International Journal of Applied Mathematics

Volume 38 No. 10s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A SURVEY OF INTRUSION DETECTION SYSTEMS IN IOT: MACHINE LEARNING AND FEATURE SELECTION APPROACHES

Taha M.O. Alakhras[1], Waheed A. H. M. Ghanem[1,3,4], Farizah Yunus[1], Sanaa A. A. Ghaleb[2,5], Prof. Mohammed Otair[5]

[1]Faculty of Computer Science and Mathematics, Universiti Malaysia Terengganu, Terengganu, Malaysia

[2]Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Besut, Terengganu, Malaysia

[3]Faculty of Engineering, University of Aden, Aden, Yemen

[4]Faculty of Science and Education, University of Lahej, Lahej, Yemen

[5]Faculty of Education, University of Aden, Yemen

[5]Department of Computer Science, Faculty of Information Technology, Middle East University, Amman, Jordan

Corresponding author: P5189@pps.umt.edu.my, waheedghanem@umt.edu.my

Taha M.O. Alakhras[1]: email addresses P5189@pps.umt.edu.my.

Waheed A. H. M. Ghanem[1,3,4:] email addresses waheedghanem@umt.edu.my.

Farizah Yunus[1:] email addresses farizah.yunus@umt.edu.my.

Sanaa A. A. Ghaleb[2,5:] email addresses :sanaaabduljabbar@unisza.edu.my.

Mohammed Otair[5:] email addresses m.otair@meu.edu.jo.

Declarations

Competing interests: The authors declare that they have no competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Authors contributions: Taha M.O. Alakhras performed the comparative analysis and prepared the manuscript. Waheed A.H.M. Ghanem, Farizah Yunus, Sanaa A.A. Ghaleb, and Mohammed Otair provided critical review, validation, and valuable insights for revision. All authors read and approved the final manuscript.

Ethical approval: This material is the authors' own original work, which has not been previously published elsewhere. The paper is not currently being considered for publication elsewhere. The paper reflects the authors' own research and analysis in a truthful and complete manner.

Abstract

The Internet of Things (IoT) enables automation and seamless data flow by connecting billions of devices across multiple industries. However, this networked environment also poses serious security risks, including denial-of-service attacks, unauthorized access, and data leaks.

Received: August 09, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Intrusion Detection Systems (IDS) are essential for protecting IoT networks by detecting and halting malicious activity. This paper offers a comprehensive analysis of IDS created for IoT environments, looking at advancements, challenges, and possible patterns from 2020 to 2024. Hybrid IDS models have been created by combining multiple strategies to improve detection accuracy, scalability, and efficacy. While lightweight IDS frameworks balance robust security performance with the resource limitations of IoT devices, feature selection techniques further optimize these systems by reducing computational overhead. With some frameworks nearly reaching peak performance, deep learning and machine learning techniques have shown remarkable accuracy, often surpassing 95%. However, critical metrics like F1-score, accuracy, precision, and recall need to be carefully considered in order to assess these systems. This work also compares its results with popular datasets, such as NSL-KDD, CICIDS2017, UNSW-NB15, and Bot-IoT, among others, to enable meaningful comparisons between various IDS models. Emerging research employs synthetic data creation techniques to address problems like class imbalance, even as domain-specific IDS solutions for cloud-based IoT, industrial, and medical applications gain popularity. Despite these developments, there are still significant challenges, including the need for real-time flexibility and computational overhead. Finally, future research will probably focus on combining state-of-the-art artificial intelligence techniques like supervised and unsupervised learning to create adaptive, lightweight, and privacy-preserving IDS for IoT environments.

1 Keywords Intrusion Detection Systems (IDS), Internet of Things (IoT), feature selection, machine learning, deep learning, artificial intelligence, optimization algorithms

2 Abbreviations

1	Ant Colony Optimization (ACO)	**2**	Ant Colony Optimization (ACO)
3	Artificial Bee Colony (ABC)	4	Artificial Intelligence (AI)
5	Artificial Neural Network (ANN)	6	Bacterial Foraging Optimization (BFOA)
7	Bat Algorithm (BA)	8	Binary Particle Swarm Optimization (BPSO)
9	Binary Pigeon Inspired Optimize	10	Botnet Detection (BD)
11	Cat Swarm Optimization (CSO)	12	Chaotic Cuckoo Search Optimization (CCSO)
13	Chimp Optimization Algorithm (ChOA)	14	Convolutional Neural Networks (CNN)
15	Crow Search Algorithm (CSA)	16	Deep Neural Networks (DNN)

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

17	Entropy-Based Graph (EBG)	18	Extreme Learning Machine (ELM)
19	Feature Embedding (FEmb)	20	Feature Extraction (FExt)
21	Feature Optimization (FO)	22	Feature Pairs (FP)
23	Feature Reduction (FR)	24	Feature Selection (FS)
25	Federated Learning	26	Fog Computing (FL)
27	Generative Adversarial Networks (GAN)	28	Genetic Algorithm (GA)
29	Grey Wolf Optimization (GWO)	30	Hierarchical Long Short-Term Memory (HLSTM)
31	Hybrid Classification (HC)	32	Hybrid Deep Learning (HDL)
33	Hybrid Feature Selection (HFS)	34	Hybrid Intrusion Detection (HID)
35	Hybrid Machine Learning (HML)	36	Hybrid Metaheuristics (HMH)
37	Hybrid Models (HM)	38	Hybrid Optimization (HO)
39	Hybrid Techniques (HT)	40	Hyperparameter Tuning – (HPT)
41	IIoT Security (IIoTS)	42	Impersonation Attacks (IA)
43	Industrial IoT Security (IndIIoTS)	44	Information Gain (IG)
45	Internet of Drones (IoD)	46	Internet of Everything (IoE)
47	Internet of Medical Things (IoMT)	48	Internet of Vehicles
49	Intrusion Detection Systems (IDS)		

3 Scope and Objectives of the Survey

Scope: The goal of this report is to assess and examine Intrusion Detection Systems (IDS) that, from 2020 to 2024, were specifically designed for IoT environments. A variety of IDS techniques, such as signature-based, anomaly-based, and hybrid models, were explored to detect improvements in detection abilities, scalability, and resource efficiency. Furthermore, to deal with the unique challenges of securing IoT networks, feature selection techniques and the application of machine learning and deep learning methods are investigated in this paper. Key metrics, including accuracy, false positive rates, and real-time adaptability, are the basis for

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

assessing IDS model performance, with a clear focus on how relevant they are to medical IoT (IoMT), industrial IoT (IIoT), and cloud environments.

Objectives of the study include the following:

- Examining IDS technologies and trends from 2020–2024.
- Evaluating IDS performance across multiple datasets, focusing on accuracy, false positive rates, and scalability.
- Investigating hybrid IDS models, including feature selection and deep learning approaches
- Identifying key challenges and research directions for the future.

4 Introduction

Leading the way through automation, real-time monitoring, and data-driven decision-making, the rapid development of the Internet of Things (IoT) has transformed industries. Nevertheless, despite all of these benefits, it also comes with a multitude of very real security issues, such as unauthorized access, data breaches, and DDoS attacks. Enter the Intrusion Detection Systems (IDS), a crucial line of protection against these online dangers. Using developments in machine learning, deep learning, and hybrid models, researchers have made great progress in creating IDS solutions specifically suited for IoT contexts in recent years. Still, researchers are only scratching the surface, as much of the research that has been carried out on the subject fails to examine hybrid IDS architectures that merge multiple detection techniques to increase accuracy, scalability, and adaptability. Moreover, researchers also tend to skip feature selection methods and optimization strategies that are crucial parts for decreasing the computational load on resource-limited IoT tools. Furthermore, although datasets are the foundation of any IDS assessment, rigorous benchmarking using widely used datasets is conspicuously lacking, which makes it challenging to evaluate various frameworks in an effective manner. As a result, filling in these gaps through a complete exploration of these hybrid IDS models, feature selection techniques, and optimization strategies is the goal of this study. What is more, it also provides a clearer picture of where the field stands, benchmarking these advancements against well-known IoT security datasets. This paper illustrates how machine learning, deep learning, and hybrid approaches are changing IoT security by examining the most recent developments, trends, and challenges. Though the foundation has been laid by conventional IDS frameworks for identifying cyber threats in IoT environments, they frequently fail when confronted with the dynamic nature of IoT traffic, few resources, and constantly changing attack patterns. To overcome these issues, new approaches combining machine learning, feature selection, and hybrid optimization methods are used to overcome these issues. The most recent developments in IDS for IoT will be covered in detail in the next section, along with the main obstacles and innovations influencing the development of contemporary IDS protocols.

4.1 Advances in Intrusion Detection Systems for IoT: Challenges and Innovations

Strong cybersecurity has become even more crucial thanks to the rapid development of the Internet of Things (IoT). The colossal networks of connected devices, and especially those with

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

limited processing power, are what make IoT environments so special, as they bring about many new security challenges that can threaten the whole system, such as unauthorized access, data breaches, and large-scale cyberattacks. Smarter, more advanced solutions have become necessary as conventional security measures are inadequate at effectively managing these threats.

This is where Intrusion Detection Systems (IDS) come into play. By monitoring network traffic and identifying any suspicious activity, these systems serve as an important first line of protection. Still, the downside is that traditional IDS frameworks are not always ready and able because they simply are not efficient enough to manage the variety and sheer volume of data produced by IoT devices.

With the goal of creating IDS solutions that can keep up with the fast-paced, resource-limited world of IoT networks, researchers are overcoming these challenges by developing future-oriented IDS frameworks that support machine learning (ML), deep learning, and hybrid methods. These new ideas are making a real contribution to improving detection accuracy, scalability, and efficiency.

For instance, a supplied IDS leveraging the ToN-IoT dataset, together with Chi-square feature selection and SMOTE for class balancing, to improve detection across IoT network layers was posited by [1]. Likewise, to maximize detection performance while lowering computational overhead, [2] created a deep learning method that uses Convolutional Neural Networks (CNNs) for feature extraction in conjunction with the Aquila Optimizer. These examples emphasize the rising trend toward merging machine learning with feature selection and optimization to address IoT-specific issues.

Additional developments in IDS research emphasize hybrid models and optimization strategies. For instance, to effectively reduce IoT botnet attacks, [3]combined shared information-based feature selection with machine learning classifiers, attaining high accuracy with decreased computational demands. Furthermore, combining the Gorilla Troops Optimizer and the Bird Swarm Algorithm, [4] developed a hybrid model to balance convergence speed and classification accuracy. Meanwhile, utilizing ensemble learning with collaborative feature selection, [5]concentrated on lightweight IDS designs for resource-constrained IoT devices. These studies demonstrate the significance of bettering IDS frameworks to manage resource constraints and real-time detection needs. Moreover, new improvements in feature selection and hybrid classification methods were driven by specific applications of IDS in IoT. By integrating Bidirectional Gated Recurrent Units with Intelligent Multiverse Optimization, [6] tackled hyperparameter tuning issues, improving IDS capabilities even more. [7]presented a lightweight IDS employing optimal feature pairs, highlighting efforts to improve efficiency and adaptability in IDS design, whereas [8]prioritized normalization techniques.

IDS for Industrial IoT (IIoT) environments have advanced as a result of the growing frequency of cyberthreats, such as botnets and Distributed Denial of Service (DDoS) assaults. To handle real-time detection of sophisticated assaults, developing IDS models combine ML and deep learning. Research has shown that integrating ensemble learning, feature selection, and optimization algorithms greatly enhances IDS performance. For example, to detect attacks

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

while reducing false positives, [9]employed a Modified Genetic Algorithm (MGA) and Long Short-Term Memory (LSTM) models. Furthermore, to tackle class imbalance issues and achieve higher detection accuracy in IIoT networks as a result, [10]utilized ensemble feature selection techniques with neural networks in their research.

With models that use numerous ML algorithms to improve the hardiness of IDS, hybrid strategies have also become more popular. One example of this combines feature extraction with an ensemble approach, attaining accuracy rates in benchmark IoT datasets that exceed 99%. Known as the Voting Gray Wolf Optimizer-based model, it was presented by [11] and addresses important issues such as resource limitations and imbalanced datasets, demonstrating the potential of hybrid techniques in IoT security.

The combining of machine learning, deep learning, feature selection, and optimization algorithms in IDS frameworks has become essential as IoT networks continue to increase. These advancements ensure the security and resilience of IoT and IIoT systems by delivering accurate, real-time protection against growing cyber threats. Indeed, the vital role of modern IDS frameworks in protecting critical infrastructure and adjusting to the exceptional demands of IoT environments highlights the research efforts that are crucial for future digital security.

4.2 Approach to Article Selection and Exclusion

Pertinent search terms like machine learning algorithms, swarm intelligence algorithms, metaheuristic algorithms, multi-objective optimization, optimization algorithms, feature selection algorithms, and evolutionary algorithms were combined with phrases like intrusion detection system in the Internet of Things to guarantee a thorough and focused review. Research articles from several credible academic platforms and digital libraries were gathered using these search phrases. These search terms have also become popular, with models utilizing numerous machine learning algorithms to improve the robustness of IDS.

4.3 Academic Search Engines

These websites compile academic books, papers, and articles from a variety of subjects and sources:

- Google Scholar (https://scholar.google.com)—A popular and free academic search engine, Google Scholar indexes academic literature from a variety of fields, including books, theses, research papers, conference proceedings, and more publications and sources.

- Digital Bibliography and Library Project (DBLP) (https://dblp.uni-trier.de)—A popular and free academic search engine, Google Scholar indexes academic literature from a variety of fields, including books, theses, research papers, conference proceedings, and more.

4.4 Publisher-Specific Digital Libraries

These platforms are specific to individual publishers and provide access to papers, journals, and conference proceedings within specified domains:

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- IEEE Xplore (https://ieeexplore.ieee.org)—A digital library with an emphasis on computer science, engineering, and technology. IEEE Xplore gives users access to IEEE-published technical standards, conference papers, and journal articles.

- ScienceDirect (https://www.sciencedirect.com)—A trusted full-text scientific resource, ScienceDirect provides journal articles and book chapters in a variety of disciplines, including engineering, social sciences, life sciences, and physical sciences.

- SpringerLink (https://www.springerlink.com)—Academic research, books, and journal articles from a variety of fields, including computer science, engineering, medicine, and environmental science, are accessible through SpringerLink.

- Association for Computing Machinery (ACM) Digital Library (https://dl.acm.org)—Journal articles, conference papers, and other technical literature pertaining to computing and information technology research are the primary focus of the ACM Digital Library.

- Taylor and Francis Online (https://www.tandfonline.com)—A website that offers access to scholarly publications and periodicals in a number of fields, such as the social sciences, engineering, science, and technology.

- Multidisciplinary Digital Publishing Institute (MDPI) (https://www.mdpi.com)—Numerous academic publications from a variety of fields, including science, engineering, computer science, life sciences, environmental sciences, and more, are hosted by this open-access publisher. Since MDPI is renowned for its dedication to open-access publication, all articles are publicly available.

- DBLP Computer Science Bibliography (https://dblp.uni-trier.de)—Research papers and conference proceedings in computer science are accessible through the bibliographic database DBLP. Altogether, these platforms encompass a wide variety of studies in computer science, algorithms, optimization, and related domains.

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The figure 1 illustrate the process of choosing articles for the survey that focused on Intrusion Detection Systems in Internet of Things (IoT) contexts is illustrated visually by the flowchart

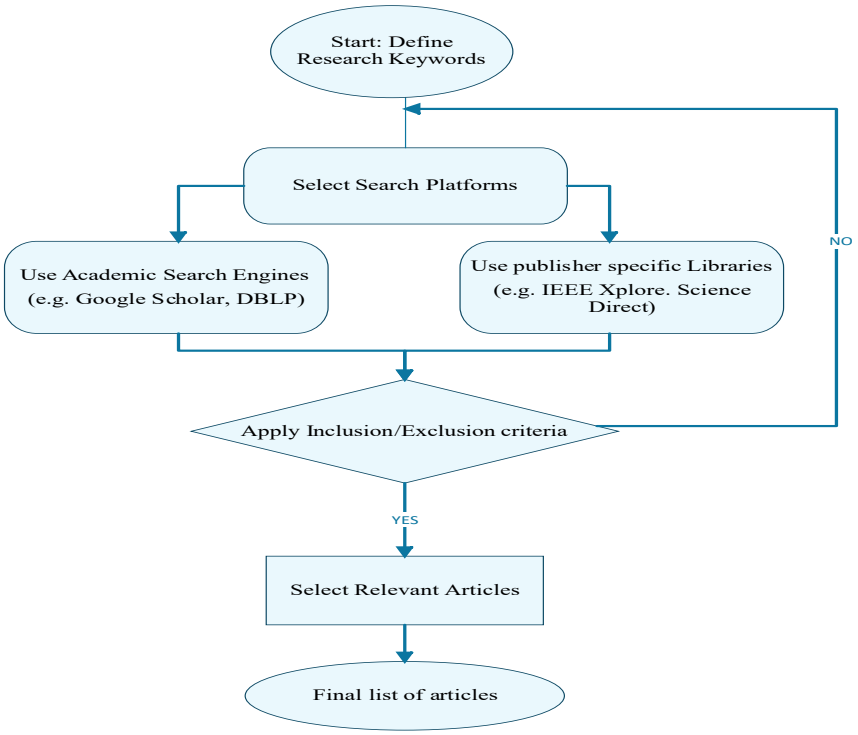

Figure 1: The process of choosing articles

5 Literature Review

A literature review is essential for understanding the current research environment, emphasizing significant developments, spotting gaps, and setting the stage for further research. Regarding the Intrusion Detection Systems (IDS) for IoT security, reviewing previous literature helps in planning the management of the latest developments, approaches, and ever-present challenges in the particular field of study. IoT networks' varied design, resource constraints, and the necessity of scalability have led to the emergence of new security threats as they spread quickly throughout sectors including smart cities, healthcare, and manufacturing. To overcome these challenges and increase detection accuracy, efficiency, and adaptability in IoT environments, researchers have been actively creating novel IDS approaches.

