Journal of Science, Technology and Social Transformation Volume 2, Issue 02, 2026

AI-Driven Intrusion Detection Systems for Cybersecurity

Divine Ezeagwuna*

Independent Researcher, Canada

Abstract

Artificial Intelligence (AI)-based Intrusion Detection Systems (IDS) have become a vital part of the cybersecurity landscape, offering intelligent, adaptive, and real-time solutions to detect malicious activities in various computing environments. Traditional signature-based detection methods have been found to be limited in their ability to detect new and changing attack patterns as cyber threats grow in complexity, numbers and sophistication. AI-powered IDS solve these issues by utilizing machine learning, deep learning, neural networks, and hybrid analytical methods to effectively identify anomalies, classify threats, and automate incident responses with greater accuracy and efficacy. This study analyzes the development of AI-driven intrusion detection systems, their components, the key AI techniques used and implementation in enterprise networks, cloud computing systems, Internet of Things (IoT) environments, critical infrastructure and host-based systems. The research also examines the performance benefits of AI-powered detection models, such as better detection accuracy and lower false positive rates, and how these models can be scaled up to handle large-scale network monitoring. Besides, it explores the key challenges that are typically encountered in the implementation of AI systems, like adversarial attacks, data privacy, computational complexity, and model interpretability, and identifies some recent trends, such as explainable AI, federated learning, edge intelligence, and predictive threat detection. Overall, the results show that AI-enabled intrusion detection systems can greatly improve cybersecurity resilience, allowing for proactive, adaptive, and intelligent defense strategies that can tackle increasingly complex cyber threats.

Keywords: Artificial Intelligence, Intrusion Detection Systems, Cybersecurity, Machine Learning, Deep Learning, Network Security, Threat Detection, Anomaly Detection, Internet of Things, Cloud Computing.

Introduction

The growth of digital technologies, cloud computing, Internet of Things (IoT) devices, enterprise applications and interconnected communication networks has greatly complicated the cyber security landscape around the world. All of these technological developments have improved the efficiency and digital transformation of operations, but they have also made it easier for cybercriminals to attack. The cyber threats faced today are more complex - such as malware, ransomware, distributed denial-of-service (DDoS) attacks, phishing attacks, insider attacks, advanced persistent threats (APTs) and zero-day exploits - and often conventional security approaches are not adequate to detect threats in time and accurately. Consequently, organizations require intelligent cybersecurity solutions capable of identifying both known and previously unseen attacks in real time (Sunkara, 2022; Khan, Arif, & Khan, 2024).

Intrusion Detection Systems (IDS) have been a cornerstone of network security for years, and they continue to play a crucial role in identifying suspicious activity and unauthorized access to a network. The traditional IDS systems are based on signature-based detection that matches incoming traffic with a set of pre-defined attack signatures. They are effective at stopping known attacks, but can't stop novel attacks, polymorphic malware or fast-changing cyber attacks because they rely on continually updated signature databases. Moreover, conventional anomaly detection techniques tend to produce a large number of false positives, leading to a higher workload for cybersecurity analysts and a decrease in efficiency (Chauhan & Mekala, 2019; Markevych & Dawson, 2023).

With the advent of Artificial Intelligence (AI), intrusion detection has undergone a complete paradigm shift, allowing cybersecurity systems to learn from past incidents and identify sophisticated attack patterns, while constantly adapting to new threats. The intrusion detection systems based on AI include machine learning, deep learning, neural networks, reinforcement learning, and hybrid analytical methods that can help identify threats without requiring any manual effort, enhance the capability of classification, and reduce false alarms. AI-based IDS is superior to

Corresponding Author: Divine Ezeagwuna, Independent Researcher, Canada

How to cite this article: Ezeagwuna, D. (2026). AI-Driven Intrusion Detection Systems for Cybersecurity. *Journal of Science, Technology and Social Transformation* 2(2), 37-51.

Source of support: Nil

Conflict of interest: None

traditional rule-based systems in its ability to detect subtle deviations in network behavior, uncover novel threats, and enable predictive security with ongoing model learning and intelligent decision-making (Salem, Azzam, Emam, & Abohany, 2024; Goswami, 2024).

Supervised learning, unsupervised learning, and semi-supervised learning approaches are all crucial to machine learning-based IDS, as they help the systems to classify network traffic, identify malicious activity, and enhance the detection capabilities. The next generation of security architectures that use deep learning improves intrusion detection systems by unearthing hierarchical features within large and complex cybersecurity data sets, helping to identify advanced attacks that can evade traditional detection methods. The hybrid AI models, which incorporate various learning algorithms, have been found to achieve better detection accuracy, robustness, and adaptability in heterogeneous network environments (Chauhan & Mekala, 2019; Khan, Arif, & Khan, 2024; Madupati, 2024).

