Journal of Computing and Communication Vol.4, No. 2, PP. 13-31, 2025

Recent Studies and A Review about Detection of Cyber Threats in Cloud Security using Artificial Intelligence

Hussam Kotb*[a], Elsayed Badr [b,c,d], Fatma Sakr[e]

[a]Department of Artificial Intelligence, Faculty of Computers and Artificial Intelligence, Benha University, Benha, Egypt

[b]Department of Scientific Computing, Faculty of Computers and Artificial Intelligence, Benha University, Benha, Egypt

[c]The Egyptian School of Data Science (ESDS), Benha, Egypt

[d]Department of Information Systems, College of Information Technology, Misr University for Science and Technology, Giza, Egypt

[e]Department of Computer Science, Faculty of Computers and Artificial Intelligence, Benha University, Benha, Egypt

*Corresponding Author: Hussam Kotb [***Hussam1091@gmail.com***]

ARTICLE DATA

Article history:
Received: 13 May 2025
Revised: 09 July 2025
Accepted: 09 July 2025
Available online:30 July 2025

Keywords:
Deep Learning
Machine Learning
Cyber Threats
Intrusion Detection
Cloud Security

ABSTRACT

Cloud computing has significantly transformed the IT industry through cost-efficient solutions, offering scalable Data. In the cloud, data may be more vulnerable than data on on-site premises. However, its rapid adoption has also introduced new cyber security risks as systems become increasingly vulnerable to sophisticated attacks. Traditional Intrusion Detection Systems (IDS) often face challenges in identifying and mitigating advanced persistent threats, zero-day exploits, and other real-time cyber threats, especially within dynamic cloud environments. This paper analyzes and evaluates the detection of cyber threats in cloud security, focusing on challenges related to recognition, aggregation, and dissemination within user system environments. The research comprehensively review recent studies have leveraged artificial intelligence (AI) methodologies to enhance cyber threat detection. Different deep learning and machine learning approaches are compared based on multiple optimization criteria, including dataset characteristics, simulation environments, real-world deployments, scalability, detection accuracy, coverage of threat types, and overall system performance. Our primary purpose is to offer ideas for the latest progression in cyber-attacks detection in AI, identifying the limitations, open research questions and suggesting potential enhancement for unresolved security challenges.

1. Introduction

Securing cloud environments from sophisticated cyber threats remains a core challenge in today's fast-developing digital ecosystem [37]. Traditional signature-based Network Intrusion Detection Systems (NIDS) operate by matching predefined attack signatures with incoming network traffic. While this approach is practical for detecting known threats, it struggles to identify new and evolving attack patterns. Restricting and reducing its adaptability in dynamic cloud environments. To overcome these shortcomings, anomaly-based NIDS leveraging (ML) and (DL) have gained attention. Fixed signatures are limited by this dynamic approach, which stresses the detection of anomalies in established network behavior. Although they have advantages, such models face important obstacles, including difficulties adapting to rapidly evolving attack strategies, high false positive rates, and scalability concerns [37]. The opaque decision-making processes of machine learning and deep learning models often create barriers to interpretability, which can hinder cybersecurity professionals from fully understanding or trusting the system outputs [38]. Addressing this issue requires the development of intrusion detection systems that balance accuracy, scalability, and transparency—particularly within the evolving landscape of cloud security.

This research presents a detailed literature review, analyzing Forty-eight studies published between 2018 and 2025 investigating the application of ML and DL in anomaly-based NIDS and different topics in IOT. These studies cover various aspects, including accuracy improvement, false positive rate reduction, and real-time processing efficiency. Additionally, some works emphasize critical challenges such as computational overhead, class imbalance, and the interpretability of deep learning architectures. The insights gathered from these studies provide a foundation for identifying gaps in existing methodologies and formulating an optimized approach for anomaly-based intrusion detection in cloud environments.

Research Methodology

The research methodology follows a structured four-phase approach: Phase 1 (Article Selection), Phase 2 (Article Classification), Phase 3 (Article Analysis), and Phase 4 (Discussion and Future Directions). Each phase has its role in an organized manner, evaluating the literature.

Phase 1: Article Selection – This initial phase identifies and filters relevant research papers.

Database Selection: To ensure credibility and relevance, articles are sourced from established databases, including ResearchGate (https://www.researchgate.net), MDPI (https://www.mdpi.com/), Springer, and ScienceDirect (https://www.sciencedirect.com/).

Screening & Filtering: Research papers are evaluated based on predefined criteria, such as relevance to anomaly-based NIDS, recent publication, and alignment with the study's objectives. Only high-quality studies meeting these requirements are included for further analysis.

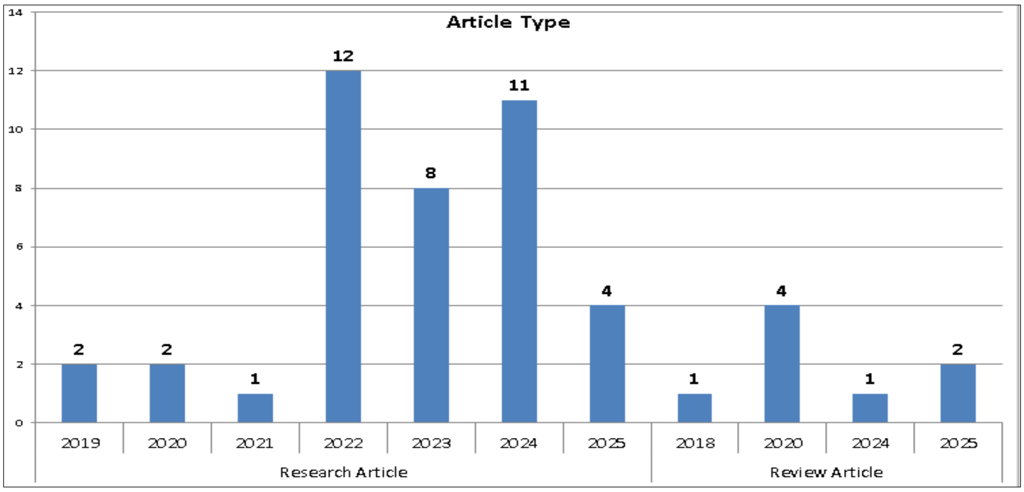

FIGURE 1: Number of Papers used in Survey, Research and Review Articles

A research article [40 papers] aims to describe a particular research study that was completed and will be based on the analysis and the interpretation of this data and based on original research. While a review article [8 papers] discusses the state of the field you are investigating and based on other published articles

Review articles can be of 3 types:

- A narrative review - explains the existing knowledge based on all the published research.
- A systematic review - find the answer to a particular question in the existing scientific.
- A meta-analysis - combines and compares the findings of previously published studies.

Phase 2: Article Classification

The selected research papers are systematically categorized based on several key factors, including the methodologies employed (e.g., machine learning and deep learning techniques), the type of Intrusion Detection System (IDS) (network-based or host-based), and the primary challenges addressed (such as reducing false positives and improving real-time detection capabilities). As seen in Figure 1, this classification shows a structured approach for analyzing current research while identifying developing trends in anomaly-based NIDS.

Phase 3: Article Analysis

This phase includes thoroughly assessing the selected studies, summarizing key findings, and highlighting existing research challenges. A critical assessment is conducted to pinpoint gaps in the current literature that require further investigation.

Phase 4: Discussion and Future Scope

key findings from the analysis are evaluated, focusing on outlining future research directions and identifying potential solutions. The methodology follows a systematic framework for selecting, categorizing, analyzing, and discussing research papers. This structured approach ensures a comprehensive understanding of anomaly-based intrusion detection systems' latest advancements, limitations, and future possibilities.

1. Background Information

1.1. This section provides an overview of the key focus areas of our survey. We begin by discussing Intrusion Detection Systems (IDS) and the challenges associated with aggregation and dissemination in anomaly-based Network Intrusion Detection Systems (NIDS). Following this, we explore various AI techniques employed to enhance the effectiveness of anomaly-based NIDS.

1.2. Data Collection

Dataset selection is a crucial step in training an anomaly-based Network Intrusion Detection System (NIDS) using ML and DL techniques. Dataset quality and diversity efficiently affect the model's ability to generalize, maintain accuracy, and effectively detect cyber threats in real-world environments. Different dataset combinations enhance the model's robustness of the mode, ensuring adaptability across different network conditions and threat landscapes.

1.3. AI Techniques

Once the dataset has been obtained and preprocessed, the next phase involves a structured approach to model selection, feature engineering, and deployment to develop a high-accuracy anomaly-based Network Intrusion Detection System (NIDS).

Baseline Machine Learning Models

- Random Forest (RF) and XGBoost are initially employed due to their effectiveness in handling imbalanced datasets and their ability to provide interpretable feature importance scores.
- RF's ensemble learning mechanism reduces overfitting by combining multiple decision trees for improved prediction stability.
- XGBoost enhances detection accuracy and optimizes decision-making in intrusion detection tasks, which leverages gradient boosting. These models serve as baselines before transitioning to more advanced deep-learning architectures. These models serve as baselines before transitioning to more advanced deep learning architectures.