5.1 Evolution of Intrusion Detection Approaches

Intrusion detection systems (IDS) have evolved through successive stages in both concept and technology, from systems based on simple rules and statistical values to those relying on machine learning and deep learning techniques. This section provides a historical overview of the most significant stages in detection technology, illustrating the shift from traditional methods to modern intelligent and hybrid approaches.

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

5.1.1 Rule-Based Systems.

Rule-Based Systems Especially when it comes to Network Intrusion Detection Systems (NIDS) like Suricata, which use preset logic to detect intrusions, rule-based systems are essential to intrusion detection. In order to identify known malicious activity, these systems compare traffic patterns or signatures against a set of rules. The action, protocol, and traffic direction are specified in the header of each rule, and the particulars of the data to be examined are defined by the detection options. Detecting harmful signatures using Indicators of Compromise (IoCs), utilizing knowledge of existing attacks, and seeing protocol usage anomalies that can point to malevolent intent are common strategies. However, creating effective rules necessitates striking a balance between generality to guarantee broad threat coverage and specificity to lower false positives. High false positive rates continue to be a major problem, requiring constant rule revisions and fine-tuning to accommodate new dangers. Notwithstanding these difficulties, rule-based systems are a crucial part of network security frameworks because of their transparency, adaptability, and real-time detection capabilities [12].

5.1.2 Statistical Methods

Statistical Methods. A crucial element of improving cybersecurity for smart cities and critical infrastructure is statistical anomaly detection. By analyzing previous data to create baselines of typical behavior, it enables the system to spot variances that might point to possible dangers. Statistical techniques like mean, variance, and standard deviation are utilized to identify abnormalities by continuously monitoring real-time data and comparing it to these baselines. In order to minimize false positives and allow security teams to concentrate on real threats, thresholds are set to differentiate between typical fluctuations and real dangers. Because it concentrates on departures from expected behavior rather than depending only on predefined signs, this method works well for identifying known as well as unknown threats. Statistical anomaly detection is also flexible and scalable, which makes it appropriate for settings with a lot of changing data. It offers a complete and proactive security solution when combined with other strategies like intrusion detection systems and behavioral analytics, allowing for prompt reactions to possible cyberthreats [13].

5.1.3 Machine Learning-based IDS

[14] suggested an anomaly-based intrusion detection system (IDS) that used the Random Forest algorithm for classification and information gain and gain ratio for feature selection. The model demonstrated its effectiveness in identifying DoS, MITM, and scanning attacks in IoT contexts by achieving a high detection accuracy of up to 99.97%. The Bot-IoT dataset was used by [15] to compare different machine-learning techniques. They found that Naive Bayes was the best classifier for differentiating between DDoS, DoS, and regular traffic after using a bijective soft-set strategy for model selection. A hybrid IDS was presented by [16] that fused a Multi-Layer Perceptron (MLP) with the Artificial Bee Colony (ABC) algorithm. This method, known as HAD-MLP, successfully detected malware and Denial-of-Service attacks and showed excellent performance across several IoT datasets. An IDS utilizing entropy-based feature selection in conjunction with a Decision Tree classifier was proposed in the paper of [17] for IoT and cloud

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

network threats, their technique successfully reduced false positives while preserving high detection accuracy.

In 2021, [18] created an IDS model that integrated Random Forest classifiers with a Genetic Algorithm for feature selection. When identifying hazards in Industrial IoT (IIoT) contexts, the model demonstrated enhanced detection accuracy and computational efficiency. A lightweight IDS with rule-based preprocessing and statistical normalization was proposed by [8] their methodology showed remarkable accuracy and speed in detecting single and hybrid cyberattacks in IoT systems. A tree-based stacking ensemble model was suggested by [19] that included SelectKBest for feature selection, Decision Trees, Random Forest, and XGBoost. For broad IoT-related threats, their method produced good detection accuracy on the NSL-KDD and UNSW-NB15 datasets.

A lightweight ensemble model comprising Decision Trees, Extra Trees, Random Forest, and Naive Bayes classifiers was put into practice by [5] the model was able to detect botnet and DDoS attacks with a low computing overhead and excellent accuracy, which made it appropriate for use in Internet of Things devices. [20] used Binary Grey Wolf Optimization (BGWO) for feature selection in their machine learning-based intrusion detection system. Across all datasets, the model's accuracy reached 100%, particularly when it came to detecting DDoS attacks in IoT networks.

[10] used OWKELM for classification and the Chaotic Cuckoo Search Optimization Algorithm (CCSOA) for feature selection. In IIoT networks with significant data heterogeneity, their model increased detection efficiency and accuracy. After comparing PCA-based feature extraction and correlation-based feature selection, [21] found that feature selection was quicker and more accurate for intrusion detection in IoT networks. In their evaluation of ResNet50, LSTM, and KNN for IDS purposes, [22] discovered that ResNet50 performed the best against Blackhole attacks, suggesting a possible bias for deeper convolutional models in specific situations. To identify current IoT-specific dangers, [23] suggested an ensemble learning method that makes use of ELM, SVM, KNN, and logistic regression. Their model sought to strike a compromise between practical deployment and excellent performance. To safeguard smart city networks, [24] created an intrusion detection system (IDS) model based on a Restricted Boltzmann Machine (RBM). Their strategy used resources well and produced encouraging outcomes.

When it came to detecting IoT attacks, [25] multi-model intrusion detection system which included BiLSTM, GRU, and ELM in a weighted voting strategy performed better than traditional IDS techniques. To secure critical infrastructure environments, [24] introduced a novel hybrid ensemble technique that combines the bagging, stacking, and AdaBoost algorithms. This technique is further enhanced using Grey Wolf Optimization (GWO).

IDS-SIoEL, a robust ensemble IDS that uses AdaBoost and Boruta for feature selection, was presented by [26] across several datasets, the system's detection accuracy for DDoS, DoS, brute force, and botnet attacks was 100%. [27] integrated XGBoost, LightGBM, Random Forest, and Extra Trees to create a multi-class ensemble classifier. The model's efficacy and scalability for detecting IoV-related attacks were excellent. For feature tweaking, [28] suggested a

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

framework that included Mayfly Optimization with Enhanced Crow Search Optimization (ECSO). This was used in conjunction with machine learning classifiers to detect IoT cyberattacks thoroughly.

In their deep IDS architecture, [29] used Sparrow Search Optimization and Hybrid Group Search Optimization (HGSO) to detect both binary and multiclass intrusions with great accuracy. [30] used ensemble feature selection with a Deep Stacked Neural Network (DSNN) to create an IDS specifically for smart industrial systems. When it came to detecting ransomware and botnet threats in IIoT networks, the model performed admirably. In their study of ML and DL techniques for IoT IDSs, [31] highlighted the value of LSTM, CNN, and ensemble learning techniques for adaptable and lightweight threat detection. [11] achieved low false positive rates and good generalization accuracy by detecting botnet-specific threats in IoT networks using Random Forest and XGBoost. An ensemble-based intrusion detection system (IDS) was suggested by [32], which used Random Forest and XGBoost to categorize various kinds of network anomalies and Pearson correlation for feature selection. A meta-analysis of ML- and DL-based anomaly detection techniques for IoT was carried out by [33] For further research, their work underlined the significance of hybrid modeling and lightweight designs. To enhance the detection of minority class assaults, [34]) created an ML-based IDS system that incorporates oversampling approaches, PCA, and stacking feature embedding. [35] addressed intrusion detection issues in cloud-based IoT systems by combining ensemble classifiers with Artificial Bee Colony (ABC) optimization for feature selection. [36] presented a preprocessing model that used SVM and XGBoost for classification and Grey Wolf Optimization (GWO) and EBG for feature selection. This methodology proved very successful in detecting DDoS and virus threats in the Internet of Things. [37] enhanced ensemble-based intrusion detection systems that target intricate IoT security patterns by implementing the Harris Hawks Optimization algorithm. To identify different types of cyberattacks in IoT environments, [38] suggested an intrusion detection system (IDS) that uses Random Forest supplemented with a Modified Binary Political Optimizer (PIO). A generic ML-based security architecture for IoT networks was created by [39] to boost real-time detection and increase model training effectiveness.

5.1.4 Deep Learning-based IDS

By combining Principal Component Analysis (PCA) with Grey Wolf Optimizer (GWO) for feature engineering, [40] created an intrusion detection system (IDS) for IoMT situations. The classification process was then carried out using a Deep Neural Network (DNN), which achieved 99.9% accuracy and successfully detected DoS, Probe, R2L, and U2R attacks while keeping computational complexity low. A Vector Convolutional Deep Learning (VCDL) framework was presented by Amma [41] with the purpose of detecting anomalies in fog computing designs. Their system detected DDoS, DoS, reconnaissance, and data theft attempts with an accuracy of 99.75% using a Vector Convolutional Network (VCN) for feature extraction and a Fully Connected Network (FCN) for classification.

[42] presented a distributed deep learning-based intrusion detection system (IDS) that combines Long Short-Term Memory (LSTM) networks for botnet identification with

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Convolutional Neural Networks (CNN) for phishing and DDoS assault detection. In large-scale IoT contexts, their method allowed for highly accurate real-time device-level intrusion detection. Using Local-Global Ratio anomaly profiling in conjunction with Deep Belief Networks (DBNs), [43] demonstrated a deep ensemble intrusion detection system. Their model was appropriate for dynamic IoT situations since it minimized retraining costs while delivering high detection performance.

A hybrid deep learning model was created by [44] that employs LSTM for attack categorization and CNN for feature extraction. Their IDS demonstrated excellent real-time performance in identifying a range of network risks unique to the Internet of Things. A deep learning-based intrusion detection system (IDS) that combines the Aquila Optimizer for feature selection and Convolutional Neural Networks (CNN) for feature extraction was proposed by [2] In IoT applications, the system minimized resource consumption while maintaining excellent detection accuracy.

An anomaly-based intrusion detection system (IDS) utilizing a hybrid Generative Adversarial Network (GAN) and Deep Neural Network (DNN) model was presented by [45] Pearson correlation was utilized for feature selection. In IoT contexts, our technique enhanced the detection of minority-class anomalies. To address various network invasions on the CICIDS2018 dataset, [46] created the HDLNIDS framework by fusing oversampling methods with SoftMax-based categorization. A hybrid deep learning model was developed by [47] that employs GRU for temporal pattern learning and CNN for spatial pattern learning. When it came to identifying DDoS, brute-force, and penetration attempts, their model performed quite well. Using SMOTE for class balancing and One-Dimensional Signal Smoothing (OSS), [48] suggested a hierarchical IDS. DoS, Probe, U2R, and R2L attacks were successfully detected by their method.

An IoT-optimized dynamic distributed GAN-based intrusion detection system was presented by [49] to adjust to changing conditions, their model included a CNN-ANFIS hybrid classifier. Smart Sentry, a threat intelligence system developed with a Deep Neural Network (DNN) and PCA, was introduced by [50] in IIoT contexts, the model showed excellent accuracy in identifying malware, DDoS, and MITM. The VTR-HLSTM model, a deep hierarchical LSTM-based intrusion detection system tailored for cloud networks, was created by [51] In recognizing complicated intrusions, it decreased latency and increased training efficiency .

Using a weighted voting system, [25] presented an ensemble deep learning model that integrates BiLSTM, GRU, and ELM. In IoT contexts, our strategy performed noticeably better than conventional IDS techniques. The IoT-Defender framework, a lightweight intrusion detection system that incorporates a refined LSTM classifier and a Modified Genetic Algorithm (MGA) for feature selection, was presented by [9] according to them, this system demonstrated efficacy in real-time detection of zero-day threats. A thorough analysis of deep learning methods for IoT IDSs was carried out by [31] with an emphasis on the combination of ensemble designs, CNN, and LSTM with metaheuristic optimization. Using Deep Neural Networks (DNN) with PCA, Sadhwani et al. (2023) created an improved version of SmartSentry that demonstrated robust performance against significant cyber threats in IIoT contexts. VTR-

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

HLSTM, a hybrid layered LSTM model that provides real-time intrusion detection with enhanced latency for cloud computing networks, was enhanced and presented by [51].

5.1.5 Hybrid IDS Approaches

A hybrid intrusion detection system (IDS) was created in the study by [40] merging a Deep Neural Network (DNN) for classification with PCA and Grey Wolf Optimizer (GWO) for feature engineering. This hybrid model showed excellent detection efficiency and precision and was customized for IoMT situations. In order to effectively address threats in resource-constrained IoT scenarios, [14] presented a hybrid anomaly-based IDS that combines information-theoretic feature selection with machine learning classifiers. By combining MLP and neural networks with hybrid bio-inspired algorithms, such as Artificial Bee Colony (ABC) and Monarch Butterfly Optimization (MBO), [52]. greatly increased detection rates for DoS, probing, and U2R attacks.

[53] presented a hybrid intrusion detection system that combines Random Forest and Decision Tree classifiers with wrapper-based feature selection. When used on IoT Wi-Fi networks, their model produced low false alarm rates and great accuracy. Using a deep learning model that combines CNN and LSTM for reliable detection of IoT-specific network assaults, [44] also contributed to hybrid detection. In order to identify intrusions in real time on IoT devices with limited resources, [7] created a lightweight hybrid intrusion detection system. Their method successfully struck a compromise between computational economy and detection accuracy. In order to improve performance on a variety of datasets, [19] suggested a stacking ensemble model that combines Random Forest, XGBoost, and Decision Trees with SelectKBest feature selection.

To increase classification accuracy for IoT intrusion detection, [4] developed a hybrid feature selection technique that combines the Gorilla Troops Optimizer (GTO) and Bird Swarm Algorithm (BSA). [5] advanced hybrid models by using a multi-model ensemble approach to effectively detect DDoS and botnet assaults while using minimal resources. In their assessment of ensemble-based hybrid approaches for anomaly detection in IoT, [54] found that these approaches, which mix ML and DL techniques including bagging, boosting, and stacking, are very accurate and adaptive.

In order to improve detection of Sybil, blackhole, and hello flooding assaults, [55] suggested a hybrid intrusion detection system (IDS) that makes use of Grey Wolf Optimization (GWO) and Dipper Throated Optimizer (DTO). A combined RF-XGB and CLK-M model for wireless sensor networks was presented by [56], and it targets DoS, U2R, and R2L threats with good scalability. Using ELM, SVM, and KNN classifiers, [23] created an ensemble-based intrusion detection system (IDS) that strikes a compromise between computational economy and detection performance. In order to identify cloud-specific invasions, [57] developed the Hybrid Intrusion Detection Model (HIDM), which combines Random Forest, Neural Networks, and Gradient Boosting. For application in satellite-terrestrial networks, [58] developed a deep hybrid intrusion detection system (IDS) that combines numerous classifiers, such as RF, ANN, LSTM, and GRU, with Recursive Feature Selection (RF-SFS).

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

To improve temporal learning in IoT intrusion data, [47] built a hybrid CNN-GRU IDS that uses Pearson correlation for feature extraction. In order to improve detection across a variety of intrusion types, [46] presented HDLNIDS, a hybrid model that combines oversampling and SoftMax classification. [59] used ensemble classifiers and Restricted Boltzmann Machine (RBM) models to detect intrusions in smart cities. IDS-SIoEL, a strong hybrid model that combines AdaBoost and Boruta for feature selection, was proposed by [26] It achieves 100% detection accuracy in both brute-force and botnet scenarios.

In order to improve the identification of IoT-based threats, [25] developed an ensemble intrusion detection system (IDS) by combining BiLSTM, GRU, and ELM using a weighted voting method. Binary GWO and Recursive Feature Elimination (RFE) were used by [20] to create an IDS that is optimized for DDoS detection in IoT networks. Targeting illegal access and data breaches, [60] created a hybrid intrusion detection system (IDS) that uses Random Forest for feature selection and RBF Neural Network for classification. In order to improve threat detection in Internet of Vehicles (IoV) environments, [27] deployed a multi-tree ensemble IDS utilizing XGBoost, LightGBM, RF, and Extra Trees.

For effective IoT anomaly detection, [24] introduced HAEMPSO, a hybrid model that combines Autoencoder and Modified PSO with DNN. In order to improve scalability and detection performance in IoT attack situations, [55] also used a hybrid feature engineering technique that combined GWO and DTO. Using FSAP-based feature selection, [61] presented SABADT, a deep hybrid intrusion detection system that provides high accuracy against DDoS and zero-day threats. In order to identify assaults using MQTT and CoAP IoT protocols, [62] constructed IACO with a Multi-Layered Ensemble IDS (MLEID).

