Machine Learning and Deep Learning for Next-Generation Intrusion Detection Systems: A Systematic Review

Neha Gosavi[1], Dhanashree Jadhav [2], Pravin Jadhav [3], Shweta Jadhav[4], and Prof. Ganesh Rathod[5]
[1,2,3,4]*Department of CSE, Dr. D. Y. Patil Pratisthan's College of Engineering, Kolhapur, India*
[5]*Dean Accreditation, Department of CSE, Dr. D. Y. Patil Pratisthan's College of Engineering, Kolhapur, India*

***Abstract*—Intrusion Detection Systems (IDS) play a critical role in safeguarding modern digital infrastructures against rapidly evolving cyber threats. As networks expand through cloud computing, virtualization, mobile devices, and billions of Internet of Things (IoT) components, traditional security mechanisms such as firewalls and signature-based IDS have become increasingly inadequate. These conventional systems rely on predefined rules and known attack signatures, limiting their ability to detect emerging, zero-day, polymorphic, and AI-driven attacks. To address these challenges, Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) techniques have transformed IDS by enabling automated feature extraction, adaptive learning, behavior modeling, and high-accuracy threat classification. AI-powered IDS can analyze vast volumes of network traffic in real time, identify subtle anomalies, reduce false positives, and learn new attack strategies with minimal human interven- tion. Recent advancements—such as CNNs for spatial traffic analysis, LSTMs for temporal sequence modeling, Autoencoders for anomaly detection, and hybrid CNN–LSTM models—have significantly improved detection performance across diverse environments. At the same time, IoT ecosystems introduce unique constraints, including lightweight communication proto- cols, resource-limited devices, and heterogeneous traffic patterns, demanding efficient and scalable IDS solutions. Datasets such as UNSW-NB15, CIC-IDS2017, and BoT-IoT have further acceler- ated research by providing realistic benchmarks for evaluating AI-driven models. This review paper provides a comprehensive analysis of mod- ern IDS architectures, ML/DL approaches, IoT-specific detection challenges, evaluation metrics, and trends such as federated learning, explainable AI, and blockchain-based IDS. The pa- per highlights key limitations in current systems and outlines future directions toward building intelligent, autonomous, and resilient intrusion detection frameworks capable of securing next- generation networks.**

I. INTRODUCTION

The exponential growth of digital connectivity has trans- formed modern computing environments. Cloud platforms, virtualized infrastructures, mobile systems, and billions of Internets of Things (IoT) devices now interact in large-scale, heterogeneous networks. While this digital expansion has enabled new services and business models, it has also intro- duced an unprecedented rise in cyberattacks. Networks are constantly targeted by Distributed Denial of Service (DDoS), ransomware, malware propagation, brute-force attacks, phishing campaigns, botnets, and zero-day exploits. Traditional cybersecurity mechanisms such as firewalls, access-control lists, and signature-based detection systems are insufficient to defend against sophisticated and evolving threats.

Intrusion Detection Systems (IDS) were introduced to identify malicious activity by analyzing network traffic or host behavior. Early IDS models relied heavily on rule-based and signature-based detection, which perform well for identifying known attack patterns. However, attackers frequently modify payloads, use encrypted channels, generate polymorphic malware, and exploit vulnerabilities unknown to the security community. As a result, static IDS approaches fail to achieve high detection accuracy for new or zero-day attack scenarios [1].

To address these limitations, researchers have turned toward Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL)-powered IDS. These techniques learn patterns directly from data, enabling automated feature extraction, anomaly detection, and more robust classification of malicious activity. AI-

powered IDS can detect subtle variations in traf- fic, identify unknown threats, reduce false-positive rates, and operate efficiently in real time. For example, ML-based systems can model statistical behaviors while DL-based systems (CNNs, LSTMs, autoencoders) can extract complex spatial and temporal patterns from raw traffic [2].