Deep Learning Models

For improved accuracy and adaptability, a hybrid CNN-LSTM model is implemented:

- Convolutional Neural Networks (CNNs) extract spatial patterns from network traffic data.
- Temporal dependencies are captured by Long-short-term memory(LSTM) networks; the system is allowed to recognize the sequential attack behavior.

Additionally, a Transformer-based IDS model incorporating self-attention mechanisms is deployed to detect subtle and complex attack patterns, enhancing contextual awareness and anomaly detection.

Feature Engineering and Optimization -To refine model performance and efficiency:

- Principal Component Analysis (PCA) reduces dimensionality of large datasets by transforming a large set of variables into smaller one that still contains most of the information in the large dataset.
- Recursive Feature Elimination (RFE) identifies the most relevant features, enhancing model interpretability and reducing computational overhead.

- SMOTE (Synthetic Minority Oversampling) is a statistical technique to address the class imbalance, generating synthetic samples to prevent bias toward majority classes and improve generalization.

Model Training and Performance Evaluation

- Bayesian optimization is used for hyperparameters tuning, adjusting learning rates, batch sizes, and network architectures to achieve optimal performance.
- ReLU activation functions introduce non-linearity, enabling the model to learn complex attack patterns.
- 10-fold cross-validation systematically evaluates model stability and prevents overfitting.
- F1-score, recall, and precision are prioritized to ensure a balance between detecting real threats and minimizing false alarms, as accuracy alone is insufficient in cybersecurity applications.

Deployment and Real-World Integration -For seamless real-world application, the trained model is:

- Containerized using Docker and orchestrated with Kubernetes for scalability.
- Deployed on AWS, ensuring computational efficiency and adaptability to changing network conditions.
- Optimized with TensorFlow Serving, reducing inference latency for real-time intrusion detection.
- Equipped with an automated retraining pipeline to update the model continuously as new cyber threats emerge.
- Integrated with Edge Computing to process network traffic closer to the source in latency-sensitive environments, enabling faster anomaly detection and response. Docker + Kubernetes focuses on containerization and orchestration, enabling efficient management and scaling of NIDS components. AWS deployment provide adaptable infrastructure ,computational resources, certifying adaptability and cost-effectiveness.

2. Related Works

Recent research has explored the application of artificial intelligence in improving cyber security measures in cloud environments, especially in real-time threat detection. One important contribution was made by [3], who suggested a transfer learning-based intrusion detection system designed for encrypted and heterogeneous network environments. Even though their work was not obviously cloud-focused, the model's flexibility suggests strong potential for adaptation to multi-tenant cloud infrastructures, in which encryption and heterogeneous protocols dominate. Building on the theme of feature learning, they introduced an end-to-end intrusion detection framework; they designed a hierarchical Convolutional Neural Network (CNN) and Gated Recurrent Unit (GRU) model to facilitate the automated extraction of spatiotemporal features from raw traffic data. This method's ability to process high-dimensional data renders it highly applicable to the dynamic and scalable architecture of cloud environments. The framework is assessed utilizing commonly employed datasets, namely, CIC-IDS2017 and CSE-CIC-IDS2018. The experiments demonstrate that our method can attain a detection accuracy of 99.9% for known attacks, thus achieving state-of-the-art performance. Our method also achieved a recall rate of over 95% for all unknown attacks.

Focusing on predictive analytics, [6] developed a machine learning-enabled cyber event forecasting system utilizing SVM, Random Forest, and time series analysis techniques. While initially intended for general cybersecurity use, the predictive capabilities of their model could enhance proactive threat detection in cloud computing systems. Also [8], the use of deep learning coupled with data augmentation strategies to enhance intrusion detection systems was explored. Their approach focused on overcoming data scarcity and imbalance challenges. It is mainly relevant to cloud security, where different and rapidly evolving datasets are standard.

Moving to particular cloud-focused solutions, [9] a robust intrusion detection system designed to detect malicious activities within cloud environments was proposed. Their model combined Radial Basis Function Neural Networks with Random Forest classifiers to reach high detection accuracy while keeping computational efficiency. The authors highlighted the importance of developing AI-based security mechanisms that adapt to the accessible and dynamic nature of cloud computing systems to reduce and overcomed the limitations of traditional intrusion detection solutions.

In the realm of real-time detection, [10] proposed a machine learning-based multi-class classification system for IoT attacks using the One-vs-Rest strategy and SMOTE for dataset balancing. Though developed for IoT contexts, the real-time responsiveness and data balancing techniques align closely with the operational needs of cloud-native security systems. Adding to this, [11] introduced a near-real-time intrusion detection system making use of supervised learning with Apache Spark, a framework widely adopted in distributed cloud architectures. Their focus on minimizing detection latency and maximizing scalability is directly applicable to cloud-based environments where speed and resilience are critical.

In terms of web-based real-time solutions adaptable to cloud services, [39] developed AI-IDS, a real-time web intrusion detection system based on CNN and LSTM architectures. Although primarily targeting web applications, the real-time capabilities and scalability of AI-IDS make it highly suitable for securing cloud-hosted services where rapid threat mitigation is vital.

Other works have also demonstrated methodologies adaptable for cloud-based real-time intrusion detection. For example, [25] proposed zero-day attack detection models in streaming data environments, applying Random Forests and Hoeffding trees to manage continuous data flows. Their approach is naturally aligned with the streaming and dynamic data processing demands of cloud computing. Additionally, [37] addressed DoS attack detection in IoT networks using a suite of machine learning algorithms, including Deep Neural Networks and XGBoost. Despite being focused on IoT, the scalability and robustness of their models position them well for adaptation into cloud-centric security frameworks.

Finally, it offered a hybrid deep learning model explicitly targeting AWS cloud environments[41]. Detecting complicated cyber threats on a large scale demonstrated significant improvement by incorporating LSTM with RF classifiers. The diversity and volume of cloud traffic are handled by the effectiveness of combining deep learning with ensemble techniques, ensuring real-time threat detection.

Complementarily, [46] introduced an AI-enabled system for efficient and effective cyber incident detection and response across cloud platforms such as Google Cloud and Microsoft Azure. Their approach integrated and combined RF models for network traffic classification and focused heavily on real-time incident response capabilities. Achieving up to 96% accuracy in malware analysis, the system emphasized high detection precision and rapid automated response, aligning perfectly with the needs of real-time cloud security. The previous advancements focus on the crucial role of AI and how it is a proactive and intelligent cyber defense mechanism within cloud ecosystems.

In line with the growing demand for robust cloud security, [47] proposed an AI-powered intrusion detection system tailored for next-generation cloud environments. Their model, leveraging deep learning techniques and evaluated on the NSL-KDD dataset, achieved a significant detection accuracy of 98.68%. Deployment in dynamic cloud infrastructures is made and optimized for real-time threat detection by low false negatives and minimal latency. The model's performance illustrates the significant potential of advanced deep learning architectures in securing cloud environments against evolving cyber threats. Among recent advancements in cloud-native security, [48] propose an integrated framework that combines real-time multi-class threat detection with adaptive deception mechanisms tailored for Kubernetes environments. This approach is particularly significant due to Kubernetes' increasing adoption in cloud infrastructures and its exposure to dynamic and complex threats such as privilege escalation, reconnaissance, and DoS attacks.

The authors address key limitations found in traditional intrusion detection systems, such as high false positive rates and poor adaptability to evolving attack patterns. Their framework leverages machine learning models hosted on KServe, feature extraction via CICFlowMeter, and dynamic decoy deployment using KubeDeceive, all orchestrated through the MAPE-K feedback loop for continuous adaptation. Notably, their model achieves 91% detection accuracy and a decoy success rate of up to 93%, validating its robustness and real-time capabilities.

3. Data Collection, Aggregation, and Dissemination Challenges in Anomaly-NIDs

Effectiveness of anomaly based Network intrusion detection (NIDS) is affected obviously by data collection , aggregation and dissemination in order to identify unusual pattern.

3.1 Data Collection Challenges:

- Volume and Velocity of Network Traffic: Losing critical data is a big challenge facing the data collection flood managment for real time detection system (NIDS).
- Data Quality and Preprocessing: Network data often contains noise and irrelevant packets, requiring precise preprocessing techniques to enhance data integrity.
- Proper preprocessing is crucial for accurate anomaly detection. Anomaly detection is under the management of proper preprocessing data.
- Imbalanced Datasets: When a dataset is balanced, the number of positive and negative labels is about equivalent. However, when unusual activities are uncommon or rare compared to normal traffic, the data is biased toward normal traffic or patterns, thus reducing its sensitivity to anomalies.

3.2 Data Aggregation Challenges:

- Preserving Anomaly Signatures: subtle anomalies are obscured making them difficult to detect by aggregating data and it's crucial to ensure that aggregation methods keep the integrity of anomaly signatures for detection efficiency.
- Real-Time Processing: Well-timed detection of anomalies is crucial.
- Aggregation processes must be optimized not to introduce significant delays, which could delay prompt responses to potential threats
- Scalability: As networks grow, the amount of data to be aggregated increases, requiring scalable aggregation techniques that can deal with massive datasets without compromising performance..
- Timely Distribution of Alerts: Prompting alerts to relevant teams is crucial once an anomaly is detected because delays may cause slower response threats.
- Security of Dissemination Channels: Security teams must secure the channels they use to disseminate detection results and alerts to prevent interception or tampering by malicious actors. They must prioritize maintaining the confidentiality and integrity of these channels.
- Information Overload: Unnecessary alerts. Security teams are overwhelmed by false positives, leading to alert fatigue. Distribution strategies should filter and prioritize alerts to guarantee that critical threats receive appropriate attention. Development of advanced data handling techniques are a must for handling these challenges, such as robust preprocessing methods, scalable aggregation algorithms, secure and efficient dissemination protocols to improve the efficiency of anomaly-based (NIDs).