In order to detect zero-day threats in IoT systems, [9] created IoT-Defender, a hybrid intrusion detection system (IDS) that combines a modified genetic algorithm (MGA) with fine-tuned long short-term memory (LSTM). The importance of hybrid IDS frameworks that combine ensemble optimizers with DL models like LSTM/CNN for scalable detection was highlighted by [31] A hybrid intrusion detection system (IDS) with strong efficiency and threat response was developed by [63] and optimized using genetic algorithms for feature selection and tuning. To combat cloud-based IoT attacks, [35] suggested a hybrid intrusion detection model that uses ensemble classifiers and ABC for feature selection.

In order to identify complex infiltration behaviors in IoT contexts, [37] used ensemble models in conjunction with Harris-Hawks Optimization (HHO). A hybrid wrapper technique integrating GA-ELM and SVM was presented by [64] for precise detection in high-dimensional IoT datasets. DenseNet201 and RAPNet were used in a hybrid architecture by [65] to identify SQL injection, brute-force, and DDoS assaults in Internet of Things systems.

The figure 2 illustrates the evolutionary progression of intrusion detection systems transitioning from traditional rule-based approaches to intelligent hybrid models. It highlights how artificial intelligence techniques have gradually advanced to enhance the accuracy and efficiency of anomaly detection systems aligning them with the growing complexity and security challenges of modern IoT environments.

Received: August 09, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

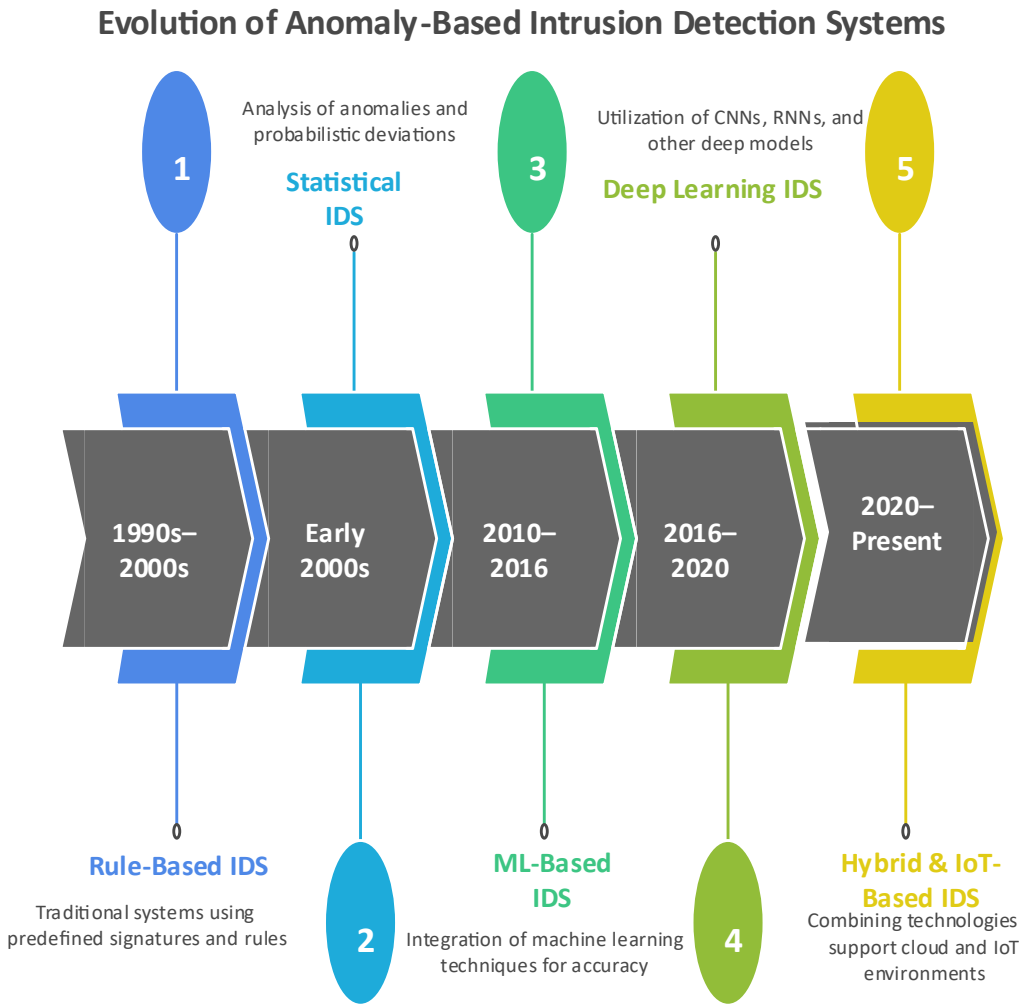

Figure 2:Evolution of Intrusion Detection Approaches

5.2 Classification of Intrusion Detection Systems

There are numerous ways to categorize IDS depending on the detection technique used, location deployed, environment, and response model. As such, this section outlines the different classification systems to help contrast the different types and to identify each class's respective strengths and weaknesses regarding accuracy, flexibility, and modern-day applicability challenges, especially in the cloud and Internet of Things (IoT) environments.

The classification of Intrusion Detection Systems (IDS) can be organized according to four main criteria as illustrated in Figure 3 these include the detection technique and system deployment and response mechanism and detection environment. The detection technique distinguishes IDSs based on the analytical approach used such as signature-based and anomaly based or hybrid methods System deployment refers to where the system is implemented whether at the host level (HIDS) and network level (NIDS) or a combination of both. The response mechanism determines whether the IDS reacts passively by generating alerts or actively by preventing intrusions (IPS). Finally, the detection environment classification

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

considers the operational context of the IDS including traditional networks and cloud infrastructures and Internet of Things (IoT) systems

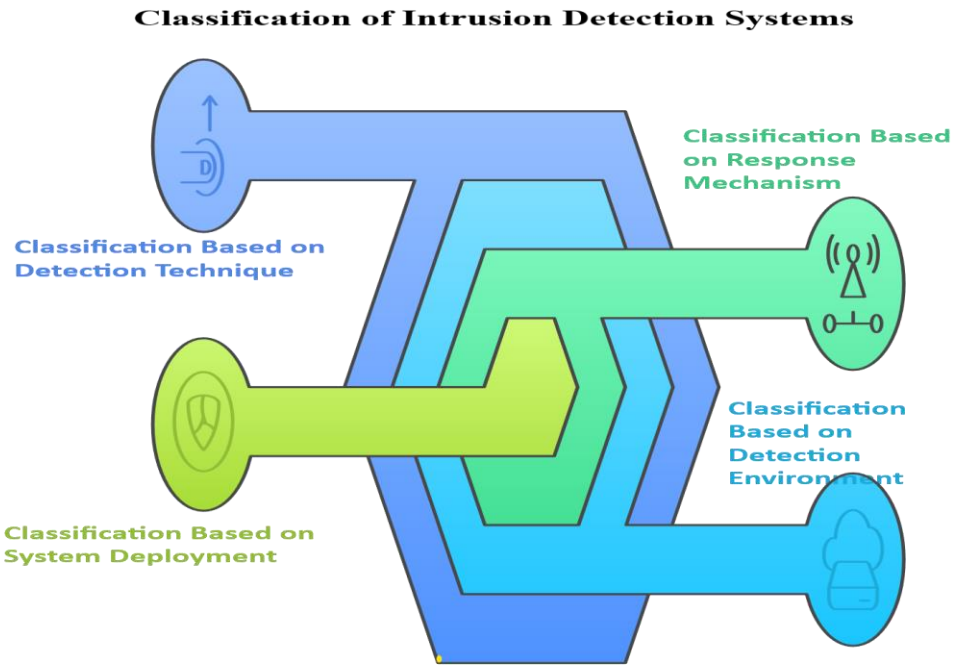

Figure 3 :Classification of Intrusion Detection Systems

5.2.1 Classification Based on Detection Technique

Detection techniques are a critical aspect of classification systems, as they determine how data or signals are identified and categorized. Based on the underlying methodology, detection techniques can be broadly classified into three categories.

5.2.1.1 Signature-Based IDSs

By comparing network behavior to a database of recognized attack signatures, signature-based intrusion detection systems (IDS) are able to detect threats. This approach is a popular choice for many commercial applications since it maintains low false positive rates and offers high accuracy in recognizing known threats. However, its ability to protect against polymorphic malware and zero-day assaults is limited due to its dependence on predetermined patterns. Machine learning methods like Decision Trees and Naive Bayes, as well as sophisticated deep learning models like Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), are frequently added to Signature-Based IDS in order to overcome these drawbacks. Because of its dependability, Signature-Based IDS is widely used to strengthen cybersecurity defenses in a variety of IoT scenarios, such as cloud systems, industrial IoT (IIoT), and medical IoT (IoMT) [66]; [67].

5.2.1.2 Anomaly-Based IDSs

By detecting departures from established regular behavior patterns in network traffic, anomaly-based intrusion detection systems (IDS) detect threats. These systems use statistical or artificial

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

intelligence models to identify deviations from normal patterns. This technique can reveal previously undiscovered attacks, making it very effective against zero-day threats. It is prone to high false positive rates, nevertheless, particularly when examining intricate or erratic traffic patterns. Anomaly-Based IDS frequently uses artificial immune systems, machine learning techniques, and statistical analysis to increase accuracy. Notwithstanding its benefits, this method has trouble handling massive amounts of data and heavily relies on accurate dataset labeling to enhance detection performance [66]; [67].

5.2.1.3 Hybrid IDSs

To improve detection accuracy and reduce false positive rates, hybrid-based intrusion detection systems (IDS) combine the techniques of anomaly-based and signature-based systems. It successfully detects both known and unexpected threats by fusing the advantages of both strategies. This system uses a two-layer mechanism: signature-based detection confirms recognized dangers, while anomaly detection highlights odd behaviors. Complex IoT environments are particularly well-suited for hybrid IDS, which offers enhanced security with high alarm reliability and fewer false positives. Nevertheless, combining several detection methods may lead to a higher computing cost [66];[67].

5.2.2 Classification Based on System Deployment

The deployment structure of intrusion detection systems (IDSs) determines their ability to detect threats and their operational range. The classification process enables organizations to select IDS systems that fulfill their specific security requirements based on their architectural needs. The three main IDS deployment types consist of Host Based IDSs (HIDS) and Network Based IDSs (NIDS) and Hybrid IDSs. Host based intrusion detection systems (IDSs) monitor specific hosts to detect internal threats and system changes through their host-based activity tracking functionality. Network based intrusion detection systems (IDSs) analyze network traffic to detect malicious activities while protecting the entire network from external threats. Hybrid intrusion detection systems (IDSs) achieve complete network protection through their combination of host-based and network-based monitoring capabilities which leverage HIDS and NIDS advantages. The multi-layered approach reduces false positives while enhancing detection precision and enables organizations to handle evolving cyber threats. Organizations can select IDS systems that match their security requirements through understanding the different deployment categories.

5.2.2.1 Host-Based IDSs (HIDS)

This multi-layered strategy lowers false positives, improves detection accuracy, and adjusts to the changing complexity of contemporary cyberthreats. Organizations may strategically deploy IDS systems that are suited to their particular security needs by being aware of these deployment classifications. It can also prohibit access to private ports and keep an eye on particular occurrences, like port activity. Its ability to effectively identify internal threats, such as insider assaults, and provide comprehensive information about modifications or tampering within the host system is one of its main features. Because it can access the host's decrypted files, it is also ideally suited for detecting encrypted data. However, its reach is restricted to a

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

single host, and its functionality is reliant on the resources and operating system of the host, which may cause the host to execute more slowly [68];[67].

5.2.2.2 Network-Based IDSs (NIDS)

Instead of concentrating on examining data from individual devices, network-based monitoring examines traffic from the entire network. It works by looking at packet data as it moves over the network to find indications of assaults, frequently with the use of anomaly detection techniques or signature detection (predefined attack patterns). It logs assault details for later study and sounds alerts in real-time. One of its main benefits is its extensive monitoring capacity, which enables it to effectively identify malicious traffic and external threats coming from outside the network. It also doesn't depend on any one host, which lessens the effect it has on host performance. Its drawbacks, however, include the inability to analyze encrypted communication and possible difficulties managing large traffic volumes, which may result in false positives and negatives. To increase accuracy and decrease false alarms, it also has to be significantly adjusted [68];[67].

5.2.3 Classification Based on Detection Environment

The design and functionality of intrusion detection systems (IDSs) are significantly impacted by the detection environment. Threats change along with computing environments, necessitating IDS solutions made especially for various operating contexts. IDSs are categorized in this section based on their deployment contexts, with a focus on two important categories: cloud-based and IoT-based IDSs. While IoT-based IDSs handle the unique problems of resource-constrained and heterogeneous IoT networks, cloud-based IDSs concentrate on resolving issues in virtualized and distributed cloud systems. Because every environment has different security requirements and threats, different detection techniques and system designs have been developed. We can better understand how IDSs adjust to various contexts to deliver effective cybersecurity against persistent attacks by investigating these categories.

5.2.3.1 Cloud-Based IDSs

Cloud-based intrusion detection systems, or IDSs, are essential for protecting cloud environments, which are becoming more and more vulnerable to cyberattacks because of their extensive use. Cloud infrastructures, which are often divided into three primary service models: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS), are monitored and fraudulent activity is detected by these systems. Vulnerabilities that are specific to each model include SQL injection attacks in SaaS, phishing attacks in PaaS, and virtual machine image assaults in IaaS. Cloud-based intrusion detection systems can be broadly categorized as follows: Distributed IDS (DIDS), which combines multiple IDS components to prevent single points of failure; Network-Based IDS (NIDS), which analyzes network traffic to detect external threats like DDoS attacks; Host-Based IDS (HIDS), which keeps an eye on individual hosts, such as virtual machines, for internal threats; and Hypervisor-Based IDS (HYIDS), which concentrates on securing the hypervisor layer. Detection techniques include anomaly-based detection, which finds deviations from typical activity; hybrid detection, which combines both techniques to increase accuracy and lower false positives; and signature-based

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

detection, which matches known attack patterns. Cloud-based IDSs must, however, overcome obstacles such as managing resource overhead, processing encrypted traffic, protecting data confidentiality, and fixing hypervisor vulnerabilities. Using machine learning methods like deep learning, incorporating IDSs into the middleware layer, and employing Virtual Machine Introspection (VMI) for external monitoring are some future prospects. Overall, even though cloud-based intrusion detection systems (IDSs) are crucial for protecting cloud infrastructures, their efficacy hinges on resolving these issues using sophisticated detection methods and creative approaches [51];[69]

5.2.3.2 IoT-Based IDSs

IoT-Based Intrusion Detection Systems (IDSs) are specialist solutions made to handle the particular difficulties presented by IoT ecosystems, which are distinguished by a variety of surroundings and low-resource devices. These IDSs are designed to function well on Internet of Things devices with constrained memory, processing capacity, and energy resources while maintaining strong defense against a variety of online dangers. Real-time threat detection without taxing system resources is made possible by IoT-based intrusion detection systems (IDSs) that use lightweight machine learning (ML) models, such as decision trees, k-nearest neighbors (KNN), and Naive Bayes classifiers, which are tuned for low-power devices. In heterogeneous IoT environments, where devices use several communication protocols like Wi-Fi, Bluetooth, and Zigbee and range in complexity from basic sensors to sophisticated smart appliances, these solutions work especially well. IoT-based IDSs frequently use anomaly detection techniques, like statistical methods, proximity-based methods, and ensemble methods, which are effective at spotting departures from typical behavior and identifying unknown or zero-day attacks, to guarantee compatibility and adaptability across a variety of networks. IoT-based IDSs also use decentralized techniques like edge computing and federated learning to address privacy issues and lessen the need for centralized cloud servers. While edge computing provides local data processing, lowering latency and improving privacy, federated learning enables devices to work together to train models without exchanging sensitive data. IoT-based IDSs have drawbacks despite their benefits, including scalability issues, data privacy concerns, resource limitations, and the heterogeneity of IoT devices. Emerging technologies like 5G network integration and model compression methods (such as pruning, quantization, and knowledge distillation) are being investigated as solutions to these problems. By increasing the effectiveness, scalability, and reactivity of IoT-based IDSs, these developments hope to better position them for practical uses in smart home, healthcare, and industrial IoT settings. In conclusion, IoT-based intrusion detection systems (IDSs) are crucial for protecting the quickly growing IoT ecosystem because they provide scalable, lightweight, and efficient security solutions that are adapted to the particular limitations of IoT environments [70].