Furthermore, IoT ecosystems introduce additional security challenges. IoT devices operate with low power, limited memory, lightweight communication protocols, and high heterogeneity. These constraints make it difficult to deploy traditional IDS, requiring lightweight and adaptive AI models that can function at the edge, fog layer, or gateway devices. Attackers often exploit this heterogeneity by launching botnet attacks (e.g., Mirai), injecting malicious firmware, or hijacking devices to perform coordinated attacks [3].

In this paper, we present a comprehensive review of AI-powered IDS. The major contributions of this review include:

- A detailed analysis of classical, ML, and DL-based IDS models.
- A comparative discussion of datasets commonly used for IDS benchmarking .Expanded diagrams illustrating system architecture, data pipelines, and detection workflows.
- An evaluation overview explaining metrics used to measure IDS effectiveness.
- A dedicated section on IoT intrusion detection challenges and lightweight model design.
- A forward-looking discussion on emerging directions including blockchain, XAI, federated learning, and edge- based detection.

II. LITERATURE REVIEW

Research in Intrusion Detection Systems (IDS) has evolved significantly over the past decade, transitioning from traditional signature-based mechanisms to intelligent AI-driven detection engines. This section reviews influential studies relevant to IDS development, IoT security, feature engineering, and deep learning approaches.

A. Classical and Signature-Based IDS

Early intrusion detection mechanisms focused on static rule matching, where predefined patterns were used to detect threats. Although widely used in commercial tools such as Snort and Suricata, these approaches require continuous up- dates and fail to detect unknown or obfuscated attacks. critically reviewed these systems and emphasized that traditional IDS cannot meet the demands of modern dynamic networks, especially in IoT ecosystems where device behavior is highly variable.

B. Machine Learning-Based IDS

The shift toward Machine Learning (ML) began when researchers identified the need for adaptive detection models capable of learning from traffic patterns. Proposed a novel feature-selection technique tailored for IoT networks, demon- starting that lightweight ML models can achieve high detection accuracy with reduced computation. Their work high-lighted the importance of dimensionality reduction in resource- constrained environments.

Similarly, conducted extensive feature analysis for ML-based IoT IDS. Their findings indicated that features such as packet size, inter-arrival time, flow duration, and TCP flag patterns significantly influence detection performance. These studies collectively suggest that ML-based IDS performance largely depends on high-quality feature engineering.

C. Deep Learning Techniques in IDS

Deep Learning (DL) has become a trending direction in IDS research due to its ability to extract hierarchical representations from raw or partially processed traffic. emphasized the need for explainable DL models, noting that security analysts re- quire transparency regarding model decisions. Their universal feature-set approach integrates DL with interpretability mech- anisms, making real-world deployments more feasible. They also argued that DL models are particularly effective in detecting low-frequency or stealthy attacks that are often missed by classical ML approaches.

D. IDS for IoT and Resource-Constrained Environments

IoT networks introduce new pathways for intrusion due to limited hardware resources, low-power communication protocols, and diverse device behaviors. Paper [4] explored energy-efficient detection mechanisms using compressive sensing and

lightweight models. Their findings demon- started that traditional IDS are too heavy for IoT deployments and that optimized feature compression is crucial.

The Author in [5] designed an intelligent smart-environment IDS integrating sensor-level anomaly detection with cloud analytics. Their architecture showcased the viability of hybrid approaches combining local lightweight detection with centralized DL models. The BoT-IoT dataset introduced by [6] has become a benchmark for IoT IDS research. Their intrusion detection framework demonstrated that DL models outperform ML baselines in detecting botnets, DDoS, and reconnaissance attacks.

E. Recent Trends and Research Gaps

The collective literature identifies several emerging trends:

- Integration of explainable AI (XAI) into IDS decision- making.
- Use of federated learning for privacy-preserving, multi- site IDS training.
- Adoption of blockchain for secure logging and tamper- proof audit trails.
- Increasing focus on IoT-specific datasets and lightweight edge-based IDS deployment.

Despite remarkable progress, significant research gaps re- main. There is a lack of standardized, large-scale IoT datasets. Many DL models are "black boxes," making security analysts reluctant to trust them. Furthermore, adversarial attacks pose threats to ML/DL-based IDS, and real-time deployment challenges persist in high-speed networks.