4. Summary of the papers

Here in this section the table will give a review and summary about the cyber-attacks detection in variant methods which used artificial intelligence techniques listed in table 1.

Table 1: Summary of used algorithms and deployed accuracies of survey researches

Ref.	Name	Type of IDS	Algorithm	Primary challenges addressed	Datasets	Accuracy	Year
[1]	An Efficient CNN-Based Intrusion Detection System for IoT: Use Case Towards Cyber Security	Anomaly-Based	CNN	Accuracy improvement in IoT,Reducing false positives	BoT - IoT	98.2%	2024
[2]	Big Data-Driven Deep Learning Ensembler for DDoS Attack Detection	Anomaly-Based	SVM, ANN-GWO, GRU-RNN, CNN, LSTM, and DBN	Improving detection in DDoS,Handling big	IoT-23 , APA-DDoS	99.05%	2024

				data, Real-time detection			
[3]	Multiple Kernel Transfer Learning for Enhancing Network Intrusion Detection in Encrypted and Heterogeneous Network Environments .	Anomaly-Based	Transfer learning	Encrypted & heterogeneous data,Transfer learning	CIC-IDS-2017, CSE-CIC-IDS-2018	90%	2024
[4]	End-to-End Network Intrusion Detection Based on Contrastive Learning .	Anomaly-Based	CNN and GRU	Feature extraction,Improving accuracy	CIC-IDS2017,cSE-CIC-IDS2018	99%	2024
[5]	A Comparative Analysis of the TDCGAN Model for Data Balancing and Intrusion Detection	Anomaly-Based	TDC(traffic data conditional)Generative Adversarial Network (GAN), DT, RF	Data imbalance,GAN for balancing	CIC-IDS 2017, CSE-CIC- IDS 2018, KDD-Cup 99, BOT-IOT	85%, 88%	2024
[6]	Rapid Forecasting of Cyber Events Using Machine Learning-Enabled Features	Anomaly-Based	SVM , RF, Naïve bayes , time series	Time-sensitive detection,Early warning system	CSE-CIC-IDS2018	99.2%	2024
[7]	Improvement of Distributed Denial of Service Attack Detection through Machine Learning and Data Processing	Anomaly-Based	RF,DT,ADA (AdaBoost),XGB (Extreme Gradient Boosting)	DDoS mitigation,Reducing false alarms	CICDDoS2019	RF: 99.97%	2024
[8]	Enhancing Intrusion Detection Systems Using a Deep Learning and Data Augmentation Approach	Anomaly-Based	CNN	Data scarcity,Improved DL accuracy	UNSW-NB15, CIC-IDS-2017, 5G-NIDD, FLNET2023	91%	2024
[9]	Towards an Intelligent Intrusion Detection System to Detect Malicious Activities in Cloud Computing	Anomaly-Based	Radial Basis Function Neural Network (RBFNN) ,RF	Malicious activity detection,Cloud security	Bot-IoT, NSL-KDD	92%	2023
[10]	Using Machine Learning Multiclass Classification Technique to Detect IoT Attacks in Real Time.	Anomaly-Based	OneVsRest , SMOTE	Real-time detection,Imbalanced data handling	IoT-23	98.89%	2024
[11]	Towards Near-Real-Time Intrusion Detection for IoT Devices using Supervised Learning and Apache Spark	Anomaly-Based	DT,RF	Big data processing,Real-time capabilities	SYN-DOS	>99%	2020
[12]	Ensemble-Based Deep Learning Models for Enhancing IoT Intrusion Detection	Anomaly-Based	CNN,LSTM,GRU	Combining DL models,High detection rate	KDD’99	99.7%	2023
[13]	Intrusion Detection System Using Feature Extraction with Machine Learning Algorithms in IoT	Anomaly-Based	VGG-16, DenseNet,RF,KNN ,SVM	Efficient feature use,IoT threat detection	IEEE Dataport	98%	2023
[14]	Deep Learning Approach for SDN-Enabled Intrusion Detection System in IoT Networks	Anomaly-Based	LSTM.SVM,CNN	IoT-SDN integration,Deep learning benefits	SDNIoT-focused	97%	2023
[15]	An Intrusion Detection System Using BoT-IoT	Anomaly-Based	ensemble bag ,DT	Dataset-specific optimization,	Bot-IoT	100%	2023
[16]	Deep Learning-Based Malicious Smart Contract and Intrusion Detection System for IoT Environment	Anomaly-Based	LSTM,GRU,	Blockchain/IoT security,Malicious behavior	NSL-KDD	99.12%	2023
[17]	Realguard: A Lightweight Network Intrusion Detection System for IoT Gateways	Anomaly-Based	DNN	Lightweight,IoT gateways	UNSW-NB15	99.5%	2022
[18]	A Particle Swarm Optimization and Deep Learning Approach for Intrusion Detection System in Internet of Medical Things	Anomaly-Based	PSO,LSTM,CNN	Medical IoT,Optimization	Combined Network Traffic and Patient Sensing Data	96%	2022
[19]	Performance Investigation of Principal Component Analysis for Intrusion Detection System Using Different Support Vector Machine Kernels	Anomaly-Based	SVM	Dimensionality reduction,Kernel performance	KDD Cup’99 , UNSW-NB15	99.11%, 93.94%	2022
[20]	Evaluation and Selection Models for Ensemble Intrusion Detection Systems in IoT	Anomaly-Based	Binary and Multi-classification	Model comparison,Selection framework	UNSW-NB15, Aposemat IoT-23, ToN_IoT	99.45%, 97.81%	2022

[21]	A Composite Approach of Intrusion Detection Systems: Hybrid RNN and Correlation-Based Feature Optimization	Anomaly-Based	LSTM,GRU	Handling imbalanced datasets,Improved detection accuracy	CICIDS 2017	99.13%	2022
[22]	A Deep Learning Model for Network Intrusion Detection with Imbalanced Data	Anomaly-Based	LSTM,CNN	Cyber threat detection,IoT focus	NSL-KDD	90.73%	2022
[23]	IMIDS: An Intelligent Intrusion Detection System against Cyber Threats in IoT	Anomaly-Based	CNN	Smart factory protection,Edge computing integration	UNSW-NB15, CICIDS2017	96.6%,95.9%	2022
[24]	IIoT Malware Detection Using Edge Computing and Deep Learning for Cyber security in Smart Factories	Anomaly-Based	Edge computing , CNN	Zero-day attacks,Streaming data processing	Malimg	98.93%	2022
[25]	Zero-Day Attack Detection Analysis in Streaming Data Using Supervised Learning Techniques	Anomaly-Based	RF,RT,Naïve bayes , Hoeffding tree	Alert fatigue,Efficiency in alert systems	CICIDS	99.97%	2022
[26]	DualAC2NN: Revisiting and Alleviating Alert Fatigue from the Detection Perspective	Review Paper (Anomaly-Based focus)	CNN	Reviewing models for botnet detection,IoT attack classification	real-world HTTP traffic	97.89%	2022
[27]	Deep Learning-Based Intrusion Detection System for Detecting IoT Botnet Attacks: A Review	Anomaly-Based	RNN,SNN,MLP,KNN, CNN, LSTM	Collaborative detection,IoT-specific	NSL-KDD, BoT-IoT, CIC-IDS2017 ,CSE-CIC-IDS2018	87%, 99.95%, 91.27%, 99.96%	2025
[28]	CoLL-IoT: A Collaborative Intruder Detection System for Internet of Things Devices	Review	CoLL-IoT	APTs overview,Future research direction	UNSW-NB15	98%	2021
[29]	A New Proposal on the Advanced Persistent Threat: A Survey	Anomaly-Based	SVM, k-NN , DT	Comparing ML classifiers,Cyber intrusion detection	No Dataset applied		2020
[30]	IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model	Review	NB,LR, KNN,SVM	Accuracy benchmarking,Technique comparison	KDD'99		2022
[31]	Performance Comparison and Current Challenges of using Machine Learning Techniques in Cyber Security	Review	NB, RF, DT, SVM, DBN, ANN	Insider threat models,Open challenges	KDD Cup 99, Enron, Spambase	The greatest accuracy is: DT for IDS: 99.96%,	2020
[32]	A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations	Review	LSTM , GRU	Systematic review,Deep learning in anomaly detection	RTU (Remote terminal unit), NSLKDD/KDD-99, Schonlau, APEX' 07, RUU, TWOS		2020
[33]	Anomaly-Based Intrusion Detection Systems in IoT Using Deep Learning: A Systematic Literature Review	Anomaly-Based	AE ,CNN	Fog environments,Resource efficiency	Mirai-RGU, Yahoo Webscope S5, KDDUP99	99.99%,99.62%,99.78%	2020
[34]	A Lightweight Perceptron-Based Intrusion Detection System for Fog Computing	Anomaly-Based	MLP	Unsupervised learning,Deep belief networks	ADFA	94%linux 74% Win.	2019
[35]	Building an Effective Intrusion Detection System Using the Modified Density Peak Clustering Algorithm and Deep Belief Networks	Anomaly-Based	MDPCA (modified density peak clustering algorithm), DBN	Big data processing,Comparison study	NSL-KDD, UNSW-NB15	97.5%	2019
[36]	Comparative Study between Big Data Analysis Techniques in Intrusion Detection	Anomaly-Based	DT	DoS detection,IoT and ICN focus	MAWILab	99.95%	2018
[37]	Detection of DoS Attacks for IoT in Information-Centric Networks Using Machine Learning: Opportunities, Challenges, and Future Research Directions	Signature-Based	NN, DT, clustering algorithms, J48, XGBoost, (DNNs), MLP-BP, RBF-PSO, RBF-JAYA	Fuzzy clustering, Enhanced accuracy	ndnSIM		2024
[38]	Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering	Anomaly-Based	RF, KNN,DT, SVM,LSTM,ANN	Web threats,Real-time detection	NSL-KDD	RF: 99.50%	2025