5.2.4 Classification Based on Response Mechanism

An intrusion detection system's (IDS) response mechanism is a key component in assessing how well it protects networks and systems from online attacks. IDSs are divided into two primary groups based on how they react to threats they detect: Passive IDSs and Active IDSs (Intrusion Prevention Systems, or IPS). With an emphasis on monitoring and alerting, passive

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

IDSs produce thorough logs and warnings that enable administrators to manually look into and address possible risks. Although this method offers useful forensic data and reduces the possibility of false positives, it mostly depends on human participation, which may cause replies to be delayed. Conversely, Active IDSs (also known as IPSs) provide proactive defense against malicious activity by taking prompt, automatic action to block or neutralize threats in real time. In high-security settings where quick threat neutralization is crucial, this automated response is especially helpful. To prevent false positives from interfering with real processes, it must be configured carefully. Organizations can select the best IDS type to meet their security requirements by being aware of these reaction mechanisms, which strike a balance between automation and human oversight for the best possible protection.

5.2.4.1 Passive IDSs

The purpose of passive intrusion detection systems (IDSs) is to keep an eye on and identify any questionable activity or possible security risks within a system or network. They do not directly mitigate or block threats that are detected, in contrast to active IDSs. Rather, they produce logs or warnings that system administrators or security teams can manually examine and react to. In order to spot irregularities or known attack patterns, passive intrusion detection systems (IDSs) continuously monitor network traffic, system logs, or user behavior. They then provide comprehensive records and alarms for more research. These systems rely on human intervention for analysis and response, and they do not disrupt system operations or network traffic. Passive IDSs are frequently employed in settings like research or low-risk networks where human monitoring is desirable or where automated responses could interfere with lawful operations. Their benefits include thorough logging, which is helpful for forensic investigation and comprehending the nature of threats, and a minimal danger of false positives because they do not perform automatic activities. However, because they do not automatically stop or mitigate assaults, they have drawbacks such as limited real-time protection and delayed reactions because they depend on human interaction. Passive IDSs include host-based systems that keep an eye on particular systems for illegal access or file alterations, recording events for later analysis, and network-based systems that watch traffic for unusual patterns without blocking it [71].

5.2.4.2 Active IDSs (IPS)

In addition to identifying possible threats, active intrusion detection systems (IDSs), often referred to as intrusion prevention systems (IPS), act quickly to stop or lessen them. These systems offer automated defense against malevolent activity and are made to react to threats instantly. Real-time threat mitigation, where they can automatically block suspicious traffic, cut off connections, or reconfigure firewalls to stop attacks from completing, is one of the main features of active IDSs. They are appropriate for high-security settings because they can take proactive steps to neutralize threats without human assistance. Active IDSs are frequently used to stop malware infections, Distributed Denial of Service (DDoS) assaults, and unauthorized access. They are perfect for settings where quick reaction is essential, such as financial institutions, healthcare systems, or vital infrastructure. Active IDSs provide the advantages of better security, which lowers the chance of damage or data loss by preventing attacks before

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

they can cause harm, and quick response, which offers real-time protection by automatically neutralizing threats. They do have drawbacks, though, like the possibility of false positives, in which automated responses might block legitimate traffic if the system misinterprets benign activity as malicious, and the difficulty of balancing security and performance through careful configuration, since too aggressive responses can interfere with regular operations. Examples of active intrusion detection systems are host-based IPS, which keeps an eye on individual systems and can take actions like stopping unauthorized access attempts or terminating suspicious processes, and network-based IPS, which keeps an eye on network traffic and can block or reroute malicious traffic in real-time, such as detecting and mitigating DDoS attacks by blocking source IP addresses [71]..

5.3 Feature Engineering and Optimization in Intrusion Detection Systems

The modern intrusion detection systems rely on the selection and optimization of relevant and important features. It is the most critical stage of building systems as it determines all the systems accuracy and performance. This section presents the leading techniques for feature engineering and the most common optimization approaches used for dimension reduction, information extraction, and most importantly, strengthening the reliability of detection systems and smart systems.

5.3.1 Feature Selection and Optimization Methods

Finding and keeping the most instructive features from the original dataset is the goal of feature selection, a crucial strategy in intrusion detection systems (IDS). Feature selection improves computing performance and model interpretability by lowering the dimensionality of data. In this approach, common techniques like Gini-impurity, mutual information, and correlation-based selection are commonly employed. By removing superfluous or unnecessary features, these methods guarantee that the machine learning model concentrates on the qualities that are most important for identifying abnormalities. Feature selection's capacity to shorten training and inference periods is one of its main advantages, which makes it ideal for lightweight intrusion detection systems in IoT environments with limited resources. Additionally, it maintains the features' original semantic meaning, which is beneficial for debugging and human comprehension. The quantity and caliber of features chosen, however might affect how successful feature selection is since too aggressive reduction can result in a drop in detection accuracy [72].

A genetic programming-based intrusion detection system (IDS) was created by [73] to identify HELLO-Flood, sinkhole, and blackhole attacks in Internet of Things networks. Their threshold modulation method preserved scalability for IIoT systems while increasing detection accuracy by up to 95%. In order to improve feature selection in a DNN-based intrusion detection system, [40] integrated PCA and Grey Wolf Optimization (GWO). This hybrid framework enhanced detection performance and dimensionality reduction.

In an IoT setting with limited resources, [14] improved classifier accuracy and decreased false positives by using information gain and gain ratio to choose pertinent features. [74] proposed an IDS utilizing NSGA-II and Jumping Gene for feature selection, combined with Extreme

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Learning Machine (ELM) for classification. Their approach effectively handled DDoS detection in large-scale IoT datasets. In resource-constrained IoT scenarios, [17] used an entropy-based feature selection technique that greatly decreased dimensionality and improved classification accuracy. In order to improve model detection results in industrial IoT environments, [18] used genetic algorithms to choose the best features.

[75] designed a metaheuristic IDS framework using a multi-objective feature selection strategy that optimized detection performance while minimizing feature dimensionality. For real-time IoT intrusion detection, [1] employed ensemble classifiers such as XGBoost, KNN, and Random Forest along with chi-square-based feature selection and SMOTE resampling. To improve feature convergence and classification accuracy, [4] used a hybrid optimization technique that included the Gorilla Troops Optimizer (GTO) and Bird Swarm Algorithm (BSA).

After comparing correlation-based feature selection with PCA-based feature extraction, [21] concluded that feature selection improves IoT IDS accuracy and efficiency. In order to achieve better classification of IoT assaults, [55] used a mix of GWO and DTO for efficient dataset balancing and feature relevance identification. To improve detection accuracy in heterogeneous IIoT data, [10] combined OWKELM with Chaotic Cuckoo Search Optimization (CCSOA) for classification. A hybrid feature selection system that combines a voting-based ensemble with the DTO-guided Whale Optimization Algorithm (WOA) was presented by [55], yielding reliable detection results in a variety of IoT applications.

Using optimal feature selection techniques, [49] suggested a GAN-based distributed IDS with CNN-ANFIS integration that can adapt to changing IoT scenarios. In order to overcome feature imbalance and enhance overall classification performance, Krishnan and Saraswathi (2023) used OSS and SMOTE. A GA-ELM wrapper model for feature selection with SVM classification, intended for high-dimensional incursion datasets, was adopted by [64]. [61] achieved great accuracy in recognizing DDoS and zero-day attacks by integrating FSAP for feature selection with the SABADT hybrid model. [36] developed a lightweight preprocessing pipeline that targets malware and DDoS attacks by combining GWO and EBG optimizers with SVM and XGBoost.

[76] classified medical IoT intrusions, such as unauthorized access, using AdaBoost and PSO for feature selection. [65] applied DenseNet201 and RAPNet for deep feature engineering within a scalable IDS framework for IoT cybersecurity. [50] used PCA and DNN to create SmartSentry, which effectively reduces features and detects anomalies in IIoT environments. Using IBFO and Z-score normalization, [77] optimized Bacterial Foraging with a focus on smart city infiltration datasets. A dual optimization model combining the ECSO and Mayfly algorithms was presented by [28] for reliable cyberattack detection in the Internet of Things.

[78] employed CCR-ELM classifiers in conjunction with the Binary Chimp Optimization Algorithm (BCOA) to identify IoT hazards unique to WSNs. In order to improve the LSTM-based detection performance in IoT-Defender, [9] used a Modified Genetic Algorithm (MGA) for dimensionality reduction. In order to manage intricate, high-dimensional IoT traffic, they have suggested a Bat Algorithm that combines PCA with Random Node Selection (RNS).

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

In order to improve classification across IoT intrusion types, [79] presented an ensemble learning approach that combines PCA, Information Gain (IG), and Grey Wolf Optimization (GWO). [72] determined the best practices for improving IDS classifiers by contrasting PCA-based extraction and IG-based feature selection. [63] introduced a tuning technique improved using Genetic Algorithms that increased the accuracy and responsiveness of IoT IDS. By adding PCA and stacking to their IDS system, [34] successfully enhanced minority-class intrusion detection in massive amounts of data. For effective IoT attack classification, [80] suggested using Random Forest in conjunction with the Crow Search Algorithm (CSA) for relevant feature selection. Artificial Bee Colony (ABC) optimization was used by [35] to reduce the dimensions of cloud IoT intrusion detection systems.

5.3.2 Feature Extraction

In contrast, feature extraction preserves the most important information while converting the original features into a lower-dimensional space. In contrast to feature selection, which selects a subset of preexisting data, feature extraction uses neural networks or mathematical projections to produce completely new features. For this, methods like Autoencoders (AE) and Principal Component Analysis (PCA) are frequently employed. While autoencoders use deep learning to convert high-dimensional data into compact representations, PCA uses eigenvectors and eigenvalues to reduce dimensionality. Feature extraction performs consistently over a range of feature quantities and is especially useful for managing intricate, high-dimensional datasets. It is appropriate for identifying a variety of cyberattacks since it can also pick up subtle patterns that feature selection would overlook. Interpretability may become more difficult, though, as extracted features frequently lose their intuitive meaning. Furthermore, in resource-constrained IoT systems, real-time applications may encounter difficulties because of the computing demands of techniques such as autoencoders [72].

[2] created a deep learning method that uses Convolutional Neural Networks (CNNs) for feature extraction in conjunction with the Aquila Optimizer. These examples emphasize the rising trend toward merging machine learning with feature selection and optimization to address IoT-specific issues. With models that use numerous ML algorithms to improve the hardiness of IDS, hybrid strategies have also become more popular.

A Vector Convolutional Deep Learning (VCDL) framework was presented by [41] with the purpose of detecting anomalies in fog computing designs. Their system detected DDoS, DoS, reconnaissance, and data theft attempts with an accuracy of 99.75% using a Vector Convolutional Network (VCN) for feature extraction and a Fully Connected Network (FCN) for classification.

With models that use numerous ML algorithms to improve the hardiness of IDS, hybrid strategies have also become more popular. One example of this combines feature extraction with an ensemble approach, attaining accuracy rates in benchmark IoT datasets that exceed 99%. Known as the Voting Gray Wolf Optimizer-based model, it was presented by [11] and addresses important issues such as resource limitations and imbalanced datasets, demonstrating the potential of hybrid techniques in IoT security.

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

After comparing PCA-based feature extraction and correlation-based feature selection, [21] found that feature selection was quicker and more accurate for intrusion detection in IoT networks. A hybrid deep learning model was created by [44] that employs LSTM for attack categorization and CNN for feature extraction. Their IDS demonstrated excellent real-time performance in identifying a range of network risks unique to the Internet of Things. A deep learning-based intrusion detection system (IDS) that combines the Aquila Optimizer for feature selection and Convolutional Neural Networks (CNN) for feature extraction was proposed by [2].

In IoT applications, the system minimized resource consumption while maintaining excellent detection accuracy. To improve temporal learning in IoT intrusion data, [47] built a hybrid CNN-GRU IDS that uses Pearson correlation for feature extraction.

Feature extraction and feature selection are two essential dimensionality reduction techniques widely applied in Intrusion Detection Systems (IDS) as presents in figure 4 feature extraction transforms raw data into new compact representations by capturing complex and subtle patterns through mathematical projections often improving detection capability but reducing interpretability. In contrast feature selection identifies and retains the most relevant features from the original dataset maintaining their intuitive meaning while improving model accuracy and computational efficiency. Together both techniques play a critical role in optimizing IDS performance by balancing detection accuracy and interpretability and processing cost.

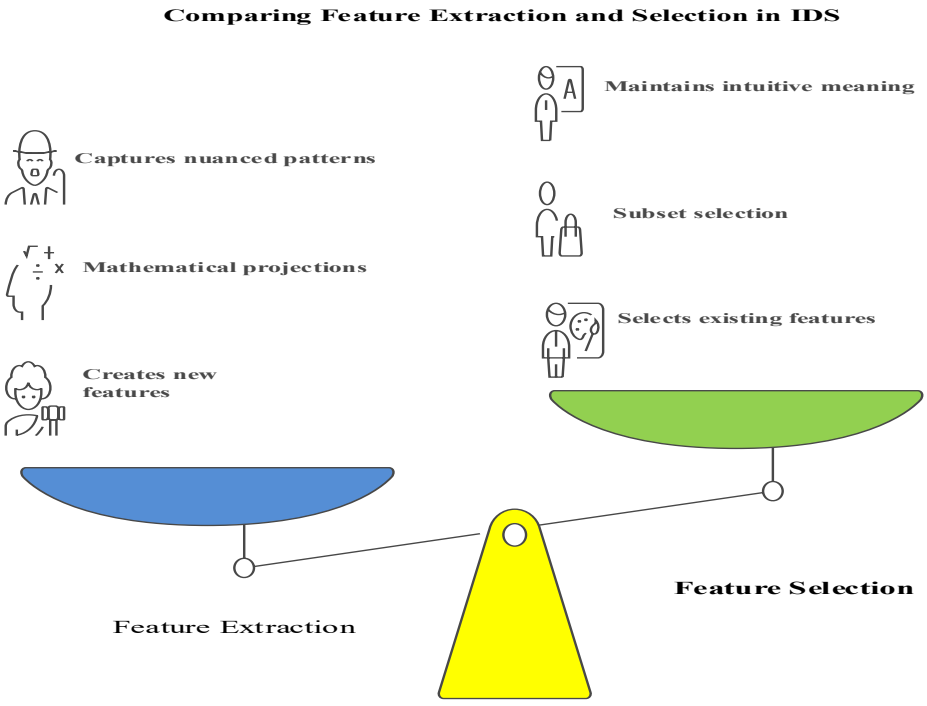

Figure 4: Comparing Feature Extraction and Selection in IDS

Received: August 09, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

6 Comprehensive Review of IDS Technologies and Trends for IoT Environments over the Last Five Years (2020–2024).

6.1 Comparative Analysis of 2020 IoT Intrusion Detection Systems: Methods, Techniques, and Future Directions.

A comparison of intrusion detection systems (IDS) created for the Internet of Things in 2020 is displayed in Table 3. It lists the main conclusions from each study as well as the features, targeted attack types, detection strategies, and procedures. In 2020, research focused on hybrid models and optimization techniques to improve efficiency and accuracy. Scalable and efficient IDS for cloud, industrial, and Internet of Things applications have been made possible by the combination of feature selection, machine learning, and deep learning. Challenges like class imbalance, real-time performance, and the utilization of more reliable datasets are the focus of future study. The main metrics and popular IDS methods used in 2020 are compiled in Table 1. High accuracy (94.8% to 99.9%) employing methods like PCA-GWO, DNN, and NSGA-II, which also decreased computing cost, was one of the primary KPIs for IDS in 2020. Malware and DDoS attack detection rates increased, and false positives were reduced via feature selection that was optimized (e.g., RFE, NSGA-II). Distributed designs improved scalability and real-time detection, while Naive Bayes and other lightweight techniques addressed computing efficiency. The following were common methods: hybrid approaches (Genetic Programming, PCA-GWO with DNN), distributed/ensemble models (Vector Convolutional Deep Learning, Voting Classifier), anomaly detection (Naive Bayes, SVM), feature selection (PCA-GWO, NSGA-II, RFE), and deep learning (DNN, CNN-LSTM).