AI-powered intrusion detection is being used in many aspects of cyber security. Intelligent IDS solutions are becoming more popular for enterprise networks, which are increasingly facing threats to their distributed infrastructures, want to monitor user activity and protect their organizational assets from both external threats and insiders. In cloud computing, AI can improve the detection and identification of threats, the assessment of risk in real time and the implementation of automated countermeasures, protecting the virtual resources and multi-tenant architectures (Kamadi, 2022; Wang & Xie, 2025). Likewise, with the proliferation of IoT ecosystems, there has been an ever-pressing need for lightweight yet intelligent intrusion detection mechanisms that can defend resource-constrained devices from botnets, propagation of malware, and unauthorized access. Hybrid machine learning and neural network models that leverage AI have proven to be highly effective in enhancing IoT security while ensuring timely detection of threats (Nay, 2024).

Sophisticated cyberattacks that can have significant impacts on the economy and society have emerged as a target for critical infrastructure systems, such as the energy sector, transportation networks, healthcare, financial institutions, and industrial control systems. AI-based IDS systems offer predictive threat intelligence, proactive monitoring, and swift response times, making these critical systems more resilient. The advanced AI algorithms help in detecting early signs and trends of attacks and help in moving beyond reactive cybersecurity to predictive and self-learning methods (Khalaf et al., 2025; Al Abdulwahid, 2025).

Recent advancements have placed more focus on the host-based IDS, which also utilizes AI-based detection and anomaly detection in addition to signature-based approaches to enhance the endpoint security. Combining these two methods can help organizations achieve a more reliable and accurate signature detection and mitigate false negatives while simultaneously detecting unknown attacks by analyzing their behavior (Rehman, Mushtaq, & Zaman, 2024). Moreover, the evolution of AI-driven cybersecurity processes further enhances network security by incorporating smart decision-making capabilities, automated response systems, and adaptive learning features into contemporary security operation centers (SOCs), ensuring quick and efficient responses to emerging cyber threats (Rai et al., 2025).

Despite these significant advancements, AI-driven intrusion detection systems continue to face several technical and operational challenges. These include adversarial machine learning attacks designed to evade AI models, limited availability of high-quality labeled cybersecurity datasets, model interpretability, computational complexity, scalability across distributed environments, and concerns related to data privacy and regulatory compliance. Addressing these challenges remains essential for improving the reliability, transparency, and trustworthiness of AI-enabled cybersecurity systems. Current research increasingly focuses on explainable AI, federated learning, edge intelligence, autonomous cybersecurity, and predictive threat detection as promising directions for enhancing future intrusion detection capabilities (Raja, 2025; Salem et al., 2024).

This study examines the role of AI-driven intrusion detection systems in strengthening modern cybersecurity by reviewing the evolution of intelligent IDS architectures, AI techniques employed in threat detection, deployment across diverse application domains, performance advantages, implementation challenges, and emerging research trends. Through a comprehensive analysis of recent developments, the study provides insights into how AI technologies are transforming intrusion detection into a proactive, adaptive, and intelligent cybersecurity capability capable of defending increasingly complex digital infrastructures against rapidly evolving cyber threats.

Literature Review

Evolution of Intrusion Detection Systems

Intrusion Detection Systems (IDS) have long served as a fundamental component of cybersecurity by monitoring network traffic and system activities to identify malicious behavior. Traditional IDS primarily relied on signature-based techniques, which compare observed activities against a database of known attack patterns. While these methods are effective in detecting previously identified threats, they often fail to recognize zero-day attacks, polymorphic malware, and sophisticated Advanced Persistent Threats (APTs). The rapid evolution of cyber threats has therefore necessitated the development of intelligent detection mechanisms capable of adapting to dynamic attack environments (Chauhan & Mekala, 2019).

The integration of Artificial Intelligence (AI) into intrusion detection has transformed cybersecurity by enabling systems to learn from historical data, recognize complex behavioral patterns, and detect anomalies that conventional rule-based

approaches cannot identify. AI-driven IDS utilize machine learning algorithms, deep learning architectures, and neural networks to continuously improve detection performance while minimizing human intervention. According to Sunkara (2022), AI enhances cybersecurity by providing adaptive threat detection, automated decision-making, and continuous learning capabilities that significantly improve network resilience against emerging attacks.

Recent literature indicates that AI-driven IDS have evolved from standalone anomaly detection tools into comprehensive cybersecurity frameworks capable of supporting enterprise networks, cloud infrastructures, Internet of Things (IoT) ecosystems, and critical infrastructure. Markevych and Dawson (2023) emphasize that modern AI-enabled IDS integrate multiple learning techniques to improve classification accuracy, reduce false positives, and enable proactive cybersecurity defense.