[39]	AI-IDS: Application of deep learning to real-time web intrusion detection	Hybrid	CNN,LSTM	Combining RNN and SVM,High accuracy	CSIC-2010, CICIDS2017	91-93%	2020
[40]	HDLNIDS: Hybrid Deep-Learning-Based Network Intrusion Detection System	Hybrid	RNN,SVM	Cloud deployment,Model fusion	CICIDS-2018	98.90%	2023
[41]	Intrusion Detection on AWS Cloud through Hybrid Deep Learning Algorithm	Anomaly-Based	LSTM,RF	Feature selection,Optimization techniques	CSE-CIC-IDS-2018	95.3%	2023
[42]	A Novel Anomaly-Based Intrusion Detection Model Using PSOGWO-Optimized BP Neural Network GA-Based Feature Selection	Anomaly-Based	PSO – Grey Wolf Optimizer	Evaluation metrics,Performance measurement	NSL-KDD	94.2%	2022
[43]	EM-AUC: A Novel Algorithm for Evaluating Anomaly Based Network Intrusion Detection systems	Anomaly-Based	evaluation metrics for anomaly-based NIDS	Feature selection methods,High accuracy	NSL-KDD, UNSW-NB15		2025
[44]	Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms	Comparative	DT,KNN, RF, SVM, feature selection, Correlation-based Feature Selection, GA	Comparing ML & DL,Performance benchmarking	IoTID20	Without FS: 99.94%, 99.95%, 99.71%, 99.81% With GA: 100%, 100%,88.29%,99.90%	2024
[45]	Deep Learning vs. Machine Learning for Intrusion Detection in Computer Networks: A Comparative Study	Anomaly-Based	MLP,CNN, LSTM, Logistic regression, NB,RF,DT,KNN	Incident response, Cloud security	cicids2017	98%, 99.9%	2025
[46]	AI-Enabled System for Efficient and Effective Cyber Incident Detection and Response in Cloud Environments	Anomaly-Based	Random Forest, Isolation Forest, Neural Networks	Cloud & federated learning, Model diversity	NSL-KDD, UNSW-NB15, CIC-IDS-2017, Malware dataset	96%	2024
[47]	AI-Powered Intrusion Detection Systems for Next-Generation Cloud Security	Anomaly-Based	CNN, LSTM, DT, SVM, RF, Federated Learning	Kubernetes integration, Adaptive deception	NSL-KDD, CICIDS2017, UNSW-NB15	CNN: 98.5%, LSTM: 97.8%, (RF): 94.6%, (SVM): 92.8%, (DT): 91.3%	2025
[48]	Real-time Multi-class Threat Detection and Adaptive Deception in Kubernetes Environments	Anomaly-Based	PCA + Auto encoders for multi-class classification	Improved Accuracy in IoT, Reducing false positives		91% - detection 93% - decoy success rate	2025

5. Action Plan

Table 2: Summary of used Algorithms and Applied Procedures

Ref.	Name	algorithm	Implemented actions
[1]	An Efficient CNN-Based Intrusion Detection System for IoT	CNN	automatically extract spatial features from IoT traffic.
[2]	Big Data-Driven Deep Learning Ensembler for DDoS	SVM, ANN-GWO, GRU-RNN, CNN, LSTM, and DBN	Combined multiple DL models (CNN, LSTM, GRU, DBN) with ML (SVM, ANN-GWO) for ensemble accuracy
[3]	Multiple Kernel Transfer Learning for Enhancing NIDS	Transfer learning	Applied transfer learning to improve model generalization on encrypted and heterogeneous data
[4]	End-to-End Network IDS Based on Contrastive Learning	CNN and GRU	Used contrastive learning with CNN and GRU to learn better feature representations
[5]	TDCGAN Model for Data Balancing and IDS	TDC(traffic data conditional) (GAN), DT, RF	Used GANs (TDCGAN) for balancing datasets before training classifiers
[6]	Rapid Forecasting of Cyber Events Using ML	SVM , RF, Naïve bayes , time series	Combined time series and classic ML models (SVM, RF, Naive Bayes) for early warning
[7]	DDoS Detection through ML & Data Processing	RF,DT,ADA (AdaBoost),XGB (Extreme Gradient Boosting)	Applied ensemble models (RF, DT, XGBoost, AdaBoost) for boosted detection
[8]	DL and Data Augmentation for IDS	CNN	Used CNN with data augmentation to improve training and robustness
[9]	Intelligent IDS for Cloud	Radial Basis RBFNN) ,RF	Used RF and RBFNN with optimized cloud-based IDS for malicious activity classification

[10]	ML Multiclass for IoT Real-Time Detection	OneVsRest , SMOTE	Applied One-vs-Rest and SMOTE for multiclass classification and imbalance correction
[11]	Near-Real-Time IDS for IoT via Apache Spark	DT,RF	Used Apache Spark with DT and RF for scalable real-time detection
[12]	Ensemble DL Models for IoT IDS	CNN,LSTM,GRU	Built ensemble using CNN, LSTM, GRU for stronger detection capability
[13]	Feature Extraction with ML in IoT	VGG-16, DenseNet,RF,KNN,SVM	Utilized pretrained CNNs (VGG-16, DenseNet) with ML classification
[14]	SDN-Enabled IDS in IoT Networks	LSTM.SVM, CNN	Combined LSTM, CNN, SVM in an SDN-enabled framework
[15]	IDS Using BoT-IoT	ensemble bag ,DT	Ensemble bagging with DT optimized on Bot-IoT
[16]	Malicious Smart Contract and IDS for IoT	LSTM,GRU,	LSTM and GRU models used to detect blockchain-related threats
[17]	Realguard: Lightweight IDS for IoT Gateways	DNN	Used lightweight DNN architecture for resource-constrained IoT
[18]	PSO + DL for IoMT IDS	PSO,LSTM, CNN	PSO used for parameter tuning of LSTM/CNN hybrid in IoMT
[19]	PCA for IDS Using SVM Kernels	SVM	Applied PCA to reduce feature dimensionality before using SVM with different kernels
[20]	Ensemble IDS in IoT	Binary and Multi-classification	Used classification voting ensemble on multiple IoT datasets
[21]	Deep Learning Model for NIDS with Imbalanced Data	LSTM,GRU	Used LSTM and CNN with class weighting to handle imbalanced data
[22]	IMIDS: Intelligent IDS for IoT	LSTM,CNN	Utilized CNN on IoT-specific datasets to enhance pattern learning
[23]	IIoT Malware Detection with Edge Computing	CNN	Implemented CNN with edge computing for low-latency threat detection
[25]	DualAC2NN: Alert Fatigue Alleviation	RF,RT, Naïve bayes , Hoeffding tree	Used CNN with dual attention mechanisms to reduce redundant alerts
[26]	DL-Based IDS for IoT Botnet Attacks (Review)	CNN	Analyzed DL methods like RNN, CNN, and MLP on botnet detection
[27]	CoLL-IoT: Collaborative IDS for IoT	RNN,SNN,MLP,KNN, CNN, LSTM	Introduced a collaborative lightweight architecture for IoT device security
[29]	IntruDTree: ML-Based IDS	SVM, k-NN , DT	Compared classic ML algorithms (KNN, SVM, NB) on cyber intrusion tasks
[30]	ML Techniques in Cyber Security: Comparison	NB,LR, KNN,SVM	Benchmarked multiple ML algorithms like DT, RF, DBN on large datasets
[31]	Review of Insider Threat Detection	NB, RF, DT, SVM, DBN, ANN	Discussed RNNs and GRUs for sequential insider behavior detection
[32]	Anomaly-Based IDS in IoT Using DL	LSTM , GRU	Surveyed CNN and AE architectures across various datasets
[33]	Lightweight IDS for Fog Computing	AE ,CNN	Applied MLP tuned for fog node resource constraints
[34]	Modified Density Peak Clustering and DBN	MLP	Combined unsupervised clustering (MDPCA) with DBN for classification
[35]	Big Data Analysis for IDS	MDPCA (modified density peak clustering algorithm), DBN	Used Decision Trees in big data environments for performance benchmarking
[36]	DoS Attack Detection in ICNs Using ML	DT	Used ensemble and optimization-based ML techniques for attack detection
[37]	Signature-Based IDS with ML & DL	NN, DT, clustering algorithms, J48, MLP XGBoost, (DNNs), MLP-BP, RBF-PSO,	Combined RF, SVM, and DL with fuzzy clustering for enhanced signature match
[38]	AI-IDS: DL for Real-Time Web Intrusion Detection	RF, KNN,DT, SVM,LSTM,ANN	Applied CNN and LSTM for web traffic analysis in real time
[39]	HDLNIDS: Hybrid Deep Learning IDS	CNN,LSTM	Integrated RNN with SVM in a hybrid IDS for performance boost
[40]	Intrusion Detection on AWS Cloud	RNN,SVM	Combined LSTM and RF deployed in cloud to detect real-time intrusions
[41]	PSOGWO + GA-Based Anomaly IDS	LSTM,RF	Used PSOGWO for BP Neural Net optimization and GA
[42]	EM-AUC: Algorithm Evaluation for Anomaly-Based NIDS	PSO – Grey Wolf Optimizer	Introduced a new metric EM-AUC for evaluating IDS
[43]	Anomaly IDS for DoS in IoT	anomaly-based NIDS	Applied multiple feature selection methods with ML classifiers
[44]	DL vs ML for IDS: Comparative Study	DT,KNN, RF, SVM, Feature Selection, GA	Compared DL (CNN, LSTM) and ML (RF, DT, SVM) on IDS datasets
[45]	AI-Enabled System for Cyber Incident Detection in Cloud	MLP,CNN, LSTM, NB,RF,DT,KNN	Used Isolation Forest and NN with feature selection for cloud threats
[46]	AI-Powered IDS for Next-Gen Cloud Security	Random Forest, Isolation Forest, Neural Networks	Combined CNN, LSTM, FL with traditional ML for scalable detection
[47]	Real-time Threat Detection in Kubernetes	CNN, LSTM, DT, SVM, RF, Federated Learning	Used PCA + Autoencoders for classifying and reacting to threats in containers
[48]	An Efficient CNN-Based Intrusion Detection System for IoT	PCA + Autoencoders for multi-class classification	Used CNN to automatically extract spatial features from IoT traffic data