Table 1 Comparison of IoT Intrusion Detection Systems (2020): Methodologies, Techniques, Characteristics, and Attack Types

Author(s)	Detection Methodology	Specific Techniques	Characteristics	Type of Attacks
[73]	**Threshold-based modulation using Genetic Programming**	**Genetic Programming for threshold modulation**	**Real-time, scalable for IIoT networks**	**HELLO-Flood, Version Number, Sinkhole, Blackhole**
[40]	**Hybrid PCA-GWO for feature selection and DNN**	**PCA for dimensionality reduction, GWO for feature selection**	**High accuracy (99.9%), reduced computational costs**	**IoMT-specific attacks (DoS, Probe, R2L, U2R)**
[41]	**Vector Convolutional**	**VCN for feature extraction, FCN**	**Distributed fog computing model, scalable**	**DDoS, DoS, Reconnaissance, Theft**

Received: August 09, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

	Deep Learning (VCDL)	**for classification**		
[14]	**Hybrid feature selection with Random Forest**	**Information Gain, Gain Ratio for feature selection**	**High detection accuracy (up to 99.97%), low false-positive rates**	**DoS, MITM, Scanning**
[42]	**Distributed deep learning with CNN and LSTM**	**CNN for phishing/DDoS, LSTM for Botnet detection**	**Device-level and back-end detection, highly accurate**	**Phishing, Botnet**
[81]	**KVM-based introspection with ensemble learning**	**LibVMI for introspection, VotingClassifier for detection**	**Robust detection, combines static and dynamic analysis**	**Malware, Rootkits**
[74]	**NSGA-II for multi-objective feature selection**	**NSGA-II with Jumping Gene, ELM classifier**	**Reduces redundancy, balances relevance, achieves high accuracy (99.9%)**	**DDoS**
[15]	**Bijective soft set for ML algorithm selection**	**Bijective soft set method for ML selection**	**Identifies optimal algorithms for specific attack types**	**Bot-IoT (DDoS, DoS, Normal)**
[82]	**Support Vector Machine for SDN**	**SVM classifier with WRFS feature selection**	**Optimized for SDN environments, high detection accuracy**	**DDoS**
[83]	**Comprehensive IDS survey**	**Taxonomy of IDS techniques,**	**Highlights challenges like evasion techniques,**	**Zero-day attacks, network intrusions**

Received: August 09, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

		dataset evaluation	**dataset limitations**	
[83]	**Naive Bayes-based anomaly detection**	**Naive Bayes classifier**	**Lightweight, scalable**	**IoT-specific anomalies**
[16]	**Hybrid anomaly-based IDS (using MLP)**	**Hybridization of Artificial Bee Colony (ABC) and Dragonfly Algorithm (DA) named HAD Algorithm; Multi-layer Perceptron (MLP) neural networks optimized by HAD to effectively classify network traffic into malicious and non-malicious activities.**	**Demonstrates superior performance compared to traditional back-propagation and other metaheuristic algorithms (ABC, ACO, PSO, GA, etc.). Achieved high accuracy and detection rates on four benchmark datasets (KDD Cup '99, NSL-KDD, ISCX2012, UNSW-NB15). Particularly high classification accuracy (~100%) on subsets of ISCX2012 dataset with zero false alarms, proving good balance between exploration**	**Various attacks including Denial-of-Service (DoS), Probing attacks, Remote-to-Local (R2L), User-to-Root (U2R), Distributed Denial-of-Service (DDoS), HTTP flooding, infiltration/injection attacks, and brute-force login attempts across standard IDS datasets (KDD Cup 99, NSL-KDD, ISCX 2012, UNSW-NB15) .**

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

			and exploitation.	
[52]	**Hybrid anomaly-based detection (Neural network-based IDS optimized using hybrid metaheuristic) .**	**Hybrid Artificial Bee Colony (ABC) and Monarch Butterfly Optimization (MBO) (HAM algorithm) used for training Multilayer Perceptron (MLP) neural networks (HAM-MLP) .**	**Provides significant accuracy enhancement and efficiency improvement over nine other metaheuristic algorithms (ACO, ALO, ABC, EHO, ES, HS, MBO, SCA, WOA). Evaluated on KDD Cup 99, ISCX 2012, UNSW-NB15 datasets. Achieved high accuracy and detection rates while reducing false alarms.**	**Denial-of-Service (DoS), Probing, User-to-Root (U2R), Remote-to-Local (R2L), HTTP flooding, infiltration/injection attacks, and brute-force login attempts.**

6.2 Comparative Analysis of 2021 IoT Intrusion Detection Systems: Methods, Techniques, and Future Directions.

Effective and optimal feature selection strategies, adaptive anomaly detection approaches, and machine learning-based classification designed for IoT and IIoT contexts were highlighted in the research examined from 2021. During this time, entropy-based and filter-wrapper feature selection techniques were used in detection systems, which greatly decreased false positives while balancing computing resources. Notable models included [17], who used Decision Trees and entropy-based feature selection to detect IoT and cloud network threats, and (Albulayhi & Sheldon, 2021)Ozturk et al. (2021), who combined filter and wrapper methods to balance detection performance and computational efficiency, focusing on attacks specific to the Internet of Things. Local-Global Ratio anomaly profiling with Deep Belief Networks (DBNs) was used by [43] to enable adaptive detection in IoT contexts with less retraining required. While [8]) improved detection accuracy against general network threats by statistical normalization-based preprocessing, [18] improved detection accuracy and computing efficiency in IIoT networks by utilizing Genetic Algorithms with Random Forest classifiers. In general, resource efficiency, adaptation to IoT-specific threats, and attaining high detection accuracy were the main focuses

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

of IDS methodology in 2021. These **approaches supported further research on real-time performance and scalability upgrades.**

Table 2: Comparison of IoT Intrusion Detection Systems (2021): Methodologies, Techniques, Characteristics, and Attack Types

Author's	Detection Methodology	Specific Techniques	Characteristics	Type of Attacks
[3]	**Mutual Information-based feature selection**	**Mutual Information with PCA and ANOVA for feature selection**	**Combines PCA and ANOVA f-test, robust multi-class classification**	**IoT botnet (Mirai, Bashlite)**
[17]	**Entropy-based feature selection and Decision Tree**	**Entropy-based feature selection combined with Decision Tree classifier**	**Simple but effective, reduces false positives**	**IoT and cloud network attacks**
[84]	**Filter and wrapper-based feature selection**	**Combination of filter and wrapper methods for feature refinement**	**Efficient, balances computational load and detection performance**	**IoT-specific attacks**
[43]	**Local-Global Ratio anomaly detection, DBNs for classification**	**Local-Global Ratio profiling with Deep Belief Networks**	**Reduces retraining overhead, high detection performance**	**IoT-specific, adaptive environments**
[18]	**GA for feature selection, tree-based classifiers for detection**	**Genetic Algorithm for feature selection, Random Forest, Decision Trees**	**Enhances accuracy and efficiency in IIoT**	**IIoT-specific attacks**

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[8]	**Statistical normalization for preprocessing**	**Statistical ranking-based method for normalization selection**	**Improves preprocessing, ensures high detection performance**	**General network attacks**
[53]	**Hybrid wrapper-based feature selection**	**Wrapper-based feature selection combined with ANN classifier**	**Efficient against impersonation attacks**	**IoT Wi-Fi network attacks**
[44]	**Hybrid CNN-LSTM model**	**CNN for feature extraction, LSTM for attack classification**	**Efficient in learning complex patterns**	**IoT-specific network attacks**
[7]	**Optimal feature pairs from Bot-IoT dataset**	**Feature pair-based evaluation with 10 ML algorithms**	**Lightweight, energy-efficient**	**IoT-specific (Bot-IoT)**
[2]	**CNN with Aquila Optimizer for feature selection**	**CNN for feature extraction and Aquila Optimizer for selection**	**Lightweight, reduces computational complexity, high-dimensionality**	**IoT-specific attacks**
[85])	**Anomaly-based network intrusion detection (behavior-based IDS) using machine-learning classification of network traffic (monitors**	**Multi-Layer Perceptron (MLP) classifier optimized by a hybrid metaheuristic (HADMLP model combining Artificial Bee**	**Achieves high detection accuracy and low false alarms on benchmark datasets (e.g. ~97.2% accuracy with 97.86% detection rate**	**Covers a wide range of network intrusions, including Denial-of-Service (DoS) attacks, Probe/Scanning attacks, Remote-to-**

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

abnormal vs. normal behavior).	**Colony (ABC) and Dragonfly Algorithm (DA) for training) link.springer.com. Utilizes multi-objective wrapper feature selection with an ABC algorithm (MO-ABC) to choose optimal feature subsets link.springer.com. The integrated model is termed MO-HADMLP (Multi-Objective Hybrid ABC-DA MLP).**	**on KDD'99; ~95.37% accuracy with 93.45% detection on ISCX 2012, with false alarm rates ~0.04 and 0.025). Uses a reduced feature set (selected via multi-objective optimization) rather than all features, improving computational efficiency without degrading performance.**	**Local (R2L) and User-to-Root (U2R) exploits (as per KDD Cup 99 dataset), as well as modern attack scenarios from ISCX 2012 (such as distributed denial-of-service (DDoS) – including HTTP flooding – infiltration/injection attacks, and brute-force login attempts) core.ac.uk.**

6.3 Comparative Analysis of 2022 IoT Intrusion Detection Systems: Methods, Techniques, and Future Directions.

In 2022, the research focused on hybrid optimization techniques, improved feature selection strategies, and intricate machine and deep learning models developed for Internet of Things environments. Key strategies included feature selection and optimization techniques such as Chi-square, Mutual Information, Gorilla Troops Optimizer (GTO), Bird Swarm Algorithm (BSA), Aquila Optimizer, Modified Deer Hunting Optimization (MDHO), Particle Swarm Optimization (PSO), and Genetic Algorithm (GA) to improve intrusion detection system (IDS) accuracy while reducing computational complexity and false positives. Tree-based stacking ensembles that integrated XGBoost, Random Forest, and Decision Trees enhanced the robustness of detection, and deep learning and machine learning models were significant. In addition, CNN models improved with Aquila demonstrated usefulness for high-dimensional IoT data, while Bi-directional GRU (BiGRU) models enhanced by Multiverse Optimization (MVO) demonstrated excellent performance. Resource efficiency and scalability were major considerations for developing lightweight solutions for real-time IoT activities, such as

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

collaborative ensemble learning and Deep Autoencoder techniques improved by MDHO. These models targeted a variety of threats, including general IoT attacks, IoE-specific threats, DDoS, R2L, U2R, probing attacks, and botnets (Mirai, Bashlite). The 2022 study concentrated on hybrid models, intensive feature optimization, and advanced ensemble techniques to address IoT and IIoT cybersecurity challenges, particularly in resource-constrained, real-time, and scalable scenarios.

Table 3: Comparison of IoT Intrusion Detection Systems (2022): Methodologies, Techniques, Characteristics, and Attack Types

Author's	Detection Methodology	Specific Techniques	Characteristics	Type of Attacks
[1]	**Chi-square for feature selection and SMOTE**	**XGBoost, KNN, RF for classification**	**Real-time, scalable, handles IoT-specific patterns**	**IoT-specific (Binary & Multi-class scenarios)**
[19]	**Tree-based stacking ensemble with SelectKBest**	**Stacking ensemble model with DT, RF, and XGBoost**	**High detection accuracy, ensemble methods improve robustness**	**General IoT attacks**
[4]	**GTO and BSA for hybrid feature selection**	**Hybrid of Gorilla Troops Optimizer and Bird Swarm Algorithm**	**Optimized for IoT, improves convergence speed**	**IoT intrusion detection**
[5]	**Collaborative feature selection with ensemble learning**	**Decision Trees, Extra Trees, Random Forest, and XGBoost for ensemble learning**	**Efficient, lightweight, ensemble-based**	**DDoS, botnet**
[86]	**MDHO for feature selection, Deep**	**Modified Deer Hunting Optimization for feature**	**Highly efficient, optimized for resource-**	**DoS, R2L, U2R, Probe**

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

	Autoencoder for detection	**selection, Deep Autoencoder for classification**	**constrained networks**	
[87]	**Systematic review of AI techniques**	**Review of AI methods such as SVM, RF, CNN, RNN, hybrid models**	**Broad overview, highlights trends and effectiveness**	**IoT (varied attack types)**
[6]	**BiGRU with MVO for hyperparameter optimization**	**Multiverse Optimization for tuning BiGRU hyperparameters**	**High accuracy, BiGRU enhances performance**	**IoE-specific threats**
[88]	**PSO for feature selection, RF for detection**	**Particle Swarm Optimization for feature selection, RF for classification**	**Optimized for IoT networks, high detection accuracy**	**IoT network attacks**

6.4 Comparative Analysis of (2023) IoT Intrusion Detection Systems: Methods, Techniques, and Future Directions.

A comparison of intrusion detection systems (IDS) created for the Internet of Things in 2023 is shown in Table 4. That year's research demonstrated notable advancements in hybrid and ensemble models, which are especially intended for IoT, IIoT, and smart environments. The development of IDS solutions that facilitate real-time and decentralized operations was made possible by major emphasis on feature optimization, scalability, and computing efficiency. In order to handle changing assault scenarios, future research attempts to investigate bigger datasets, improve data balancing strategies, and incorporate sophisticated deep learning models.

With numerous models surpassing 95% and frameworks like IDS-SIoEL, BGWO-RFE-XGBoost, and POGO reaching 100%, the primary metrics for IDS in 2023 show remarkable accuracy. In IoT situations with limited resources, lightweight models—like those that use Grasshopper Optimization and Hybrid Autoencoder with PSO—showed remarkable performance. In addition to feature selection approaches like Grey Wolf Optimization and Chimp Optimization, sophisticated methods like Improved Ant Colony Optimization with

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Ensemble Classifier and Random Forest with RBFNN were used to reduce false positive rates. Lightweight models (like Binary Chimp Optimization and ExtraTree classifiers) and dimensionality reduction strategies (like PSO-GA and ECSO) increased efficiency. Adaptive Tree-Based Ensemble Networks (ATBEN) and ResNet-GRU for multi-class classification in IoT and IoV environments improved adaptability, while distributed systems (e.g., DD-GAN) and federated learning models (e.g., ResNet-GRU with Federated Learning) addressed scalability.

Typical IDS methods included machine learning techniques (e.g., XGBoost, Random Forest, ResNet50), hybrid models (e.g., POGOA, Hybrid Autoencoder with PCA), and feature selection and optimization (e.g., BGWO, GOA, PSO-GA). For managing high-dimensional data and identifying zero-day threats, deep learning models like as CNN-GRU, GAN-DNN, and BiLSTM were extensively utilized. High accuracy and robustness were attained by hybrid and ensemble approaches, such as AdaBoost with Mutual Information and Hybrid Autoencoder with PSO. Scalability and privacy were prioritized in distributed and federated learning models, such as ResNet-GRU with Federated Learning. With fewer false positives, anomaly detection methods like Sparse Capsule Autoencoder and Hybrid Autoencoder with Modified PSO focused on IoT-specific anomalies. Efficiency and adaptability in IoT security applications were further enhanced by advanced optimization techniques like Dung Beetle Optimization and Enhanced Cat Swarm Optimization.

Table 4: Comparison of IoT Intrusion Detection Systems (2023): Methodologies, Techniques, Characteristics, and Attack Types

Authors	Detection Methodology	Specific Techniques	Characteristics	Type of Attacks
[89]	**Systematic review of IDS literature focusing on decision tree models**	**Decision Trees, RNN, LSTM, CNN, DBN, GAN**	**Focus on enhancing anomaly detection with decision tree-based frameworks**	**General network intrusions**
[54]	**Review of ensemble learning methods for anomaly detection**	**Bagging, Boosting, Stacking**	**Improves detection rates and adaptability using ensemble learning**	**General cyber threats**
[21]	**Comparison of feature selection and feature**	**Correlation-based feature selection,**	**Optimizes feature reduction for**	**IoT network intrusions**

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

	extraction techniques	**PCA-based extraction**	**efficient detection**	
[45]	**GA for feature selection, RF for classification**	**Genetic Algorithm for feature selection, Random Forest for classification**	**Reduces false positives, increases detection accuracy**	**IoT network attacks**
[55]	**Hybrid optimization approach for dataset balancing**	**Grey Wolf Optimization, Dipper Throated Optimization, LSH-SMOTE**	**Addresses dataset imbalances in IoT networks**	**IoT-specific attacks like Sybil, blackhole, hello flooding**
[10]	**Chaotic Cuckoo Search Optimization Algorithm with Optimal Wavelet Kernel Extreme Learning Machine**	**CCSOA for feature selection, OWKELM for classification**	**Targets IIoT challenges with high data heterogeneity**	**General IIoT threats**
[55]	**Voting classifier with metaheuristic optimization**	**DTO-Guided WOA, Neural Networks, RF, KNN**	**Optimized ensemble improves classifier performance**	**IoT-specific intrusions like Sybil, hello flooding**
[90]	**Comprehensive review of ML techniques for H-IoT security**	**CNN, SVM, Random Forest, Chi-Square tests**	**Focuses on privacy and real-time anomaly detection**	**H-IoT threats like DoS, injection attacks**
[56]	**Hybrid classification with RF-XGB**	**RF-XGB, CLK-M**	**Tailored to hierarchical WSNs for**	**WSN attacks like DoS, U2R, R2L**

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

	and K-Means clustering		**anomaly detection**	
(Maseno & Wang, n.d. 2023)	**Stacked ensemble of multiple classifiers**	**ELM, SVM, KNN, Logistic Regression**	**Enhances detection accuracy for IoT networks**	**Modern IoT-specific threats**
[45]	**DNN with GAN-based class balancing**	**GAN-DNN, Pearson's correlation for feature selection**	**Addresses class imbalance in IoT datasets**	**IoT traffic anomalies**
[57]	**Hybrid model combining signature and anomaly-based detection**	**Random Forest, Neural Networks, Gradient Boosting**	**Focuses on known and unknown cloud attacks**	**Cloud-specific intrusions**
[58]	**Hybrid ML/DL models for satellite networks**	**RF-SFS with RF, ANN, LSTM, GRU**	**Balances detection accuracy and efficiency in STINs**	**Satellite-terrestrial intrusions**
[91]	**Literature review of supervised ML techniques for IoT security**	**Decision Trees, Random Forest, SVM, KNN, Bagging, Boosting**	**Focuses on lightweight IDS and IoT-specific datasets**	**IoT-specific cyber threats**
[47]	**Hybrid CNN-GRU deep learning model for spatial and temporal patterns**	**CNN for spatial, GRU for temporal, Pearson Correlation for feature selection**	**Enhances feature learning for zero-day attack detection**	**DDoS, brute force, infiltration**
[46]	**CNN-RNN hybrid for spatial and temporal data patterns**	**SoftMax for classification, oversampling for imbalance**	**Targets high accuracy and low false positives**	**Diverse network intrusions**