This literature review highlights the evolution of IDS technologies, identifies key contributions from recent works, and sets the foundation for the architectural and technical discussions in subsequent sections Research in Intrusion Detection Systems (IDS) has evolved significantly over the past decade, transitioning from traditional signature-based mechanisms to intelligent AI-driven detection engines. This section reviews influential studies relevant to IDS development, IoT security, feature engineering, and deep learning approaches.

III. INTRUSION DETECTION SYSTEM (IDS) ARCHITECTURE

An Intrusion Detection System (IDS) is typically composed of multiple functional layers that work together to collect, pro- cess, analyze, and classify network or system behavior. Mod- ern IDS architectures incorporate AI, Machine Learning, and Deep Learning to enhance detection accuracy and minimize false alarms. This section provides an expanded architectural overview and presents a detailed diagram representing the end- to-end workflow of an AI-driven IDS. Traditional IDS architecture largely relied on signature matching, logging, and rule-based scanning. These architectures have evolved into multi-stage intelligent systems that merge statistical modeling, adaptive learning, and automated decision-making. Fig. 1 illustrates a modern IDS architecture with enhanced preprocessing, AI detection modules, and alerting layers. Each component is described below.

A. Data Collection Layer

The first stage of an IDS architecture is responsible for gathering raw traffic or system-level data. Sources may include:

- Network Traffic (Packet captures, flow records, Net- Flow/IPFIX)
- Host-Level Logs (authentication logs, system calls, kernel logs)
- IoT telemetry (sensor values, device communication pat- terns)

This layer must efficiently manage continuous data streams generated by complex and high-speed networks.

B. Preprocessing and Normalization

Raw data is often noisy, unstructured, or incomplete. This stage performs cleaning, encoding, timestamp alignment, packet parsing, and conversion of flow-based attributes into structured formats. In IoT, additional transformations such as protocol normalization (MQTT, CoAP) are required. Effective preprocessing significantly influences ML/DL model performance

C. Feature Extraction and Selection

Feature engineering translates packet-level patterns into numerical or categorical features for AI models. Common features include header fields, flag statistics, flow duration, byte count, and temporal correlations. Advanced systems integrate automatic feature extraction (e.g., CNN feature maps, LSTM hidden

states). Feature selection reduces dimensionality and improves computational efficiency.

D. AI-Based Detection Engine

The detection engine is the core of the IDS. Classical ML models (SVM, RF, NB) rely on statistical relationships, while DL models (CNN, LSTM, Autoencoders) capture complex behavioral patterns. Hybrid models combine supervised and unsupervised learning to improve zero-day detection. This layer determines whether an event is normal or malicious.

E. Alerting and Response System

Upon identifying malicious activity, the IDS generates alerts or triggers automated defenses. Advanced architectures inte- grate with:

- SIEM systems
- Firewalls / IPS for mitigation
- Forensic analysis tools

The effectiveness of an IDS depends on its ability to minimize false positives while providing actionable insights in real