Artificial Intelligence Techniques in Intrusion Detection

Artificial Intelligence encompasses a wide range of computational techniques that enable intrusion detection systems to analyze vast volumes of network traffic and identify suspicious activities in real time. Machine learning remains one of the most widely adopted approaches because it enables systems to classify normal and malicious behaviors through supervised, unsupervised, and semi-supervised learning models. These techniques continuously improve detection accuracy as additional training data become available (Chauhan & Mekala, 2019).

Deep learning has further enhanced intrusion detection by enabling automated feature extraction from high-dimensional cybersecurity datasets. Deep Neural Networks (DNNs), Convolutional Neural Networks (CNNs), and Recurrent Neural Networks (RNNs) have demonstrated exceptional capability in detecting complex attack patterns that are difficult to identify using conventional statistical approaches. Salem et al. (2024) explain that deep learning significantly improves the detection of sophisticated cyber threats through hierarchical pattern recognition and automated representation learning.

Hybrid AI models combine machine learning, neural networks, and statistical anomaly detection techniques to improve both accuracy and computational efficiency. These integrated models reduce false alarm rates while maintaining high detection capabilities across heterogeneous network environments. Nay (2024) demonstrates that hybrid machine learning and neural network architectures substantially enhance IoT intrusion detection by providing rapid classification of diverse attack types with improved scalability.

In addition to machine learning and deep learning, explainable AI (XAI) has emerged as an important research direction because cybersecurity professionals increasingly require transparent and interpretable AI decisions. Khan et al. (2024) note that explainable AI improves analyst confidence by providing meaningful explanations for threat classifications, thereby supporting more informed cybersecurity decision-making.

AI-Based Intrusion Detection Models

AI-driven intrusion detection systems generally employ three primary learning paradigms: supervised learning, unsupervised learning, and semi-supervised learning. Supervised learning algorithms utilize labeled datasets to classify network traffic into normal and malicious categories. Popular algorithms include Decision Trees, Random Forests, Support Vector Machines (SVM), and Artificial Neural Networks. These approaches typically achieve high classification accuracy when high-quality labeled datasets are available (Chauhan & Mekala, 2019).

Unsupervised learning methods detect anomalies without requiring labeled training data by identifying deviations from established behavioral patterns. Such approaches are particularly valuable for detecting zero-day attacks and previously unseen cyber threats. Semi-supervised learning combines both labeled and unlabeled data to improve detection performance while reducing the cost associated with extensive data annotation (Salem et al., 2024).

Recent studies have increasingly focused on hybrid intrusion detection models that combine signature-based detection with AI-driven anomaly detection. Rehman et al. (2024) report that integrating traditional signature detection with AI anomaly analysis enhances host-based intrusion detection by simultaneously identifying known attacks and discovering novel malicious activities. Similarly, Rai et al. (2025) argue that AI-powered hybrid IDS provide more comprehensive network protection by leveraging complementary detection mechanisms to improve overall cybersecurity effectiveness.

Applications of AI-Driven Intrusion Detection Systems

The application of AI-driven intrusion detection has expanded significantly across multiple cybersecurity domains. Enterprise organizations increasingly deploy AI-enabled IDS to monitor distributed networks, detect insider threats, and secure application programming interfaces (APIs). Kamadi (2022) demonstrates that AI-powered intrusion detection strengthens enterprise API security by continuously monitoring distributed Java environments and automatically identifying malicious interactions.

Cloud computing environments have also benefited substantially from AI-driven intrusion detection due to their highly dynamic and scalable architectures. AI algorithms facilitate continuous monitoring of cloud workloads while enabling automated threat mitigation and adaptive resource protection. Wang and Xie (2025) highlight that AI significantly improves cloud security by combining intelligent intrusion detection with automated mitigation strategies capable of responding to evolving cyber threats.

The Internet of Things presents additional cybersecurity challenges because of the large number of interconnected devices with limited computational resources. AI-driven hybrid intrusion detection models provide lightweight yet highly effective mechanisms for detecting botnets, malware propagation, and unauthorized device access. Nay (2024) demonstrates that hybrid machine learning and neural network architectures substantially improve intrusion detection accuracy within IoT environments while maintaining computational efficiency.

Critical infrastructure, including energy systems, transportation networks, healthcare facilities, and industrial control systems, increasingly relies on AI-enabled cybersecurity solutions to defend against sophisticated cyberattacks. Khalaf et al. (2025) report that real-time AI-driven threat detection significantly enhances the resilience of critical infrastructure by enabling predictive threat identification and rapid automated response mechanisms.

Current Challenges and Future Research Trends

Despite substantial advancements, AI-driven intrusion detection systems continue to face several technical and operational challenges. One major concern involves high false positive rates, which can overwhelm cybersecurity analysts and reduce operational efficiency. AI models are also vulnerable to adversarial attacks, where carefully crafted malicious inputs manipulate model predictions and evade detection (Madupati, 2024).