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[29]**. (2023)**	**Hunger Games Search Optimization (HGSO) with Graph Convolutional Network (GCN)**	**HGSO for features, Sparrow Search Optimization for hyperparameters**	**Optimizes detection in IIoT networks**	**Binary and multiclass attacks**
[49]	**DD-GAN with Improved Firefly Optimization**	**GAN for distributed systems, Hybrid CNN-ANFIS for classification**	**Distributed anomaly detection for IoT**	**IoT-specific attacks like DDoS, DoS**
[59]	**Hybrid model with Autoencoder for feature extraction and Random Forest for selection**	**RBM for classification**	**Designed for smart city IoT environments**	**Smart city network threats**
[48]	**1D-CNN with Chimp Optimization for feature selection**	**OSS, SMOTE for balancing, hierarchical model**	**Focuses on feature optimization**	**DoS, Probe, U2R, R2L**
[30]	**Hybrid ensemble with PCA for feature extraction**	**Bagging, Stacking, AdaBoost optimized with GWO**	**Focuses on SCADA and smart city security**	**Critical infrastructure threats**
[91]	**Review of supervised ML techniques for IoT IDS**	**Decision Trees, Random Forest, SVM, KNN, Bagging, Boosting**	**Lightweight IDS for IoT, focus on datasets and algorithms**	**IoT-specific cyber threats**
[47]	**Hybrid CNN-GRU model**	**CNN for spatial and GRU for temporal patterns**	**Enhanced zero-day attack detection with feature optimization**	**DDoS, brute force, infiltration**

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[46]	**Hybrid CNN-RNN IDS**	**SoftMax for classification, oversampling to address imbalance**	**Handles high data volume and complex traffic**	**Diverse network intrusions**
[29] **(2023)**	**HGSO with GCN**	**HGSO for feature selection and SSO for hyperparameter tuning**	**Addresses IIoT complexities and resource constraints**	**Binary and multiclass attacks**
[92]	**PSO-GA for feature selection with ELM-BA classifier**	**Bootstrap aggregation for improved accuracy**	**Effective IDS for IoT with high detection accuracy**	**IoT-specific threats**
[49]	**DD-GAN with Improved Firefly Optimization**	**Hybrid CNN-ANFIS**	**Distributed IDS for IoT with adaptive features**	**DDoS, DoS**
[59]	**Hybrid model with Autoencoder for feature extraction**	**Random Forest, Restricted Boltzmann Machine (RBM)**	**Focused on smart city security**	**IoT-based smart city intrusions**
[30]	**Hybrid ensemble with PCA for feature reduction**	**Bagging, Stacking, Adaboost, GWO optimization**	**Focuses on SCADA system security**	**Industrial sensor and SCADA attacks**
[93],	**Ensemble Learning with AdaBoost**	**AdaBoost with Boruta, Mutual Information, and Pearson Correlation for feature selection**	**High accuracy, real-time detection, low processing time**	**DDoS, DoS, Brute Force, Botnet**
[25]	**Hybrid Metaheuristics-Deep Learning Model**	**BiLSTM, GRU, and ELM combined in a weighted ensemble,**	**Optimized for high-dimensional IoT data, real-time capabilities**	**DDoS, IoT-specific attacks**

Received: August 09, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

		HHO-EFDM for feature selection		
[77]	**Z-score with Improved Bacterial Foraging Optimization**	**Z-score normalization, IBFO for feature selection, MLSTM for classification**	**High accuracy, reduced computational cost**	**Smart city IoT anomalies**
[22].	**Comparative ML Model Analysis**	**ResNet50, LSTM, and KNN models compared**	**High accuracy with ResNet50, optimized for ad hoc IoT networks**	**Black Hole Attacks**
[92].	**Hybrid Ensemble ELM-BA**	**PSO-GA for feature selection, ELM-BA for classification**	**High accuracy, resilient to diverse IoT attack types**	**PortScan, SQL Injection, Brute Force**
[94].	**Federated Learning with ResNet-GRU**	**Federated learning with Chi-Square, RFE, Lasso for feature selection**	**High privacy, decentralized model, optimized for edge IoT systems**	**Botnet Attacks**
[20].	**Hybrid BGWO-RFE-XGBoost**	**Binary Grey Wolf Optimization, RFE for feature selection, XGBoost for classification**	**High detection rates, lightweight, SMOTE for data balancing**	**IoT-specific DDoS**
[60].	**RF with RBFNN Hybrid Model**	**Random Forest for feature selection, RBFNN for classification**	**Reduced computational overhead, high Matthews Correlation Coefficient (MCC)**	**Data Breaches, Unauthorized Access**

Received: August 09, 2025

International Journal of Applied Mathematics
Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[95]	**Adaptive Tree-Based Ensemble Network (ATBEN)**	**XGBoost, LightGBM, RF, and Extra Trees in a cascading structure**	**Optimized for multiclass classification, handles data imbalance effectively**	**IoV-specific attacks**
[28]	**Cat Swarm Optimization with Twin SVM**	**ECSO for feature selection, Mayfly Optimization with Twin SVM for classification**	**High-dimensional data, efficient detection**	**IoT-specific Cyberattacks**
[96]	**Privacy Preserving Model for Smart Agriculture**	**Sparse Capsule Autoencoder (SCAE), AGRU for anomaly detection**	**Privacy preservation, optimized for agricultural IoT systems**	**IoT Agriculture Anomalies**
[97]	**Deep Belief Network with Blockchain**	**HBA for feature selection, OHDBN for classification, Dung Beetle Optimization**	**High accuracy, secure against evolving threats**	**Blockchain IoT Anomalies**
[24]	**Hybrid Autoencoder and PSO**	**HAEMPSO for feature selection, DNN for classification**	**High accuracy, lightweight, reduced computational load**	**IoT-specific Anomalies**
[55]	**GWDTO Hybrid Optimization Model**	**Grey Wolf Optimization and Dipper Throated Optimization combined**	**Efficient feature selection, balances exploration and exploitation**	**Sybil, Blackhole, Sinkhole, DDoS**
[61]	**FSAP and SABADT Hybrid Model**	**FSAP for feature selection, SABADT for hybrid detection**	**High accuracy, robust against known and unknown attacks**	**Zero-day, DoS, DDoS**

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[50].	**Lightweight ExtraTree Classifier**	**ExtraTree for feature selection, LR, NB, RF, ANN, and KNN for classification**	**Lightweight, scalable for constrained IoT devices**	**DDoS**
[78].	**Binary Chimp Optimization Algorithm**	**BCOA for feature selection, CCR-ELM for classification**	**Lightweight, high accuracy, optimized for WSN environments**	**IoT WSN-specific Attacks**
[62]	**Ant Colony Optimization with Ensemble Classifier**	**IACO for feature selection, MLEID with DDT, ANFIS, and MDSVM**	**High accuracy, low false positive rate**	**IoT Protocol-Specific Attacks**

6.5 Comparative Analysis of (2024) IoT Intrusion Detection Systems: Methods, Techniques, and Future Directions.

A comparison of intrusion detection systems (IDS) created for the Internet of Things in 2024 is shown in Table 5. It lists the main conclusions from each study as well as detection strategies, tactics, features, and targeted attack kinds. IDS for IoT and associated contexts saw major gains in 2024 as a result of research that focused on hybrid, ensemble, and domain-specific models. The goal was to develop accurate, scalable, and lightweight models that could detect in real time across a variety of applications. In order to adjust to dynamic and changing threat landscapes, future research attempts to correct class imbalances, significantly minimize processing overhead, and include cutting-edge AI techniques.

IoT-Defender, DenseNet201-based IDS, and SmartSentry were among the frameworks that achieved outstanding detection rates throughout IoT and IIoT scenarios in 2024, according to key metrics for IDS in IoT that emphasized high accuracy. Methods like GWO-based ensemble learning and VTR-HLSTM increased accuracy while lowering false positive rates. Lightweight models that optimized feature selection and classification for resource-constrained contexts employing Genetic Algorithms (GA), Bat Algorithms (BA), and Particle Swarm Optimization (PSO) were used to emphasize efficiency. Distributed models that addressed scalability, such as IoT-Defender and DenseNet201, demonstrated good performance in extensive IoT and IIoT networks. Domain-specific solutions, such those designed for medical IoT (IoMT) and IIoT, improved adaptability by successfully addressing particular challenges in these contexts. Feature selection methods such as PCA, IG, and RNS were used to reduce false positive rates.

Modified Genetic Algorithm (MGA) in conjunction with LSTM, Bat Algorithm (BA), and PSO in conjunction with AdaBoost or deep learning models were examples of common IDS

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

techniques that involved feature selection and optimization. The resilience of machine learning techniques like Random Forest (RF) and XGBoost in managing intricate IoT traffic and real-time detection led to their widespread deployment. DenseNet201 with CGAN and VTR-HLSTM are two examples of deep learning models that enhanced classification accuracy and resource optimization. Voting Gray Wolf Optimizer (GWO) and stack classifiers are examples of hybrid and ensemble approaches that improved detection performance and dealt with unbalanced datasets. Domain-specific models, such as VTR-HLSTM for cloud environments and PSO-AdaBoost for IoMT, offered customized defenses against certain threats. In IoT and IIoT systems, anomaly detection models like DenseNet201 with RAPNet and DNN-based SmartSentry successfully detected malware, brute force assaults, and DDoS.

Table 5: Comparison of IoT Intrusion Detection Systems (2024): Methodologies, Techniques, Characteristics, and Attack Types.

Authors (APA with Year)	Detection Methodology	Specific Techniques	Characteristics	Type of Attacks
[9]	**Network-based IDS**	**MGA for feature selection, LSTM for classification**	**Lightweight IDS for IoT, optimized for edge computing. Real-time intrusion detection.**	**Detects a variety of cyberattacks, including zero-day attacks.**
[9]**.**	**Network-based IDS**	**Ensemble feature selection with DSNN**	**Focuses on improving detection in IIoT using ensemble methods. High performance against DDoS and ransomware.**	**Handles emerging threats like botnets and ransomware in IIoT environments.**
[98]**.**	**Network-based IDS**	**Bat Algorithm and RNS for feature selection**	**Handles high-dimensional data with improved computational efficiency.**	**Focuses on high-dimensional network traffic to detect various attack types effectively.**
[79]**.**	**Network-based IDS**	**PCA and IG with GWO**	**Lightweight model suitable for IoT with ensemble classifiers.**	**Cyberattacks in IoT, specifically focusing on imbalanced datasets.**

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[99].	**Network-based IDS**	**Feature selection (IG), feature extraction (PCA)**	**Comparison of feature selection and extraction techniques for resource-constrained IoT devices.**	**IoT-specific attack mitigation by optimizing computational load and detection efficiency.**
[31].	**Network-based and host-based IDS**	**LSTM, CNN, and ensemble learning**	**Comprehensive review of ML/DL techniques, with a focus on addressing real-time anomaly detection challenges.**	**Discusses attacks like DDoS, SQL injection, and brute force in IoT.**
[11]	**Network-based IDS**	**Random Forest, XGBoost**	**Focused on botnet attack detection with high accuracy and minimal resource use.**	**Botnet-specific attack detection in IoT environments.**
[32]	**Network-based IDS**	**Pearson correlation-based feature selection, ensemble models**	**Addresses challenges like high dimensionality and imbalanced datasets with multi-class classification techniques.**	**Multi-class network anomalies, including various types of intrusions.**
[33]	**Anomaly-based NIDS**	**Review of various ML and DL models**	**Summarizes trends in datasets, validation methods, and algorithms for anomaly detection in NIDS.**	**Discusses a wide variety of anomaly-based detection methods for modern attack scenarios.**
[63]	**Anomaly-based NIDS**	**GA-based hyperparameter tuning, hybrid feature selection**	**Optimized models for better accuracy and detection time.**	**Focuses on improving computational efficiency in detecting network anomalies in IoT environments.**

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[34]	**Anomaly-based NIDS**	**Oversampling, PCA, stacking feature embedding**	**Addressing imbalanced data issues with scalable, high-performance ML models.**	**Detection of minority class attacks in large-scale datasets.**
[80]	**Anomaly-based IDS**	**Improved CSA with DAP, Min-Max Scalar for balancing**	**Efficient class balancing and scaling for IoT datasets.**	**General network intrusions, addressing class imbalance.**
[100]	**Anomaly-based IDS**	**K-Best feature selection, stack classifier**	**Focuses on top 15 critical features to enhance classification in IoT networks.**	**Diverse IoT network attacks in Ton-IoT datasets.**
[23] **2024**	**Anomaly-based IDS**	**GA-ELM feature selection, SVM for classification**	**Reduces feature set efficiently while maintaining high accuracy.**	**General IoT intrusions with high-dimensional datasets.**
[35]	**Anomaly-based IDS**	**ABC optimization for feature selection, ensemble models**	**Efficient feature reduction and high detection speed tailored for cloud environments.**	**Intrusions in cloud environments, tackling high-dimensional data.**
[36]	**Anomaly-based IDS**	**GWO and EBG for feature selection, SVM, XGBoost**	**Lightweight preprocessing model balancing detection accuracy with IoT resource constraints.**	**IoT-specific attacks, including malware and DDoS.**
[37]	**Anomaly-based IDS**	**Harris-Hawks Optimizer, ensemble techniques**	**Combines multiple optimization algorithms with**	**IoT anomalies, focusing on complex interconnected systems.**

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

			classifiers for IoT-specific security.	
[76]	**Anomaly-based IDS**	**PSO for feature selection, AdaBoost for classification**	**Tailored for IoMT environments, emphasizing medical data security.**	**Medical device intrusions, such as DoS and unauthorized access.**
[65]	**Anomaly-based IDS**	**DenseNet201, RAPNet for feature extraction**	**Addresses imbalanced datasets with CGAN and improves attack detection in IoT networks.**	**IoT attacks like DDoS, brute force, and SQL injection.**
[38]	**Anomaly-based IDS**	**Modified Binary PIO, Random Forest for classification**	**Reduces FPR and enhances detection accuracy with optimized feature selection.**	**IoT cyber assaults, including benign and malicious traffic.**
[50]	**Anomaly-based IDS**	**DNN, PCA for feature selection**	**High accuracy for binary and multiclass classifications in IIoT.**	**IIoT-specific attacks like DDoS, MITM, and malware.**
[39]	**Anomaly-based IDS**	**Machine Learning Algorithms**	**Focuses on IoT environments, enhancing security through machine learning-based intrusion detection and prevention.**	**General IoT intrusions**
[51]**.**	**Anomaly-based IDS**	**VTR-HLSTM deep learning model**	**Tailored for cloud computing environments, focusing on optimizing performance and**	**Cloud-specific intrusions**

Received: August 09, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

bolstering security measures.

7 Challenges in Current IDS Research

The report identifies a number of important obstacles that intrusion detection system (IDS) development must overcome especially when considering IoT environments the imbalance and limits of datasets is one of the main problems Training and evaluating IDS models is hampered by the lack of diversity and realism and representativeness of contemporary IoT scenarios in many of the datasets now in use. Additionally underrepresented attack types in imbalanced datasets result in subpar detection performance for minority classes. Dealing with changing cyberthreats including zero-day assaults is another crucial concern. Because they lack the patterns that current IDS models are trained to identify these new and undiscovered vulnerabilities are becoming more challenging to identify in order to keep up with new threats, IDS solutions must have features for ongoing learning and adaptability. Furthermore, computational overheads continue to be a major obstacle particularly in real time applications. Since many IoT networks are made up of devices with limited resources the high processing and memory requirements of sophisticated IDS algorithms may not be feasible to effectively handle this challenge, systems must be designed with minimal latency and a balance between accuracy and efficiency. All of these challenges highlight the necessity of creative methods in IDS research and development.

Figure 5 illustrates how the characteristics of the Internet of Things (IoT) environment such as interconnected devices limited resources and high variability lead to significant cybersecurity challenges these challenges reveal the limitations of traditional intrusion detection systems particularly in the IoT where they struggle to handle large amounts of data consequently this drives innovation toward advanced intrusion detection frameworks that integrate machine learning and deep learning and feature selection and hybrid approaches ultimately leading to more accuracy and efficiency.