6. Datasets used in the survey selected articles :

The following table 2 lists all datasets used in our selected researches:

TABLE 2: Datasets used in Systems Deployments

Ref.	Dataset Name	Data Size	Dataset Type	Additional Details
[51]	UNSW-NB15	2,540,044 records	Network Intrusion Detection	Contains nine types of attacks, including Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms.
[52]	IoT-23	IoT-23: 1,048,576 records; APA-DDoS: 151,201 records	IoT Malware and DDoS Detection	IoT-23 consists of 20 malware captures and 3 benign captures from IoT devices, while APA-DDoS focuses on network connection characteristics for DDoS detection.
[53]	CIC-IDS-2017	Not specified	Intrusion Detection Evaluation	Includes various attack scenarios such as DoS, DDoS, and Brute Force.
[54]	CSE-CIC-IDS2018	Not specified	Intrusion Detection Evaluation	Captures modern attack scenarios and benign traffic.
[55]	KDD Cup 1999	~4 million instances	Network Intrusion Detection	Derived from DARPA 1998 dataset; widely used for intrusion detection research.
[56]	ADFA-LD	Not specified	Host-Based Intrusion Detection	Includes Linux-based system call traces of normal and malicious activity.
[57]	CSE-CIC-IDS2019	Not specified	Network Intrusion Detection	Captures modern attack scenarios and benign traffic.
[58]	NSL-KDD	~148,517 records	Network Intrusion Detection	An improved version of KDD Cup 99 dataset with reduced redundancy.
[59]	CICDDoS2019	~3 million records	DDoS Attack Detection	Includes common real-world DDoS attack scenarios.
[60]	5G-NIDD	~2.2 GB (raw data)	5G Network Intrusion Detection	A dataset for testing intrusion detection in 5G networks.
[61]	FLNET2023	Not specified	Network Intrusion Detection (Federated Learning)	A benchmark dataset for intrusion detection in Federated Learning environments.
[62]	KDD99	~4 million instances	Network Intrusion Detection	Same as KDD Cup 99; widely used for evaluating IDS models.
[63]	Australian Defence Force Academy (ADFA) IDS Datasets	Not specified	Host-Based Intrusion Detection	Includes datasets for Linux and Windows system call-based intrusion detection.
[64]	CSIC-2010	~61,000 HTTP requests	Web Application Intrusion Detection	Web traffic dataset with normal and attack requests, covering SQL injection, buffer overflow, XSS, and more.
[65]	Schonlau	50 user profiles, 15,000 commands each	Masquerade Detection	UNIX command dataset for detecting masquerading attacks.
[66]	CERT Insider Threat Test Dataset	~87.23 GB	Insider Threat Detection	Simulated dataset for detecting insider threats in enterprise environments.

7. Limitations

TABLE 3: Overview of IDS paper limitation

Paper Ref.	Title	Scalability	False Positives	Interpretability
[1]	An Efficient CNN-Based Intrusion Detection System for IoT	CNNs are computationally intensive and not well-suited for resource-constrained IoT devices. Scalability to large or real-time deployments is not addressed.	While the model aims to improve accuracy, there is no explicit evaluation or mitigation strategy for false positives	The deep learning-based model operates as a black box, and no interpretability methods (e.g., SHAP, LIME) are discussed.
[2]	Big Data-Driven Deep Learning Ensembler for DDoS Attack Detection	The ensemble model integrates multiple DL architectures for big data, but its real-time scalability and processing efficiency under high throughput is not demonstrated.	False positive mitigation is claimed via ensemble learning, but detailed analysis or metrics are not provided.	The model is complex, involving GRU, GhostNet, and PCA-LLP, making interpretability difficult. No explanation mechanisms are offered.
[3]	Multiple Kernel Transfer Learning for Enhancing Network Intrusion Detection	DetMKTL requires training many kernel classifiers, which limits scalability. StoMKTL improves efficiency but still requires validation in large-scale settings.	The effect of the model on false positives is not discussed, despite the emphasis on accuracy and domain adaptation.	The transfer learning framework with multiple kernels is opaque, and no interpretability methods are included.
[4]	End-to-End Network Intrusion Detection Based on Contrastive Learning	Processing raw PCAP data through CNN and GRU layers adds computational overhead. Scalability to real-time detection is not tested.	The false positive rate is not detailed or compared to other models, despite reporting high accuracy.	Contrastive learning and deep neural nets lack transparency. Interpretability is not addressed at all.
[5]	A Comparative Analysis of the TDCGAN Model for Data Balancing and Intrusion Detection	GAN-based data balancing improves accuracy but adds training overhead. Its scalability in production settings remains unverified.	The paper improved minority class detection, but no direct mitigation or measurement for false positives is provided.	GANs and ensembles are hard to interpret. The paper does not discuss any means to explain decisions.
[6]	Rapid Forecasting of Cyber Events Using Machine Learning-Enabled Features	The model is designed for time-sensitive detection but does not discuss long-term scalability or streaming input processing.	No specific evaluation of false positive rate or how the model reduces them.	Used traditional ML models, which could be interpretable, but no tools or explanations are provided in the paper.
[7]	Improvement of DDoS Attack Detection through Machine Learning and Data Processing	Boosting models like XGBoost are used, but the paper lacks analysis on scalability in large-scale, high-traffic networks.	False alarms are mentioned as a challenge, yet there's no quantitative comparison of FP reduction.	The paper does not explore how predictions can be interpreted or understood by users or analysts.
[8]	Enhancing IDS Using Deep Learning and Data Augmentation	Combining DL with data augmentation increases training complexity; real-time scalability is not evaluated.	Improved detection accuracy is shown, but the effect on false positives is not explicitly analyzed.	No efforts are made to explain how DL models make predictions, despite using complex architectures.
[9]	Towards an Intelligent IDS to Detect Malicious Activities in Cloud Computing	Cloud infrastructure is addressed, but no benchmarking or distributed scalability tests are included.	Mitigation strategies or analysis of FP are not included, despite mentioning malicious activity detection.	Model explanations or interpretability are not considered in the design or evaluation.