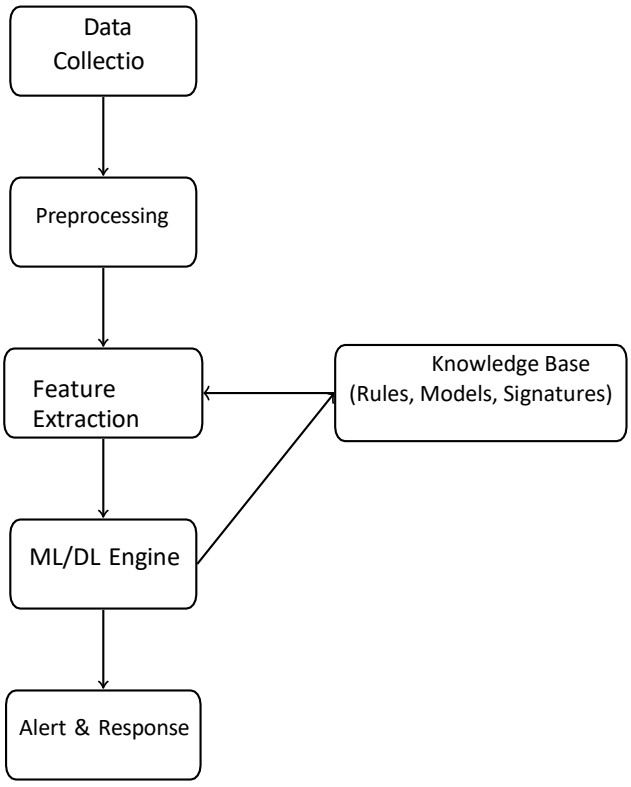

Fig. 1. Expanded Architecture of an AI-Powered Intrusion Detection System

F. Enhanced Architecture Diagram

This enhanced architecture provides a comprehensive view of modern IDS operations, highlighting the interaction be- tween AI models, real-time monitoring, and adaptive learning components. The integration of a knowledge base enables continuous model refinement, allowing the IDS to improve performance over time.

IV.IDS Workflow Diagram

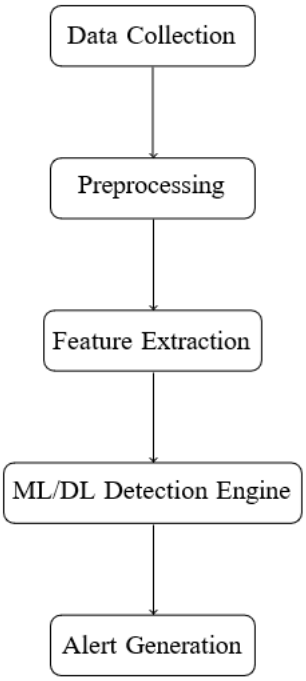

Fig. 2. General IDS Workflow

The workflow illustrated in Fig. 2 represents the key stages involved in the operation of a modern Intrusion Detection System (IDS). The process begins with Data Collection, where raw network packets, system logs, and communication flows are gathered from routers, servers, IoT devices, firewalls, and endpoints. These heterogeneous data sources ensure that the IDS has comprehensive visibility across the network.

The collected data is sent to the Preprocessing stage, which performs crucial tasks such as noise removal, packet filtering, normalization, encoding of categorical values, and alignment of timestamps. This step ensures that the resulting dataset is clean, consistent, and ready for analysis.

Next, the processed data enters the Feature Extraction component, where meaningful attributes such as flow du- ration, packet count, byte distribution, protocol type, inter- arrival times, and flag statistics are derived. These features capture behavioral and statistical characteristics essential for identifying malicious patterns.

The extracted features are then fed into the Machine Learning / Deep Learning Detection Engine. This stage involves classification, clustering, or anomaly detection using models such as Random Forest, Support Vector Machines, Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, or Autoencoders. The detection engine determines whether each flow or event is normal or suspicious.

Finally, the Alert Generation module triggers warnings, logs detected anomalies, and communicates alerts to security analysts or automated response systems such as Intrusion Prevention Systems (IPS) or SIEM dashboards. This helps in initiating timely responses and mitigating potential threats in real time. This structured workflow ensures that IDS can analyze traf- fic efficiently, detect threats accurately, and support automated or human-driven security responses.

V. POPULAR DATASETS FOR IDS EVALUATION

Datasets play a critical role in developing, training, and benchmarking Intrusion Detection Systems (IDS). An IDS can only perform effectively if the underlying data used for training represents real-world traffic patterns, diverse attack families, and legitimate background traffic. Over the years, numerous datasets have been developed for different envi- ronments such as traditional networks, IoT networks, cloud environments, and industrial systems. This section provides an extensive review of the most widely used datasets, their characteristics, limitations, and usage trends in IDS research.

A. Importance of Benchmark Datasets

Benchmark datasets are essential for:

- Training machine learning and deep learning models.
- Comparing the performance of different IDS techniques.
- Evaluating detection accuracy, false alarms, and scalability.
- Identifying model weaknesses, such as bias or overfitting.

An effective IDS dataset must include real-world traffic, diverse attacks, and minimal redundancy. However, modern encrypted communication and evolving threats pose challenges in dataset generation.