Received: August 09, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

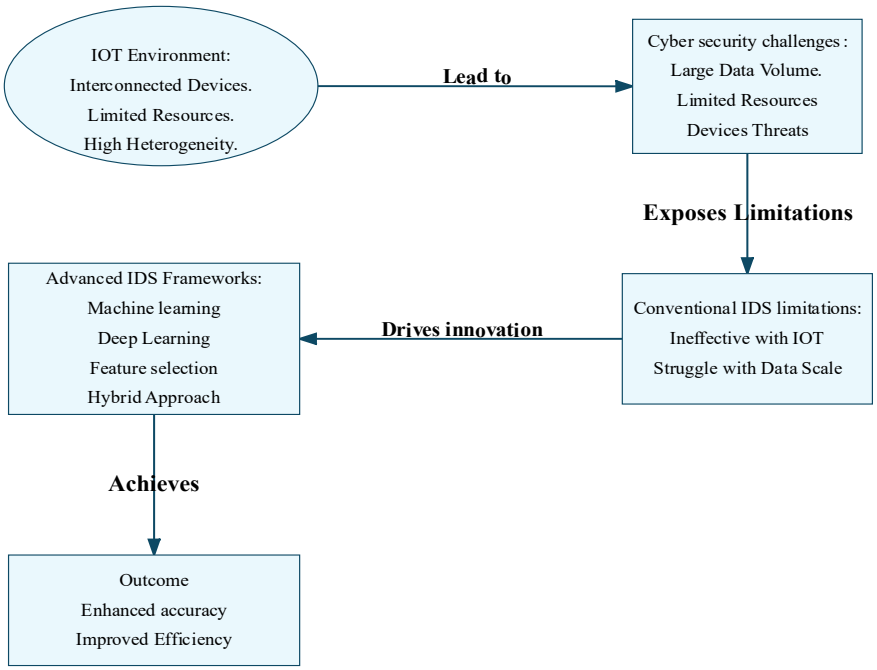

Figure 5: Evolution of Intrusion Detection Systems (IDS) to Address IoT-Specific Challenges

8 Future Directions and Recommendations

In order to improve the efficacy of Intrusion Detection Systems (IDS) in Internet of Things environments, the paper highlights a number of crucial areas for further research. Integrating cutting-edge artificial intelligence (AI) methods like generative adversarial networks (GANs) and reinforcement learning is one crucial avenue. While GANs can enhance anomaly detection by producing realistic synthetic data to solve issues like class imbalance, reinforcement learning can allow IDS to dynamically adapt to changing threats by gradually learning the best responses. The creation of privacy-preserving IDS using federated learning is another crucial area of emphasis. Federated learning ensures data privacy and lowers the possibility of sensitive information being revealed during training by enabling several IoT devices to work together to train IDS models without exchanging raw data. Furthermore, IDS that are adaptable and lightweight and that can function well in IoT situations with limited resources are desperately needed. In order to expand to meet the increasing complexity and volume of IoT networks, these systems need to achieve a balance between high detection accuracy and low computing overhead. When combined, these developments will contribute to the development of reliable, scalable, and secure IDS solutions that are suited to the particular difficulties faced by IoT ecosystems.

9 Conclusion

An intriguing interaction between creativity and necessity can be seen in the development of Intrusion Detection Systems (IDS) for Internet of Things contexts. Hybrid models, including

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

CNN-LSTM and PCA-GWO, have changed the game by combining many approaches to improve threat identification, scalability, and accuracy. In order to reduce computing costs without compromising performance, feature selection techniques such as Particle Swarm Optimization (PSO), Genetic Algorithms (GA), and Recursive Feature Elimination (RFE) have proven essential. Random Forest, XGBoost, CNN, LSTM, and GRU are machine and deep learning models that are pushing the envelope and are particularly good at detecting IoT-specific attacks using both anomaly and signature-based detection. In resource-constrained IoT ecosystems, lightweight IDS designs have proven crucial in ensuring security does not compromise efficiency. Many models currently perform better than 95% of the time, and frameworks like DenseNet201 and SmartSentry are getting closer to perfection. Methods like ensemble learning and Ant Colony Optimization have improved detection even more, reducing false positives while preserving high precision. Scalability is being directly addressed by distributed intrusion detection systems (IDS) techniques, such as DD-GAN and ResNet-GRU with Federated Learning, which allow for real-time threat monitoring over large networks. But problems still exist. Class imbalances are still a problem, but SMOTE and GAN-based balancing show promise in identifying infrequent but serious dangers. The necessity for customized security solutions is highlighted by domain-specific models for cloud, IIoT, and IoMT settings. But the lack of realistic, varied datasets and the persistent rise of zero-day threats necessitate ongoing attention to detail. In large-scale installations, computational overheads continue to impede real-time performance, necessitating more optimization. IDS will likely become smarter and more adaptive in the future. While Federated Learning provides a privacy-preserving route for decentralized IoT security, reinforcement learning, GANs, and hybrid deep learning models have the potential to completely transform threat responsiveness. The final objective? IDS that are able to learn, adapt, and remain ahead of cyber threats in real time—not just react. Although there is still a long way to go before IoT security is really resilient, the progress gained thus far suggests an exciting and safe future.

10 Reference.

[1] A. R. Gad, M. Haggag, A. A. Nashat, and T. M. Barakat, “A Distributed Intrusion Detection System using Machine Learning for IoT based on ToN-IoT Dataset,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 6, 2022, doi: 10.14569/IJACSA.2022.0130667.

[2] A. Fatani, A. Dahou, M. A. A. Al-qaness, S. Lu, and M. A. Abd Elaziz, “Advanced Feature Extraction and Selection Approach Using Deep Learning and Aquila Optimizer for IoT Intrusion Detection System,” *Sensors*, vol. 22, no. 1, p. 140, Dec. 2021, doi: 10.3390/s22010140.

[3] M. Al-Sarem, F. Saeed, E. H. Alkhammash, and N. S. Alghamdi, “An Aggregated Mutual Information Based Feature Selection with Machine Learning Methods for Enhancing IoT Botnet Attack Detection,” *Sensors*, vol. 22, no. 1, p. 185, Dec. 2021, doi: 10.3390/s22010185.

[4] S. S. Kareem, R. R. Mostafa, F. A. Hashim, and H. M. El-Bakry, “An Effective Feature Selection Model Using Hybrid Metaheuristic Algorithms for IoT Intrusion Detection,” *Sensors*, vol. 22, no. 4, p. 1396, Feb. 2022, doi: 10.3390/s22041396.

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[5] M. Alanazi and A. Aljuhani, "Anomaly Detection for Internet of Things Cyberattacks," *Comput. Mater. Contin.*, vol. 72, no. 1, pp. 261–279, 2022, doi: 10.32604/cmc.2022.024496.

[6] M. Ahmed Hamza *et al.*, "Hyperparameter Tuned Deep Learning Enabled Intrusion Detection on Internet of Everything Environment," *Comput. Mater. Contin.*, vol. 73, no. 3, pp. 6579–6594, 2022, doi: 10.32604/cmc.2022.031303.

[7] E. Özer, M. İskefiyeli, and J. Azimjonov, "Toward lightweight intrusion detection systems using the optimal and efficient feature pairs of the Bot-IoT 2018 dataset," *Int. J. Distrib. Sens. Netw.*, vol. 17, no. 10, p. 155014772110522, Oct. 2021, doi: 10.1177/15501477211052202.

[8] M. A. Siddiqi and W. Pak, "An Agile Approach to Identify Single and Hybrid Normalization for Enhancing Machine Learning-Based Network Intrusion Detection," *IEEE Access*, vol. 9, pp. 137494–137513, 2021, doi: 10.1109/ACCESS.2021.3118361.

[9] Y. K. Saheed, O. H. Abdulganiyu, and T. A. Tchakoucht, "Modified genetic algorithm and fine-tuned long short-term memory network for intrusion detection in the internet of things networks with edge capabilities," *Appl. Soft Comput.*, vol. 155, p. 111434, Apr. 2024, doi: 10.1016/j.asoc.2024.111434.

[10] R. Gopi *et al.*, "Intelligent Intrusion Detection System for Industrial Internet of Things Environment," *Comput. Syst. Sci. Eng.*, vol. 44, no. 2, pp. 1567–1582, 2023, doi: 10.32604/csse.2023.025216.

[11] T. Zhukabayeva, L. Zholshiyeva, K. Ven-Tsen, A. Adamova, Y. Mardenov, and N. Karabayev, "Enhancing IoT Security: Effective Botnet Attack Detection Through Machine Learning," *Procedia Comput. Sci.*, vol. 241, pp. 421–426, 2024, doi: 10.1016/j.procs.2024.08.058.

[12] K. T. W. Teuwen, T. Mulders, E. Zambon, and L. Allodi, "Ruling the Unruly: Designing Effective, Low-Noise Network Intrusion Detection Rules for Security Operations Centers," in *Proceedings of the 20th ACM Asia Conference on Computer and Communications Security*, Hanoi Vietnam: ACM, Aug. 2025, pp. 1428–1441. doi: 10.1145/3708821.3710823.

[13] G. Amirthayogam, N. Kumaran, S. Gopalakrishnan, K. R. A. Brito, S. RaviChand, and S. B. Choubey, "Integrating Behavioral Analytics and Intrusion Detection Systems to Protect Critical Infrastructure and Smart Cities," *Babylon. J. Netw.*, vol. 2024, pp. 88–97, July 2024, doi: 10.58496/BJN/2024/010.

[14] P. Maniriho, E. Niyigaba, Z. Bizimana, V. Twiringiyimana, L. J. Mahoro, and T. Ahmad, "Anomaly-based Intrusion Detection Approach for IoT Networks Using Machine Learning," in *2020 International Conference on Computer Engineering, Network, and Intelligent Multimedia (CENIM)*, Surabaya, Indonesia: IEEE, Nov. 2020, pp. 303–308. doi: 10.1109/CENIM51130.2020.9297958.

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[15] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city," *Future Gener. Comput. Syst.*, vol. 107, pp. 433–442, June 2020, doi: 10.1016/j.future.2020.02.017.

[16] W. A. H. M. Ghanem, A. Jantan, S. A. A. Ghaleb, and A. B. Nasser, "An Efficient Intrusion Detection Model Based on Hybridization of Artificial Bee Colony and Dragonfly Algorithms for Training Multilayer Perceptrons," *IEEE Access*, vol. 8, pp. 130452–130475, 2020, doi: 10.1109/ACCESS.2020.3009533.

[17] A. Guezzaz, S. Benkirane, M. Azrour, and S. Khurram, "A Reliable Network Intrusion Detection Approach Using Decision Tree with Enhanced Data Quality," *Secur. Commun. Netw.*, vol. 2021, pp. 1–8, Aug. 2021, doi: 10.1155/2021/1230593.

[18] S. M. Kasongo, "An Advanced Intrusion Detection System for IIoT Based on GA and Tree Based Algorithms," *IEEE Access*, vol. 9, pp. 113199–113212, 2021, doi: 10.1109/ACCESS.2021.3104113.

[19] M. Rashid, J. Kamruzzaman, T. Imam, S. Wibowo, and S. Gordon, "A tree-based stacking ensemble technique with feature selection for network intrusion detection," *Appl. Intell.*, vol. 52, no. 9, pp. 9768–9781, July 2022, doi: 10.1007/s10489-021-02968-1.

[20] B. Xu, L. Sun, X. Mao, R. Ding, and C. Liu, "IoT Intrusion Detection System Based on Machine Learning," *Electronics*, vol. 12, no. 20, p. 4289, Oct. 2023, doi: 10.3390/electronics12204289.

[21] V.-D. Ngo, T.-C. Vuong, T. V. Luong, and H. Tran, "Machine Learning-Based Intrusion Detection: Feature Selection versus Feature Extraction," July 04, 2023, *arXiv*: arXiv:2307.01570. Accessed: Nov. 03, 2024. [Online]. Available: http://arxiv.org/abs/2307.01570

[22] R. Salama, Wajdi Alghamdi, S. Yadav, Harikumar Pallathadka, Dolpriya Devi Manoharmayum, and M. Tiwari, "Exploring Machine Learning Methods for IoT Network Intrusion Detection Systems," *J. Adv. Zool.*, vol. 44, no. S-5, pp. 1045–1053, Oct. 2023, doi: 10.17762/jaz.v44iS-5.1089.

[23] E. M. Maseno and Z. Wang, "Intrusion Detection in IoT Using Ensemble Approach".

[24] Y. K. Saheed, A. A. Usman, F. D. Sukat, and M. Abdulrahman, "A novel hybrid autoencoder and modified particle swarm optimization feature selection for intrusion detection in the internet of things network," *Front. Comput. Sci.*, vol. 5, p. 997159, Apr. 2023, doi: 10.3389/fcomp.2023.997159.

[25] P. Sanju, "Enhancing intrusion detection in IoT systems: A hybrid metaheuristics-deep learning approach with ensemble of recurrent neural networks," *J. Eng. Res.*, p. 100122, June 2023, doi: 10.1016/j.jer.2023.100122.

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[26] C. Hazman, A. Guezzaz, S. Benkirane, and M. Azrour, "lIDS-SIoEL: intrusion detection framework for IoT-based smart environments security using ensemble learning," *Clust. Comput.*, vol. 26, no. 6, pp. 4069–4083, Dec. 2023, doi: 10.1007/s10586-022-03810-0.

[27] W. Gou, H. Zhang, and R. Zhang, "Multi-Classification and Tree-Based Ensemble Network for the Intrusion Detection System in the Internet of Vehicles," *Sensors*, vol. 23, no. 21, p. 8788, Oct. 2023, doi: 10.3390/s23218788.

[28] A. S. Almasoud, "Enhanced Metaheuristics with Machine Learning Enabled Cyberattack Detection Model," *Intell. Autom. Soft Comput.*, vol. 37, no. 3, pp. 2849–2863, 2023, doi: 10.32604/iasc.2023.039718.

[29] K. M. Alalayah *et al.*, "Optimal Deep Learning Based Intruder Identification in Industrial Internet of Things Environment".

[30] Y. Kayode Saheed, O. Harazeem Abdulganiyu, and T. Ait Tchakoucht, "A novel hybrid ensemble learning for anomaly detection in industrial sensor networks and SCADA systems for smart city infrastructures," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 5, p. 101532, May 2023, doi: 10.1016/j.jksuci.2023.03.010.

[31] S. H. Rafique, A. Abdallah, N. S. Musa, and T. Murugan, "Machine Learning and Deep Learning Techniques for Internet of Things Network Anomaly Detection—Current Research Trends," *Sensors*, vol. 24, no. 6, p. 1968, Mar. 2024, doi: 10.3390/s24061968.

[32] S. Gunupusala and S. C. Kaila, "Multi-Class Network Anomaly Detection Using Machine Learning Techniques," *Contemp. Math.*, pp. 5–22, June 2024, doi: 10.37256/cm.5220243723.

[33] Z. K. Maseer, Q. K. Kadhim, B. Al-Bander, R. Yusof, and A. Saif, "Meta-analysis and systematic review for anomaly network intrusion detection systems: Detection methods, dataset, validation methodology, and challenges," *IET Netw.*, p. ntw2.12128, June 2024, doi: 10.1049/ntw2.12128.

[34] Md. A. Talukder *et al.*, "Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction," *J. Big Data*, vol. 11, no. 1, p. 33, Feb. 2024, doi: 10.1186/s40537-024-00886-w.

[35] I. Laassar, M. Youssef Hadi, A. Arifullah, H. Remmach, and F. Salam Khan, "Proposed algorithm base optimisation plan for feature selection-based intrusion detection in cloud computing," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 33, no. 2, p. 1140, Feb. 2024, doi: 10.11591/ijeecs.v33.i2.pp1140-1149.

[36] S. A. Khanday, H. Fatima, and N. Rakesh, "A Novel Data Preprocessing Model for Lightweight Sensory IoT Intrusion Detection," *Int. J. Math. Eng. Manag. Sci.*, vol. 9, no. 1, pp. 188–204, Feb. 2024, doi: 10.33889/IJMEMS.2024.9.1.010.

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[37] J. Jose and J. E. Judith, "Unveiling the IoT's dark corners: anomaly detection enhanced by ensemble modelling," *Automatika*, vol. 65, no. 2, pp. 584–596, Apr. 2024, doi: 10.1080/00051144.2024.2304369.

[38] A. K. Dey, G. P. Gupta, and S. P. Sahu, "An Efficient Cyber Assault Detection System using Feature Optimization for IoT-based Cyberspace," *Procedia Comput. Sci.*, vol. 235, pp. 757–766, 2024, doi: 10.1016/j.procs.2024.04.072.

[39] T. Nagaraj and R. K. Channarayappa, "An efficient security framework for intrusion detection and prevention in internet-of-things using machine learning technique," *Int. J. Electr. Comput. Eng. IJECE*, vol. 14, no. 2, p. 2313, Apr. 2024, doi: 10.11591/ijece.v14i2.pp2313-2321.

[40] S. P. R.M. *et al.*, "An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture," *Comput. Commun.*, vol. 160, pp. 139–149, July 2020, doi: 10.1016/j.comcom.2020.05.048.

[41] B. A. N.G. and S. S., "Anomaly detection framework for Internet of things traffic using vector convolutional deep learning approach in fog environment," *Future Gener. Comput. Syst.*, vol. 113, pp. 255–265, Dec. 2020, doi: 10.1016/j.future.2020.07.020.

[42] G. De La Torre Parra, P. Rad, K.-K. R. Choo, and N. Beebe, "Detecting Internet of Things attacks using distributed deep learning," *J. Netw. Comput. Appl.*, vol. 163, p. 102662, Aug. 2020, doi: 10.1016/j.jnca.2020.102662.

[43] K. Albulayhi and F. T. Sheldon, "An Adaptive Deep-Ensemble Anomaly-Based Intrusion Detection System for the Internet of Things," in *2021 IEEE World AI IoT Congress (AIIoT)*, Seattle, WA, USA: IEEE, May 2021, pp. 0187–0196. doi: 10.1109/AIIoT52608.2021.9454168.