[10]	Using ML Multiclass Classification Technique to Detect IoT Attacks in Real Time	Real-time classification is proposed, but there's no performance benchmark for large-scale IoT deployments.	SMOTE is used for imbalance, which may affect FP rate, but no results or controls for FP are discussed.	The use of One-vs-Rest classification is interpretable in theory, yet no explanation framework is applied.
[11]	Towards Near-Real-Time Intrusion Detection for IoT Devices using Supervised Learning and Apache Spark	Uses Apache Spark for distributed processing, which supports scalability, but lacks detailed benchmarks for IoT-scale deployments.	No quantitative analysis of false positives is presented.	Traditional models like decision trees and random forests are used, but interpretability is not emphasized.
[12]	Ensemble-Based Deep Learning Models for Enhancing IoT Intrusion Detection	Deep ensembles increase computational overhead; real-time scalability not tested.	False positives may be reduced through ensemble averaging, but not explicitly measured or compared.	Combining LSTM, GRU, CNN makes the model a black box; interpretability is not addressed.
[13]	IDS Using Feature Extraction with ML Algorithms in IoT	Applies feature extraction for efficiency, but the modelâ€™s ability to scale with streaming IoT data is not evaluated.	Paper focuses on overall accuracy, with no specific metrics or discussion on false positives.	Uses ML models like RF and KNN which can be interpretable, but no interpretability techniques are applied.
[14]	DL Approach for SDN-Enabled IDS in IoT Networks	SDN adds control layer efficiency, but no stress testing or scale-out demonstration is provided.	No specific effort to measure or reduce false positives is discussed.	Uses CNN, LSTMâ€”complex models with no interpretability strategy or analysis.
[15]	An Intrusion Detection System Using BoT-IoT	Focused on BoT-IoT dataset performance; real-world scalability is not analyzed.	High accuracy is achieved, but FP rates are not highlighted or contrasted.	Model selection focuses on performance rather than explainability; interpretation not explored.
[16]	DL-Based Malicious Smart Contract and IDS for IoT	Smart contract evaluation with DL adds computational burden; lacks deployment analysis.	False positive mitigation is not analyzed despite claiming high accuracy.	Uses LSTM and GRU, which are complex and hard to interpret; no explanation offered.
[17]	Realguard: A Lightweight NIDS for IoT Gateways	Designed to be lightweight, yet lacks quantitative benchmarks across multiple IoT gateway types.	Claims good detection but no discussion on FP impact or rates.	Interpretability of DNNs used is not discussed, despite lightweight intention.
[18]	PSO and Deep Learning for IDS in Internet of Medical Things	Medical IoT setups require high performance, but DL and PSO can be computationally intensive; scalability not demonstrated.	The paper lacks detailed analysis of false positive rate reduction.	No model explanation methods used; DL + PSO systems are hard to interpret.
[19]	PCA for IDS Using Different SVM Kernels	PCA reduces dimensionality, supporting scalability; kernel selection may affect performance on larger datasets.	FP rates are not analyzed individually for each kernel.	SVMs can be moderately interpretable, but kernel decisions are not clarified or visualized.
[20]	Evaluation and Selection Models for Ensemble IDS in IoT	Focuses on evaluation criteria but does not benchmark real-time performance or resource efficiency.	No comparative false positive rate analysis across evaluated models.	Model selection is emphasized, but interpretability trade-offs are not discussed.

[21]	Composite IDS: Hybrid RNN + Feature Optimization	Hybrid models increase complexity; large-scale applicability not validated.	FP reduction is implied through feature optimization, but not separately measured.	RNNs are black-box models; no explainability framework is used.
[22]	DL Model for NIDS with Imbalanced Data	DL approach focuses on class imbalance but doesnâ€™t assess scalability in data-rich environments.	FP rate affected by imbalance but not directly quantified in results.	DL model not interpreted; focus is on metrics, not model reasoning.
[23]	IMIDS: Intelligent IDS for IoT	Designed for IoT, but lacks tests across varied edge devices or network scales.	High accuracy is noted, but FP metrics are not detailed.	No model transparency features discussed; CNN-based system lacks interpretability tools.
[24]	IIoT Malware Detection via Edge Computing + DL	Edge computing improves response time, but scalability across factory environments not benchmarked.	FP issues in malware detection are not addressed in the analysis.	Uses CNNs; deep model decisions are not explained.
[25]	Zero-Day Attack Detection with Supervised Learning (Springer)	Zero-day detection in streaming is discussed, but system scalability under load is not empirically tested.	Claims low FP rate but lacks multi-dataset validation or specific breakdowns.	Interpretability of alerts in streaming contexts is not analyzed.
[26]	DualAC2NN: Revisiting and Alleviating Alert Fatigue	Paper focuses on reducing alert fatigue, but scalability to large enterprise environments isn't tested.	Addresses false positive overload by neural architecture tuning; lacks rigorous cross-dataset testing.	DL-based, interpretability is not part of the approach; black-box limitations acknowledged indirectly.
[27]	DL-Based IDS for IoT Botnet Attacks: A Review	Being a review, it cites models with both scalable and non-scalable traits but doesnâ€™t evaluate them experimentally.	Highlights that many models still suffer high FP rates; emphasizes the need for better evaluation.	Concludes that most DL models are opaque; stresses the lack of interpretable methods as a key gap.
[28]	CoLL-IoT: Collaborative IDS for IoT	Collaborative nature helps scalability, but resource constraints in low-power IoT environments remain a concern.	The paper mentions reducing FP via collaboration, but does not provide comparative FP metrics.	No interpretability technique is applied or discussed despite layered architecture.
[29]	Advanced Persistent Threat: A Survey	Focuses on APT detection methods conceptually, does not include implementation or scalability discussion.	Survey identifies that false positives in APT detection remain unresolved.	Notes that APT detection requires better interpretability but lacks model-level analysis.
[30]	IntruDTree: ML-Based Cybersecurity Intrusion Detection	Tree-based models scale moderately well, but high-volume network traffic testing	Claims low false positive rates, but does not benchmark against known IDS datasets.	Decision tree architecture is inherently interpretable; no enhanced or visualize explanations.
[31]	ML Techniques in Cybersecurity: Current Challenges	Compares scalability of ML methods; points out training time and resource bottlenecks.	Highlights that FP rates are still a major concern in real-time use.	Lack of transparency in DL models is a key challenge discussed throughout.
[32]	Review of Insider Threat Detection	Survey notes scalability issues for enterprise insider threat models due to large data variety.	Insider threat models suffer high FP due to subtle behavior anomalies.	Paper notes that limited model transparency hampers adoption in organizations.
[33]	Anomaly-Based IDS in IoT Using DL: SLR	Finds that most DL-based IDS for IoT lack lightweight scalability features.	Discusses FP as a persistent challenge with anomaly-based detection.	Interpretability is highlighted as a major research gap in surveyed models.

[34]	Lightweight Perceptron-Based IDS for Fog Computing	Designed for fog environments, it claims lightweight scalability but does not test large-scale deployments.	Claims acceptable FP rates, but lacks comparative benchmarks with existing methods.	Uses simple perceptron model, which is more interpretable, though not deeply discussed.
[35]	IDS with Density Peak Clustering and DBN	Scalability limited by deep belief network training complexity and clustering overhead.	Mitigates false positives with clustering, but real-world validation is missing.	Deep Belief Networks are black-box models, and no explainability method is used.
[36]	Big Data Analysis Techniques in IDS	Analyzes big data tools, highlighting scalability of techniques like Spark, but no experimental proof.	Describes comparative FP rates but without unified evaluation framework.	Interpretability is noted as lacking in most big data IDS pipelines surveyed.
[37]	Detection of DoS Attacks in ICN Using ML	Scalability challenges due to evolving ICN architectures and dataset limitations are highlighted.	Mentions FP issue in ICN due to content-level attacks, proposes use of hybrid models.	Interpretability is briefly discussed as a future direction, but not implemented.
[38]	Signature-Based IDS Using ML/DL + Fuzzy Clustering	Scalability is moderate; fuzzy clustering introduces computational burden for large traffic volumes.	Addresses FP using clustering refinement; needs cross-validation on diverse datasets.	Fuzzy logic helps interpret decision boundaries but DL components remain opaque.
[39]	AI-IDS for Real-Time Web Intrusion Detection	Real-time processing is targeted, but scalability under heavy concurrent traffic is not tested.	FP mitigation is discussed via fine-tuning DL model; lacks adversarial robustness checks.	Relies on deep learning with no interpretability or explainability module applied.
[40]	HDLNIDS: Hybrid Deep Learning-Based NIDS	Hybrid modelâ scalability is unclear; ensemble layers increase resource demands.	Claims reduced FP through hybridization, but experimental justification is brief.	Interpretability is not addressed; focus is on accuracy and hybrid design only.
[41]	Intrusion Detection on AWS Cloud Using Hybrid DL	Scalability for AWS is discussed but lacks testing on high-throughput multi-region environments.	Uses hybrid model to reduce FPs, but lacks quantitative comparison with benchmarks.	Hybrid deep learning model is complex; lacks interpretability techniques like SHAP or LIME.
[42]	Anomaly IDS Using PSOGWO-BP and GA Feature Selection	Heuristic and hybrid models increase complexity; real-time large dataset tests are absent.	Claims optimization improves FP reduction, but robustness to new attack types is unclear.	BP neural network lacks explaining model behavior isn't interpretable by design.
[43]	EM-AUC Algorithm for Evaluating Anomaly-Based NIDS	Focuses on evaluation metric, not deployment scalability.	Proposes new metric to evaluate FP impact better, improving model tuning.	Indirectly supports interpretability through evaluation insight but no model-specific tools used.
[44]	Anomaly Detection IDS for DoS in IoT Networks	Moderate scalability on IoT datasets, but not tested in real-time edge environments.	Claims balanced accuracy, but false positive rate not directly addressed in detail.	Model interpretability not covered; focus is on detection accuracy.