B. Classical IDS Datasets

Early IDS datasets were widely used for benchmarking but have limitations such as redundancy and unrealistic traffic. Despite this, they remain a reference point in IDS research.

- KDD'99 Dataset: One of the earliest benchmark IDS datasets developed for the DARPA98 project. It includes four major attack categories: DoS, U2R, R2L, and Probe. However, it suffers from duplication and outdated attack patterns.
- NSL-KDD Dataset: Improved version of KDD'99 with- out redundant instances. It is widely used for evaluating machine learning-based IDS but still lacks modern attack vectors.

C. Modern Realistic Datasets

Modern datasets capture more realistic, diverse, and large- scale network traffic. They better represent modern attacks such as botnets, brute-force attacks, DDoS floods, ransomware, and data exfiltration.

- UNSW-NB15: Developed using the IXIA traffic generator, this dataset includes real modern attack behaviors such as exploits, backdoors, fuzzes, shellcode, and generic attacks. It contains 49 features and is widely used for ML/DL-based IDS research.
- CIC-IDS 2017 & CIC-IDS 2018: Created by the Canadian Institute for Cybersecurity (CIC), these datasets contain full packet captures (PCAP), flows, logs, and labeled attacks. The attacks include botnet, DDoS, brute-force, web attacks, infiltration, and SQL injection. They are considered one of the most realistic datasets for large-scale IDS evaluation.
- CIC-DDoS 2019: A specialized dataset for DDoS evaluation, containing over 80 attack variations. It is valuable for evaluating detection models in cloud and IoT environments experiencing high-

volume floods.

D. IoT-Specific Datasets

IoT datasets address the challenges of constrained devices, heterogeneous protocols, and unique communication patterns.

- BoT-IoT Dataset: A comprehensive IoT-focused dataset containing DDoS, DoS, reconnaissance, and information-theft attacks. It is widely used in AI-based IoT intrusion detection studies [2].
- IoT-23 Dataset: Developed by Stratosphere Labs, it includes benign IoT traffic and numerous malware families such as Mirai, Torii, and Gafgyt. It provides PCAPs and labeled attack sequences.
- MQTT-IoT Dataset: Focuses on IoT systems using the MQTT protocol. It includes authentication attacks, flooding, and spoofing in lightweight IoT communication.

TABLE I. COMPARISON OF COMMON IDS DATASETS

Dataset	Year	Traffic Type	Attacks Included
KDD'99	1999	Simulated	DoS, U2R, R2L,Probe
NSL-KDD	2009	Simulated	Improved KDD Version
UNSW-NB15	2015	Synthetic + Real	Exploits, Backdoor, Shellcode
CIC-IDS2017	2017	Realistic	Botnet, BF, DDoS, SQLi
BoT-IoT	2018	IoT Traffic	DDoS, Recon, Info Theft
IoT-23	2020	Real IoT	Malware, Mirai Variants

If your figure has E. Dataset Limitations

Despite improvements, current datasets still face limitations:

- Lack of encrypted traffic visibility due to TLS.
- Limited representation of emerging attacks (e.g., AI- powered malware).
- Synthetic datasets may not reflect real-world device diversity.
- Large datasets require heavy preprocessing and computational resources.
- Trends in Future Dataset Development
- Future IDS datasets are expected to include:
- Cloud-native microservice traffic.
- Secure encrypted flow metadata.
- Federated learning–ready distributed datasets.
- Adversarial attack scenarios to test model robustness.

These improvements will enhance the reliability of IDS evaluation in practical environments.

VI. TYPES OF INTRUSION DETECTION SYSTEMS

IDS solutions are broadly classified based on deployment, detection methods, and behavioral modeling.

A. Based on Deployment

- Network-based IDS (NIDS): Monitors network packets and detects malicious traffic patterns.
- Host-based IDS (HIDS): Monitors system logs, file integrity, and operating system activities.

B. Based on Detection Technique

- Signature-based Detection: Matches patterns of known attacks.
- Anomaly-based Detection: Detects deviations from normal behavior using AI
- Hybrid IDS: Combines both approaches to maximize accuracy.