[44] A. K. Sahu, S. Sharma, M. Tanveer, and R. Raja, "Internet of Things attack detection using hybrid Deep Learning Model," *Comput. Commun.*, vol. 176, pp. 146–154, Aug. 2021, doi: 10.1016/j.comcom.2021.05.024.

[45] B. Sharma, L. Sharma, C. Lal, and S. Roy, "Anomaly based network intrusion detection for IoT attacks using deep learning technique," *Comput. Electr. Eng.*, vol. 107, p. 108626, Apr. 2023, doi: 10.1016/j.compeleceng.2023.108626.

[46] E. U. H. Qazi, M. H. Faheem, and T. Zia, "HDLNIDS: Hybrid Deep-Learning-Based Network Intrusion Detection System," *Appl. Sci.*, vol. 13, no. 8, p. 4921, Apr. 2023, doi: 10.3390/app13084921.

[47] A. Henry *et al.*, "Composition of Hybrid Deep Learning Model and Feature Optimization for Intrusion Detection System," *Sensors*, vol. 23, no. 2, p. 890, Jan. 2023, doi: 10.3390/s23020890.

[48] D. V. G. Krishnan, S. Kaviarasan, and A. Geetha, "NETWORK INTRUSION DETECTION BASED ON ONE- DIMENSIONAL CNN WITH CHIMP OPTIMIZATION ALGORITHM," . *Vol.*, no. 10, 2023.

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[49] S. Balaji and S. S. Narayanan, "Dynamic distributed generative adversarial network for intrusion detection system over internet of things," *Wirel. Netw.*, vol. 29, no. 5, pp. 1949–1967, July 2023, doi: 10.1007/s11276-022-03182-8.

[50] S. Sadhwani, B. Manibalan, R. Muthalagu, and P. Pawar, "A Lightweight Model for DDoS Attack Detection Using Machine Learning Techniques," *Appl. Sci.*, vol. 13, no. 17, p. 9937, Sept. 2023, doi: 10.3390/app13179937.

[51] V. W. Thirumaran, N. Joseph, and U. Srikanth, "Intrusion detection system in cloud computing by utilizing VTR-HLSTM based on deep learning," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 33, no. 3, p. 1829, Mar. 2024, doi: 10.11591/ijeecs.v33.i3.pp1829-1842.

[52] W. A. H. M. Ghanem and A. Jantan, "Training a Neural Network for Cyberattack Classification Applications Using Hybridization of an Artificial Bee Colony and Monarch Butterfly Optimization," *Neural Process. Lett.*, vol. 51, no. 1, pp. 905–946, Feb. 2020, doi: 10.1007/s11063-019-10120-x.

[53] M. A. Rahman, A. T. Asyhari, O. W. Wen, H. Ajra, Y. Ahmed, and F. Anwar, "Effective combining of feature selection techniques for machine learning-enabled IoT intrusion detection," *Multimed. Tools Appl.*, vol. 80, no. 20, pp. 31381–31399, Aug. 2021, doi: 10.1007/s11042-021-10567-y.

[54] H. Q. Gheni and W. L. Al-Yaseen, "Using Ensemble Techniques Based on Machine and Deep Learning for Solving Intrusion Detection Problems: A Survey," *Karbala Int. J. Mod. Sci.*, vol. 9, no. 1, Jan. 2023, doi: 10.33640/2405-609X.3277.

[55] R. Alkanhel *et al.*, "Hybrid Grey Wolf and Dipper Throated Optimization in Network Intrusion Detection Systems," *Comput. Mater. Contin.*, vol. 74, no. 2, pp. 2695–2709, 2023, doi: 10.32604/cmc.2023.033153.

[56] G. G. Gebremariam, J. Panda, and S. Indu, "Design of advanced intrusion detection systems based on hybrid machine learning techniques in hierarchically wireless sensor networks," *Connect. Sci.*, vol. 35, no. 1, p. 2246703, Dec. 2023, doi: 10.1080/09540091.2023.2246703.

[57] L. K. Vashishtha, A. P. Singh, and K. Chatterjee, "HIDM: A Hybrid Intrusion Detection Model for Cloud Based Systems," *Wirel. Pers. Commun.*, vol. 128, no. 4, pp. 2637–2666, Feb. 2023, doi: 10.1007/s11277-022-10063-y.

[58] A. T. Azar, E. Shehab, A. M. Mattar, I. A. Hameed, and S. A. Elsaid, "Deep Learning Based Hybrid Intrusion Detection Systems to Protect Satellite Networks," *J. Netw. Syst. Manag.*, vol. 31, no. 4, p. 82, Oct. 2023, doi: 10.1007/s10922-023-09767-8.

[59] L. Oja and Dr. P. Ranjana, "An Intrusion Detection System Using a Machine Learning Approach in IOT-based Smart Cities," *J. Internet Serv. Inf. Secur.*, vol. 13, no. 1, pp. 11–21, Jan. 2023, doi: 10.58346/JISIS.2023.I1.002.

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[60] H. Attou *et al.*, "Towards an Intelligent Intrusion Detection System to Detect Malicious Activities in Cloud Computing," *Appl. Sci.*, vol. 13, no. 17, p. 9588, Aug. 2023, doi: 10.3390/app13179588.

[61] M. Ozkan-Okay, R. Samet, Ö. Aslan, S. Kosunalp, T. Iliev, and I. Stoyanov, "A Novel Feature Selection Approach to Classify Intrusion Attacks in Network Communications," *Appl. Sci.*, vol. 13, no. 19, p. 11067, Oct. 2023, doi: 10.3390/app131911067.

[62] S. Vanitha and P. Balasubramanie, "Improved Ant Colony Optimization and Machine Learning Based Ensemble Intrusion Detection Model," *Intell. Autom. Soft Comput.*, vol. 36, no. 1, pp. 849–864, 2023, doi: 10.32604/iasc.2023.032324.

[63] H. Bakır and Ö. Ceviz, "Empirical Enhancement of Intrusion Detection Systems: A Comprehensive Approach with Genetic Algorithm-based Hyperparameter Tuning and Hybrid Feature Selection," *Arab. J. Sci. Eng.*, vol. 49, no. 9, pp. 13025–13043, Sept. 2024, doi: 10.1007/s13369-024-08949-z.

[64] E. M. Maseno and Z. Wang, "Hybrid wrapper feature selection method based on genetic algorithm and extreme learning machine for intrusion detection," *J. Big Data*, vol. 11, no. 1, p. 24, Feb. 2024, doi: 10.1186/s40537-024-00887-9.

[65] T. S. Adekunle *et al.*, "An Intrusion System for Internet of Things Security Breaches Using Machine Learning Techniques," *Artif. Intell. Appl.*, vol. 2, no. 3, pp. 188–194, Mar. 2024, doi: 10.47852/bonviewAIA42021780.

[66] B. Nawaal, U. Haider, I. U. Khan, and M. Fayaz, "Signature-Based Intrusion Detection System for IoT," in *Cyber Security for Next-Generation Computing Technologies*, 1st ed., Boca Raton: CRC Press, 2023, pp. 141–158. doi: 10.1201/9781003404361-8.

[67] H. Satilmiş, S. Akleylek, and Z. Y. Tok, "A Systematic Literature Review on Host-Based Intrusion Detection Systems," *IEEE Access*, vol. 12, pp. 27237–27266, 2024, doi: 10.1109/ACCESS.2024.3367004.

[68] A. Efe and İ. N. Abaci, "Comparison of the Host Based Intrusion Detection Systems and Network Based Intrusion Detection Systems," *Celal Bayar Üniversitesi Fen Bilim. Derg.*, vol. 18, no. 1, pp. 23–32, Mar. 2022, doi: 10.18466/cbayarfbe.832533.

[69] A. Magalhaes and H. Barbosa, "Intrusion Detection Security Techniques in Cloud- Based Networks," *Journal For Innovative Development in Pharmaceutical and Technical Science (JIDPTS)*, vol. 7, no. 5, 2024, doi: https://doi.org/10.1016/j.asej.2023.102211.

[70] Sofiritari Ibikoroma Amgbara, Chukwuebuka Akwiwu-Uzoma, and Ola David, "Exploring lightweight machine learning models for personal internet of things (IOT) device security," *World J. Adv. Res. Rev.*, vol. 24, no. 2, pp. 1116–1138, Nov. 2024, doi: 10.30574/wjarr.2024.24.2.3449.

[71] L. Xing, S. Li, Q. Zhang, H. Wu, H. Ma, and X. Zhang, "A survey on social network's anomalous behavior detection," *Complex Intell. Syst.*, vol. 10, no. 4, pp. 5917–5932, Aug. 2024, doi: 10.1007/s40747-024-01446-8.

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[72] J. Li, M. S. Othman, H. Chen, and L. M. Yusuf, "Optimizing IoT intrusion detection system: feature selection versus feature extraction in machine learning," *J. Big Data*, vol. 11, no. 1, p. 36, Feb. 2024, doi: 10.1186/s40537-024-00892-y.

[73] K. N. Qureshi, S. S. Rana, A. Ahmed, and G. Jeon, "A novel and secure attacks detection framework for smart cities industrial internet of things," *Sustain. Cities Soc.*, vol. 61, p. 102343, Oct. 2020, doi: 10.1016/j.scs.2020.102343.

[74] M. Roopak, G. Y. Tian, and J. Chambers, "Multi-objective-based feature selection for DDoS attack detection in IoT networks," *IET Netw.*, vol. 9, no. 3, pp. 120–127, May 2020, doi: 10.1049/iet-net.2018.5206.

[75] W. A. H. M. Ghanem *et al.*, "Metaheuristic Based IDS Using Multi-objective Wrapper Feature Selection and Neural Network Classification," in *Advances in Cyber Security*, vol. 1347, M. Anbar, N. Abdullah, and S. Manickam, Eds., Singapore: Springer Singapore, 2021, pp. 384–401. Accessed: Apr. 26, 2025. [Online]. Available: https://link.springer.com/10.1007/978-981-33-6835-4_26

[76] Z. Sun, G. An, Y. Yang, and Y. Liu, "Optimized machine learning enabled intrusion detection 2 system for internet of medical things," *Frankl. Open*, vol. 6, p. 100056, Mar. 2024, doi: 10.1016/j.fraope.2023.100056.

[77] M. M. Khayyat, "Improved bacterial foraging optimization with deep learning based anomaly detection in smart cities," *Alex. Eng. J.*, vol. 75, pp. 407–417, July 2023, doi: 10.1016/j.aej.2023.05.082.

[78] M. Aljebreen *et al.*, "Binary Chimp Optimization Algorithm with ML Based Intrusion Detection for Secure IoT-Assisted Wireless Sensor Networks," *Sensors*, vol. 23, no. 8, p. 4073, Apr. 2023, doi: 10.3390/s23084073.

[79] Y. K. Saheed and S. Misra, "A voting gray wolf optimizer-based ensemble learning models for intrusion detection in the Internet of Things," *Int. J. Inf. Secur.*, vol. 23, no. 3, pp. 1557–1581, June 2024, doi: 10.1007/s10207-023-00803-x.

[80] D. Jayalatchumy, R. Ramalingam, A. Balakrishnan, M. Safran, and S. Alfarhood, "Improved Crow Search-Based Feature Selection and Ensemble Learning for IoT Intrusion Detection," *IEEE Access*, vol. 12, pp. 33218–33235, 2024, doi: 10.1109/ACCESS.2024.3372859.

[81] P. Mishra, I. Verma, and S. Gupta, "KVMInspector: KVM Based introspection approach to detect malware in cloud environment," *J. Inf. Secur. Appl.*, vol. 51, p. 102460, Apr. 2020, doi: 10.1016/j.jisa.2020.102460.

[82] C. Asst. Prof. Chandigarh University, Mohali, India., S. Midha, G. Kaur, and C. Asst. Prof. Manav Rachna University, Faridabad, India., "Svm Implementation for Ddos Attacks in Software Defined Networks," *Int. J. Innov. Technol. Explor. Eng.*, vol. 10, no. 1, pp. 205–212, Nov. 2020, doi: 10.35940/ijitee.A8166.1110120.

Received: August 09, 2025

Volume 38 No. 10s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[83] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, p. 20, Dec. 2019, doi: 10.1186/s42400-019-0038-7.

[84] M. Ozkan-Okay, R. Samet, and O. Aslan, "A New Feature Selection Approach and Classification Technique for Current Intrusion Detection System," in *2021 6th International Conference on Computer Science and Engineering (UBMK)*, Ankara, Turkey: IEEE, Sept. 2021, pp. 227–232. doi: 10.1109/UBMK52708.2021.9559011.

[85] W. A. H. M. Ghanem *et al.*, "Metaheuristic Based IDS Using Multi-objective Wrapper Feature Selection and Neural Network Classification," in *Advances in Cyber Security*, vol. 1347, M. Anbar, N. Abdullah, and S. Manickam, Eds., in Communications in Computer and Information Science, vol. 1347. , Singapore: Springer Singapore, 2021, pp. 384–401. doi: 10.1007/978-981-33-6835-4_26.

[86] K. A. Alissa *et al.*, "Crystal Structure Optimization with Deep-Autoencoder-Based Intrusion Detection for Secure Internet of Drones Environment," *Drones*, vol. 6, no. 10, p. 297, Oct. 2022, doi: 10.3390/drones6100297.

[87] M. Abdullahi *et al.*, "Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review," *Electronics*, vol. 11, no. 2, p. 198, Jan. 2022, doi: 10.3390/electronics11020198.

[88] Kurniabudi, .

[89] Z. Azam, Md. M. Islam, and M. N. Huda, "Comparative Analysis of Intrusion Detection Systems and Machine Learning-Based Model Analysis Through Decision Tree," *IEEE Access*, vol. 11, pp. 80348–80391, 2023, doi: 10.1109/ACCESS.2023.3296444.

[90] M. A. Khatun, S. F. Memon, C. Eising, and L. L. Dhirani, "Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation," *IEEE Access*, vol. 11, pp. 145869–145896, 2023, doi: 10.1109/ACCESS.2023.3346320.

[91] A. R. Abdulla and N. G. M. Jameel, "A Review on IoT Intrusion Detection Systems Using Supervised Machine Learning: Techniques, Datasets, and Algorithms," *UHD J. Sci. Technol.*, vol. 7, no. 1, pp. 53–65, Mar. 2023, doi: 10.21928/uhdjst.v7n1y2023.pp53-65.

[92] M. N. Alatawi *et al.*, "Cyber Security against Intrusion Detection Using Ensemble-Based Approaches," *Secur. Commun. Netw.*, vol. 2023, pp. 1–7, Feb. 2023, doi: 10.1155/2023/8048311.

[93] C. Hazman, A. Guezzaz, S. Benkirane, and M. Azrour, "lIDS-SIoEL: intrusion detection framework for IoT-based smart environments security using ensemble learning," *Clust. Comput.*, vol. 26, no. 6, pp. 4069–4083, Dec. 2023, doi: 10.1007/s10586-022-03810-0.

[94] J. A and M. A. E. A, "A Novel Paradigm for IoT Security: ResNet-GRU Model Revolutionizes Botnet Attack Detection," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 12, 2023, doi: 10.14569/IJACSA.2023.0141231.

Received: August 09, 2025

Volume 38 No. 10s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[95] W. Gou, H. Zhang, and R. Zhang, "Multi-Classification and Tree-Based Ensemble Network for the Intrusion Detection System in the Internet of Vehicles," *Sensors*, vol. 23, no. 21, p. 8788, Oct. 2023, doi: 10.3390/s23218788.

[96] K. Kethineni and P. Gera, "Iot-Based Privacy-Preserving Anomaly Detection Model for Smart Agriculture," *Systems*, vol. 11, no. 6, p. 304, June 2023, doi: 10.3390/systems11060304.

[97] F. Y. Assiri and M. Ragab, "Optimal Deep-Learning-Based Cyberattack Detection in a Blockchain-Assisted IoT Environment," *Mathematics*, vol. 11, no. 19, p. 4080, Sept. 2023, doi: 10.3390/math11194080.

[98] Y. K. Saheed, T. O. Kehinde, M. Ayobami Raji, and U. A. Baba, "Feature selection in intrusion detection systems: a new hybrid fusion of Bat algorithm and Residue Number System," *J. Inf. Telecommun.*, vol. 8, no. 2, pp. 189–207, Apr. 2024, doi: 10.1080/24751839.2023.2272484.

[99] J. Li, M. S. Othman, H. Chen, and L. M. Yusuf, "Optimizing IoT intrusion detection system: feature selection versus feature extraction in machine learning," *J. Big Data*, vol. 11, no. 1, p. 36, Feb. 2024, doi: 10.1186/s40537-024-00892-y.

[100] A. Almotairi, S. Atawneh, O. A. Khashan, and N. M. Khafajah, "Enhancing intrusion detection in IoT networks using machine learning-based feature selection and ensemble models," *Syst. Sci. Control Eng.*, vol. 12, no. 1, p. 2321381, Dec. 2024, doi: 10.1080/21642583.2024.2321381.

Received: August 09, 2025