[45]	DL vs ML for Intrusion Detection: A Comparative Study	Highlights DL scalability issues on resource-constrained devices.	Compares FP trends across ML and DL but lacks generalization beyond benchmark datasets.	Notes DL is less interpretable, advocating for interpretable ML models where feasible.
[46]	AI-Enabled Cyber Incident Detection in Cloud (arXiv)	Scalability in cloud workloads is discussed theoretically; lacks live deployment validation.	Mentions the use of ensemble techniques to reduce FP but lacks statistical validation.	No discussion of how results are interpreted or explained to users.
[47]	AI-Powered IDS for Next-Gen Cloud Security	Promotes AI scalability in cloud but lacks benchmarking under real-world scale.	Mentions threat adaptation to reduce FP, yet quantitative FP rates are not provided.	Emphasizes automation and adaptation, but little on interpretability or transparency.
[48]	Real-Time Multi-Class Threat Detection in Kubernetes	Demonstrates real-time detection in Kubernetes, but latency benchmarks are brief.	Adaptive deception techniques proposed to minimize FP; lacks comparison to other frameworks.	Interpretability not a focus; model decisions are treated as opaque.

TABLE 4: IDS Taxonomy summary

Category	Class	No. of Papers
Detection Type	Signature-Based	3
Detection Type	Anomaly-Based	30
Detection Type	Hybrid	15
ML Method	Traditional ML	12
ML Method	Deep Learning	20
ML Method	Hybrid/Ensemble Models	16
Application Area	IoT	22
Application Area	Cloud	14
Application Area	Edge/Fog/IIoT	9
Research Focus	Scalability	40
Research Focus	False Positive Reduction	35
Research Focus	Interpretability	33

8. Conclusion

Implementing an anomaly-based NIDS in real-time cloud environments offers significant advantages in detecting previously unknown attacks by identifying deviations from established standard behavior patterns. Techniques such as machine learning and deep learning have been instrumental in enhancing detection capabilities. For instance, the applications of deep learning methods have shown promise in improving intrusion detection performance within cloud computing contexts. However, challenges persist, including managing high volumes of data, reducing false positives, and ensuring timely detection without compromising system performance.

Open Problems and Questions - The study "Real-time multi-class threat detection and adaptive deception in Kubernetes environments" where proposes an integrated framework that combines machine learning-based multi-class threat detection with adaptive deception tailored for Kubernetes [48]. While the framework presents a novel and practical approach, several research gaps and opportunities for future work remain:

- Lack of Integration with SIEM Platforms

Integrating with siem is crucial for security teams as it monitors and responds to attacks or threats, so it is not effective to let the system work by itself without integration.

- Absence of Automated Model Retraining

New types of attacks are easy to appear as the model is trained once and relies on static configuration (PCA and autoencoders), so it misses the zero-day attack advantage. It may be outdated if the model does not learn automatically.

- Incomplete MAPE-K Implementation

MAPE-K: It is a model used to create self-adaptive systems that can make decisions, monitor, and adjust automatically without human input, so incomplete implementation may affect the above characteristics.

- Scalability and Resilience at the Production Scale

Current evaluation is limited to controlled environments. There is insufficient evidence regarding the framework's performance under production-scale workloads, high-velocity traffic, or multi-tenant environments. Future research should assess latency, accuracy, and fault tolerance in enterprise settings.

- Susceptibility to Decoy Evasion

They use Decoys (fake services to fool attackers), but some attackers can gain access to them, so if that happens, the prevention or detection becomes useless.

- Narrow Attack Scope and Dataset Diversity

The detection model was evaluated using 10 crafted attack scenarios based on specific CVEs. This restricts generalizability. Broader evaluations using public, real-world datasets and additional threat vectors (e.g., insider attacks, data exfiltration) are necessary.

- Lack of Multi-Cloud and Multi-Cluster Support

The proposed system is currently limited to a single Kubernetes cluster. Extending the framework to support multi-cloud and federated Kubernetes environments would address real-world deployment needs in distributed cloud-native infrastructures.

References

[1] Deshmukh, A., & Ravulakollu, K. (2024). An Efficient CNN-Based Intrusion Detection System for IoT: Use Case Towards Cybersecurity. *Technologies*, *12(10), 203.* https://doi.org /10.3390/ technologies12100203).

[2] Alshdadi, A. A., Almazroi, A. A., Ayub, N., Lytras, M. D., Alsolami, E., & Alsubaei, F. S. (2024). Big Data-Driven Deep Learning Ensembler for DDoS Attack Detection. *Future Internet, 16(12), 458.* https://doi.org/10.3390/fi16120458.

[3] Amamra, A., & Terrelonge, V. (2025). Multiple Kernel Transfer Learning for Enhancing Network Intrusion Detection in Encrypted and Heterogeneous Network Environments. *Electronics, 14(1), 80.* https://doi.org/10.3390/electronics14010080.

[4] Li, L., Lu, Y., Yang, G., & Yan, X. (2024). End-to-End Network Intrusion Detection Based on Contrastive Learning. *Sensors, 24(7), 2122.* https://doi.org/10.3390/s24072122.

[5] Jamoos, M., Mora, A. M., AlKhanafseh, M., & Surakhi, O. (2024). A Comparative Analysis of the TDCGAN Model for Data Balancing and Intrusion Detection. *Signals, 5(3), 580-596.* https://doi.org/10.3390/signals5030032.

[6] Ahmed, Y., Azad, M. A., & Asyhari, T. (2024). Rapid Forecasting of Cyber Events Using Machine Learning-Enabled Features. *Information, 15(1), 36.* https://doi.org/10.3390/info15010036.

[7] Becerra-Suarez, F. L., Fernández-Roman, I., & Forero, M. G. (2024). Improvement of Distributed Denial of Service Attack Detection through Machine Learning and Data Processing. *Mathematics, 12(9), 1294.* https://doi.org/10.3390/math12091294.

[8] Rasheed, M., Saeed, F., Almazroi, A. A., Alsubaei, F. S., & Almazroi, A. A. (2024). Enhancing Intrusion Detection Systems Using a Deep Learning and Data Augmentation Approach. *Systems, 12*(3), 79. https://doi.org/10.3390/systems12030079

[9] Attou, H., Mohy-eddine, M., Guezzaz, A., Benkirane, S., Azrour, M., Alabdultif, A., & Almusallam, N. (2023). Towards an Intelligent Intrusion Detection System to Detect Malicious Activities in Cloud Computing. *Applied Sciences, 13*(17), 9588. https://doi.org/10.3390/app13179588

[10] Alrefaei, A., & Ilyas, M. (2024). Using Machine Learning Multiclass Classification Technique to Detect IoT Attacks in Real Time. *Sensors, 24*(14), 4516. https://doi.org/10.3390/s24144516

[11] Morfino, V., & Rampone, S. (2020). Towards Near-Real-Time Intrusion Detection for IoT Devices using Supervised Learning and Apache Spark. *Electronics, 9*(3), 444. https://doi.org/10.3390/electronics9030444

[12] deh, A., & Abu Taleb, A. (2023). Ensemble-Based Deep Learning Models for Enhancing IoT Intrusion Detection. *Applied Sciences, 13*(21), 11985. https://doi.org/10.3390/app132111985

[13] Musleh, D., Alotaibi, M., Alhaidari, F., Rahman, A., & Mohammad, R. M. (2023). Intrusion Detection System Using Feature Extraction with Machine Learning Algorithms in IoT. *J. Sens. Actuator Netw.*, 12(2), 29. https://doi.org/10.3390/jsan12020029

[14] Chaganti, R., Suliman, W., Ravi, V., & Dua, A. (2023). Deep Learning Approach for SDN-Enabled Intrusion Detection System in IoT Networks. *Information*, 14(1), 41. https://doi.org/10.3390/info14010041

[15] Alosaimi, S., & Almutairi, S. M. (2023). An Intrusion Detection System Using BoT-IoT. Applied Sciences, 13(9), 5427. https://doi.org/10.3390/app13095427

[16] Shah, H., Shah, D., Jadav, N. K., Gupta, R., Tanwar, S., Alfarraj, O., Tolba, A., Raboaca, M. S., & Marina, V. (2023). Deep Learning-Based Malicious Smart Contract and Intrusion Detection System for IoT Environment. *Mathematics*, 11(2), 418. https://doi.org/10.3390/math11020418

[17] Nguyen, X.-H., Nguyen, X.-D., Huynh, H.-H., & Le, K.-H. (2022). Realguard: A Lightweight Network Intrusion Detection System for IoT Gateways. *Sensors*, 22(2), 432. https://doi.org/10.3390/s22020432

[18] Chaganti, R., Mourade, A., Ravi, V., Vemprala, N., Dua, A., & Bhushan, B. (2022). A Particle Swarm Optimization and Deep Learning Approach for Intrusion Detection System in Internet of Medical Things. *Sustainability*, *14*(19), 12828. https://doi.org/10.3390/su141912828

[19] Almaiah, M. A., Almomani, O., Alsaaidah, A., Al-Otaibi, S., Bani-Hani, N., Al Hwaitat, A. K., Al-Zahrani, A., Lutfi, A., Bani Awad, A., & Aldhyani, T. H. H. (2022). Performance Investigation of Principal Component Analysis for Intrusion Detection System Using Different Support Vector Machine Kernels. *Electronics*, *11*(21), 3571. https://doi.org/10.3390/electronics11213571

[20] Alghamdi, R., & Bellaiche, M. (2022). Evaluation and Selection Models for Ensemble Intrusion Detection Systems in IoT. *IoT*, *3*(2), 285–314. https://doi.org/10.3390/iot3020017

