Wang et al., "BS-GAT: A Network Intrusion Detection System Based on Graph Neural Network," Cybersecurity, 2025.

[10] R Dubey, "An empirical study of intrusion detection system using feature reduction based on evolutionary algorithms and swarm intelligence methods", International Journal of Applied Engineering Research, 2017. pp. 8884-8889.

[11] H. G. A. Umar et al., "Energy-Efficient Deep Learning-Based Intrusion Detection System for Edge Computing," Journal of Cloud Computing, 2025.

[12] Y. Yang and X. Peng, "BERT-Based Network for Intrusion Detection System," EURASIP Journal on Information Security, 2025.

[13] M. A. Hossain, "Deep Learning-Based Intrusion Detection for IoT Networks," EURASIP Journal on Information Security, 2025.

[14] M. Srinivasan and N. C. Senthilkumar, "Intrusion Detection and Prevention System Model for IIoT Environments Using Hybridized Framework," IEEE Access, 2025.

[15] D Rathore, A Jain, "Design Hybrid method for intrusion detection using Ensemble cluster classification and SOM network", International Journal of Advanced Computer Research, 2012.

[16] U. Ahmed et al., "Signature-Based Intrusion Detection Using Machine Learning and Deep Learning Approaches Empowered with Fuzzy Clustering," Scientific Reports, 2025.

[17] Q. Zhao et al., "Research on Intrusion Detection Model Based on Improved MLP Algorithm," 2025.

[18] P Mishra, D Rathore, "Improved the Intrusion Detection Ratio Using Feature Reduction based on Feature Selection and GSA", Engineering Universe for Scientific Research and Management, Vol-6, Issue-1, 2014.