B. Deep Learning Approaches

Deep Learning techniques automatically extract features from raw network traffic:

- Convolutional Neural Networks (CNN)
- Recurrent Neural Networks (RNN) and LSTMs
- Autoencoders for anomaly detection
- Hybrid CNN–LSTM models for sequential patterns.
- DL-based IDS outperform classical ML but require more computational power.

VIII. CHALLENGES

Despite significant advancements in AI-powered Intrusion Detection Systems (IDS), several critical challenges continue to limit their practical deployment and effectiveness. These challenges arise due to evolving cyber threats, data limitations, computational constraints, and the increasingly decentralized nature of modern computing environments such as IoT, cloud, and edge systems.

A. High False Positives in Anomaly-Based IDS

Anomaly detection models often classify normal but un- usual user behavior as malicious. These false alarms overload security teams, reduce trust in IDS, and increase operational costs. Designing models that balance sensitivity and specificity remains a key challenge.

B. Lack of High-Quality Labeled Datasets

Real-world network traffic is diverse, dynamic, and often unlabeled due to privacy concerns. Existing datasets like KDD'99 or NSL-KDD are outdated, while newer datasets such as CIC-IDS and BoT-IoT do not fully represent all modern attacks. This limits the generalization capability of ML/DL models.

C. Difficulty Inspecting Encrypted Traffic

With increasing adoption of TLS/SSL and end-to-end en- cryption, IDS lose visibility into packet payloads. Traditional header-based analysis is insufficient for detecting sophisticated attacks, making encrypted traffic inspection a major challenge.

D. Computational Constraints in IoT Devices

IoT devices have limited processing power, memory, and battery life. Heavy ML/DL models cannot run on-device, forcing reliance on cloud or edge computing. This introduces latency, bandwidth usage, and potential privacy risks.

E. Vulnerability to Adversarial Attacks

AI models can be manipulated using adversarial inputs that appear normal but are subtly modified to evade detection. Attackers can poison training data or craft adversarial packets, compromising IDS accuracy.

F. Scalability Issues in Large Networks

Enterprise and cloud environments generate terabytes of network traffic daily. Scaling IDS to operate efficiently in real- time on distributed systems is challenging, especially when using resource-intensive deep learning models.

G. Concept Drift in Network Behavior

Network traffic evolves continuously due to software up- dates, new applications, and changes in user behavior. Models trained on static datasets fail to adapt and degrade over time. Continual learning is needed but remains difficult to implement.

H. High Storage and Processing Demands

Storing raw traffic, flow records, and log data for long-term analysis requires large storage systems. Processing these logs in real-time for threat detection increases infrastructure overhead.

I. Privacy and Compliance Issues

Collecting sensitive network data may violate regulations such as GDPR, HIPAA, and industry compliance standards. ML/DL-based IDS must ensure user privacy while still enabling effective threat detection.

Collectively, these challenges highlight the need for advanced, adaptable, and explainable IDS architectures capable of operating efficiently across diverse environments.

IX. FUTURE DIRECTIONS

As cyber threats grow more sophisticated, Intrusion Detection Systems (IDS) must evolve into intelligent, autonomous, and scalable protection mechanisms supported by emerging technologies. Explainable Artificial Intelligence (XAI) will enhance transparency by helping analysts understand why deep learning models flag malicious traffic, thereby improving trust and forensic analysis. Privacy-preserving approaches such as federated learning will enable collaborative model training across organizations without sharing raw data, while blockchain-based IDS will ensure secure, tamper-proof logging of events and threat intelligence. To address IoT constraints, lightweight Edge-AI IDS models will provide real-time detection near the data source, reducing latency and bandwidth usage. Future IDS systems will also incorporate self-learning and reinforcement learning capabilities to autonomously adapt to new and evolving threats, strengthening zero-day attack detection. Multi-modal and hybrid detection models will integrate network flows, logs, IoT data, and behavioral patterns to create more robust frameworks, while adversarial robustness techniques will protect IDS models from manipulation. With cloud adoption increasing, IDS must support cloud-native and microservices-based security for containerized and distributed workloads. Standardized, large-scale datasets reflecting modern attack patterns and encrypted traffic will be essential for improving benchmarking and model reliability. Finally, collaborative threat intelligence sharing using

blockchain, secure APIs, and federated analytics will significantly enhance IDS responsiveness.
Overall, next-generation IDS solutions will be more autonomous, interpretable, scalable, and seamlessly integrated with modern computing technologies to defend complex digital ecosystems against advanced cyber threats.