[21] Gautam, S., Henry, A., Zuhair, M., Rashid, M., Javed, A. R., & Maddikunta, P. K. R. (2022). A Composite Approach of Intrusion Detection Systems: Hybrid RNN and Correlation-Based Feature Optimization. *Electronics*, *11*(21), 3529. https://doi.org/10.3390/electronics11213529

[22] Fu, Y., Du, Y., Cao, Z., Li, Q., & Xiang, W. (2022). A Deep Learning Model for Network Intrusion Detection with Imbalanced Data. *Electronics*, *11*(6), 898. https://doi.org/10.3390/electronics11060898

[23] Le, K.-H., Nguyen, M.-H., Tran, T.-D., & Tran, N.-D. (2022). IMIDS: An Intelligent Intrusion Detection System against Cyber Threats in IoT. *Electronics*, *11*(4), 524. https://doi.org/10.3390/electronics11040524

[24] Kim, H., & Lee, K. (2022). IIoT Malware Detection Using Edge Computing and Deep Learning for Cyber security in Smart Factories. *Applied Sciences*, *12*(15), 7679. https://doi.org/10.3390/app12157679

[25] https://link.springer.com/chapter/10.1007/978-981-19-0011-2_46

[26] Yang, G., Tang, C., & Liu, X. (2022). DualAC2NN: Revisiting and Alleviating Alert Fatigue from the Detection Perspective. *Symmetry*, *14*(10), 2138. https://doi.org/10.3390/sym14102138

[27] Al-Shurbaji, T., Anbar, M., Manickam, S., Hasbullah, I. H., Alfriehat, N., Alabsi, B. A., Alzighaibi, A. R., & Hashim, H. (2023). Deep Learning-Based Intrusion Detection System for Detecting IoT Botnet Attacks: A Review. 10.1109/ACCESS.2025.352671

[28] Alshahrani, H. M. (2021). CoLL-IoT: A Collaborative Intruder Detection System for Internet of Things Devices. *Electronics*, *10*(7), 848. https://doi.org/10.3390/electronics10070848

[29] Quintero-Bonilla, S., & Martín del Rey, A. (2020). A New Proposal on the Advanced Persistent Threat: A Survey. *Applied Sciences*, *10*(11), 3874. https://doi.org/10.3390/app10113874

[30] Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. (2020). IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model. *Symmetry*, *12*(5), 754. https://doi.org/10.3390/sym12050754

[31] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J. (2020). Performance Comparison and Current Challenges of Using Machine Learning Techniques in Cyber security. *Energies*, *13*(10), 2509. https://doi.org/10.3390/en13102509

[32] Al-Mhiqani, M. N., Ahmad, R., Abidin, Z. Z., Yassin, W., Hassan, A., Abdulkareem, K. H., Ali, N. S., & Yunos, Z. (2020). A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations. *Applied Sciences*, *10(15)*, *5208*. https://doi.org/10.3390/app10155208.

[33] Alsoufi, M. A., Razak, S., Md Siraj, M., Nafea, I., Ghaleb, F. A., Saeed, F., & Nasser, M. (2021). Anomaly-Based Intrusion Detection Systems in IoT Using Deep Learning: A Systematic Literature Review. *Applied Sciences*, *11(18)*, *8383*. https://doi.org/10.3390/app11188383.

[34] Khater, B. S., Abdul Wahab, A. W. B., Idris, M. Y. I. B., Hussain, M. A., & Ibrahim, A. A. (2019). A Lightweight Perceptron-Based Intrusion Detection System for Fog Computing. *Applied Sciences*, *9(1)*, *178*. https://doi.org/10.3390/app9010178.

[35] Yang, Y., Zheng, K., Wu, C., Niu, X., & Yang, Y. (2019). Building an Effective Intrusion Detection System Using the Modified Density Peak Clustering Algorithm and Deep Belief Networks. *Applied Sciences*, *9(2)*, *238*. https://doi.org/10.3390/app9020238.

[36] Hafsa, M., & Jemili, F. (2019). Comparative Study between Big Data Analysis Techniques in Intrusion Detection. *Big Data and Cognitive Computing*, 3(1), 1. https://doi.org/10.3390/bdcc3010001

[37] Bukhowah, R., Aljughaiman, A., & Rahman, M. M. H. (2024). Detection of DoS Attacks for IoT in Information-Centric Networks Using Machine Learning: Opportunities, Challenges, and Future Research Directions. *Electronics*, 13(6), 1031. https://doi.org/10.3390/electronics13061031

[38] Ahmed, U., Nazir, M., Sarwar, A., Ali, T., Aggoune, E.-H. M., Shahzad, T., & Khan, M. A. (2025). Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering. *Scientific Reports*, *15*, Article 1726. *Nature Portfolio*. https://www.nature.com/articles/s41598-025-85866-7

[39] Kim, A., Park, M., & Lee, D. H. (2020). AI-IDS: Application of deep learning to real-time web intrusion detection. *IEEE Access*, *8*, 83946-83959. https://www.researchgate.net/publication/340571787_AI-IDS_Application_of_Deep_Learning_to_Realtime_Web_Intrusion_Detection

[40] Qazi, E. U. H., Faheem, M. H., & Zia, T. (2023). HDLNIDS: Hybrid deep-learning-based network intrusion detection system. *Applied Sciences*, *13*(8), 4921. https://doi.org/10.3390/app13084921

[41] Balajee, R. M., & Kannan, M. K. J. (2023). Intrusion detection on AWS cloud through hybrid deep learning algorithm. *Electronics*, *12*(6), 1423. https://doi.org/10.3390/electronics12061423

[42] Sheikhi, S., & Kostakos, P. (2022). A novel anomaly-based intrusion detection model using PSOGWO-optimized BP neural network and GA-based feature selection. *Sensors*, *22*(23), 9318. https://doi.org/10.3390/s22239318

[43] ai, K. Z., & Fossaceca, J. M. (2025). EM-AUC: A novel algorithm for evaluating anomaly-based network intrusion detection systems. *Sensors*, *25*(1), 78. https://doi.org/10.3390/s25010078

[44] Altulaihan, E., Almaiah, M.A., & Aljughaiman, A. (2024). Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms. *Sensors*, *24*(2), 713. https://doi.org/10.3390/s24020713

[45] Ali, M. L., Thakur, K., Schmeelk, S., Debello, J., & Dragos, D. (2025). Deep learning vs. machine learning for intrusion detection in computer networks: A comparative study. *Applied Sciences*, *15*(4), 1903. https://doi.org/10.3390/app15041903

[46] Farzaan, M. A. M., Ghanem, M. C., El-Hajjar, A., & Ratnayake, D. N. (2024). AI-Enabled System for Efficient and Effective Cyber Incident Detection and Response in Cloud Environments. Published on arXivhttps://arxiv.org/abs/2404.05602v4

[47] Smith, J., & Kevin, E. (2025). AI-Powered Intrusion Detection Systems for Next-Generation Cloud Security. ResearchGate. Retrieved from https://www.researchgate.net/publication/390448273

[48] ly, A., Hamad, A. M., Al-Qutt, M., & Fayez, M. (2025). Real-time multi-class threat detection and adaptive deception in Kubernetes environments. *Scientific Reports*, *15*, Article 91606. https://doi.org/10.1038/s41598-025-91606-8

[49] González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*, *21(14)*, *4759*. https://doi.org/10.3390/s21144759.

[50] González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*, *21(14)*, *4759*. https://doi.org/10.3390/s21144759.

[51] https://unsworks.unsw.edu.au/items/4dc0e35c-6196-4c9d-945a-c50b981e5955 accessed in [01-02-2025]

[52] https://www.stratosphereips.org/datasets-iot23 accessed in [10-02-2025]

[53] https://www.unb.ca/cic/datasets/ids-2017.html accessed in [20-02-2025]

[54] https://www.unb.ca/cic/datasets/ids-2018.html accessed in [21-02-2025]

[55] https://archive.ics.uci.edu/ml/datasets/kdd%2Bcup%2B1999%2Bdata accessed in [22-02-2025]

[56] https://research.unsw.edu.au/projects/adfa-ids-datasets accessed in [23-02-2025]

[57] https://www.unb.ca/cic/datasets/ddos-2019.html accessed in [24-02-2025]

[58] https://ieee-dataport.org/documents/nsl-kdd-0 access in [25-02-2025]

[59] https://www.unb.ca/cic/datasets/ddos-2019.html accessed in [25-02-2025]

[60] https://ieee-dataport.org/documents/5g-nidd-comprehensive-network-intrusion-detection-dataset-generated-over-5g-wireless accessed in [26-02-2025]

[61] https://github.com/nsol-nmsu/FML-Network accessed in [26-02-2025]

[62] https://archive.ics.uci.edu/ml/datasets/kdd%2Bcup%2B1999%2Bdata accessed in [26-02-2025]

[63] https://research.unsw.edu.au/projects/adfa-ids-datasets accessed in [27-02-2025]

[64] https://www.impactcybertrust.org/dataset_view?idDataset=940 accessed in [28-02-2025]

[65] https://schonlau.net/intrusion.html accessed in [01-03-2025]

[66] https://kilthub.cmu.edu/articles/dataset/Insider_Threat_Test_Dataset/12841247 accessed in [01-03-2025]