X.CONCLUSION

Intrusion Detection Systems (IDS) are critical components of modern cybersecurity, especially as cyberattacks become increasingly intelligent, automated, and difficult to detect. This review provided an in-depth analysis of AI-powered IDS, covering machine learning methods, deep learning architectures, IoT-focused intrusion detection, dataset limitations, and emerging research trends. Traditional signature-based IDS, while effective for known threats, fail to detect novel attacks, polymorphic malware, and zero-day vulnerabilities. Machine Learning-based IDS improved adaptability through statistical modelling and feature-driven classification but still require manual feature engineering and face challenges with high-volume, complex network data. Deep learning models such as CNNs, LSTMs, autoencoders, and hybrids deliver superior performance by enabling automatic feature extraction, temporal behavior learning, and robust anomaly detection.

The review highlighted the unique challenges of IoT environments, including limited device resources, heterogeneous protocols, and heightened exposure to botnets and distributed attacks. Lightweight AI models, edge computing, and dataset standardization are essential for reliable IoT intrusion detection. Despite major advancements, IDS research continues to face issues such as poor-quality datasets, encrypted traffic analysis, adversarial vulnerabilities, scalability constraints, and high false-positive rates. Future IDS development will be shaped by technologies like Explainable AI, blockchain-based logging, federated learning, autonomous learning systems, and cloud-native microservice architectures. These innovations will help build transparent, resilient, and adaptive IDS capable of protecting modern digital ecosystems from evolving cyber threats.

REFERENCES

[1] A. Khraisat and A. Alazab, “A critical review of intrusion detection systems in the internet of things,” Cybersecurity, vol. 4, pp. 1–27, 2021.
[2] S. Alosaimi and S. M. Almutairi, “An intrusion detection system using bot-iot,” Applied Sciences, vol. 13, no. 9, p. 5427, 2023.
[3] Nazir, Z. Memon, T. Sadiq, H. Rahman, and I. U. Khan, “A novel feature-selection algorithm in iot networks for intrusion detection,” Sen- sors, vol. 23, no. 19, p. 8153, 2023.
[4] G. Kalnoor and S. Gowrishankar, “Iot-based smart environment using intelligent intrusion detection system,” Soft Computing, vol. 25, no. 17, pp. 11 573–11 588, 2021.
[5] M. Sarhan, S. Layeghy, and M. Portmann, “Feature analysis for machine learning-based iot intrusion detection,” arXiv preprint arXiv:2108.12732, 2021.
[6] M. M. Alani and A. Miri, “Towards an explainable universal feature set for iot intrusion detection,” Sensors, vol. 22, no. 15, p. 5690, 2022.
[7] Rathod, Ganesh, Vikrant Sabnis, and Jay Kumar Jain. "Intrusion Detection System (IDS) in Cloud Computing using Machine Learning Algorithms: A Comparative Study." Grenze International Journal of Engineering & Technology (GIJET) 10 (2024).
[8] Ganesh Rathod (2025). Optimizing Feature Selection in Intrusion Detection Using Fisher Score Algorithm: An Analytical Study. International Journal of Innovative Research In Technology (IJIRT), 12(4), 4556-4569.
[9] Rathod, Ganesh, Vikrant Sabnis, and Jay Kumar Jain. "Improving IoT botnet attack detection using machine learning: comparative analysis of feature selection methods and classifiers in intrusion detection systems." In 2024 3rd International Conference for Innovation in Technology (INOCON), pp. 1-8. IEEE, 2024.