Another significant challenge concerns computational complexity and scalability. Training advanced deep learning models requires extensive computational resources and large, high-quality datasets. This limitation is particularly relevant in resource-constrained environments such as IoT devices and edge computing systems. Raja (2025) notes that future AI-driven intrusion detection systems must achieve greater computational efficiency while maintaining high detection performance.

Data privacy and model transparency remain additional concerns. Organizations increasingly require explainable AI solutions capable of justifying detection decisions while preserving sensitive information. Al Abdulwahid (2025) proposes predictive cybersecurity approaches that leverage machine learning to identify attack precursors before malicious activities occur, enabling more proactive and intelligent cyber defense strategies.

Emerging research increasingly focuses on federated learning, edge intelligence, explainable AI, autonomous threat hunting, and predictive intrusion detection. These innovations aim to improve detection accuracy, reduce response time, enhance privacy preservation, and support real-time cybersecurity decision-making across highly distributed digital environments.

AI-Driven Intrusion Detection System Architecture

AI-driven Intrusion Detection Systems (IDS) integrate artificial intelligence technologies with conventional network monitoring mechanisms to provide adaptive, intelligent, and real-time threat detection. Unlike traditional IDS that primarily rely on predefined attack signatures, AI-driven architectures employ machine learning, deep learning, and neural network models to identify both known and unknown attacks by continuously learning from network behaviors.

Table 1: Comparative Review of AI Techniques for Intrusion Detection Systems

AI Technique	*Principle*	*Major Advantages*	*Limitations*	*Typical Cybersecurity Applications*	*Supporting References*
Machine Learning	Learns patterns from labeled or unlabeled datasets	High detection accuracy, adaptive learning, efficient classification	Requires quality training data	Network intrusion detection, malware detection	Chauhan & Mekala (2019); Khan et al. (2024)
Deep Learning	Multi-layer neural networks automatically extract complex features	Detects sophisticated attacks with high precision	High computational cost and large dataset requirements	Advanced Persistent Threat (APT) detection, anomaly detection	Salem et al. (2024); Sunkara (2022)
Neural Networks	Models nonlinear relationships in cybersecurity data	Excellent pattern recognition capability	Risk of overfitting and computational complexity	IoT intrusion detection, behavioral analysis	Nay (2024); Goswami (2024)
Hybrid AI Models	Combines multiple AI and traditional detection techniques	Lower false positives, improved robustness, comprehensive detection	Complex implementation and optimization	Enterprise security, cloud security, host-based IDS	Markevych & Dawson (2023); Rehman et al. (2024); Rai et al. (2025)
Predictive AI Models	Forecasts attack precursors using historical behavioral data	Proactive threat detection and early response	Requires continuous model updating	Critical infrastructure, predictive cybersecurity	Al Abdulwahid (2025); Khalaf et al. (2025); Raja (2025)

This intelligent architecture enhances detection accuracy, minimizes false positives, and enables rapid responses to sophisticated cyber threats across enterprise networks, cloud infrastructures, Internet of Things (IoT) ecosystems, and critical infrastructure (Chauhan & Mekala, 2019; Salem et al., 2024).

Components of AI-Driven Intrusion Detection Systems

The effectiveness of an AI-driven IDS depends on the integration of multiple architectural components that collectively monitor, analyze, classify, and respond to cyber threats. These components establish a continuous cybersecurity lifecycle capable of processing high-volume network traffic while adapting to evolving attack techniques.

Data Collection Layer

The data collection layer serves as the entry point of the intrusion detection architecture. It gathers network traffic, packet captures, system logs, application logs, API requests, endpoint activities, authentication records, and cloud telemetry from various sources. Modern AI-driven IDS architectures also collect behavioral information from IoT devices, industrial control systems, and distributed cloud services to provide comprehensive visibility across heterogeneous computing environments (Kamadi, 2022; Wang & Xie, 2025).

The quality and diversity of collected data directly influence the effectiveness of AI models. Comprehensive datasets enable learning algorithms to distinguish between normal operational behavior and malicious activities with greater precision.

Data Preprocessing and Feature Engineering

Raw cybersecurity data often contains redundant, incomplete, or noisy information that may reduce model performance. Consequently, preprocessing becomes an essential architectural stage involving data cleaning, normalization, encoding, dimensionality reduction, and feature extraction.

Feature engineering transforms raw traffic into meaningful indicators such as packet size, protocol type, session duration, connection frequency, payload characteristics, failed authentication attempts, and communication patterns. Effective feature selection reduces computational complexity while improving classification accuracy by eliminating irrelevant variables (Markevych & Dawson, 2023; Khan et al., 2024).

AI-Based Detection Engine

The AI detection engine represents the core intelligence of the intrusion detection architecture. It applies artificial intelligence algorithms to analyze extracted features and determine whether observed activities indicate legitimate behavior or potential cyberattacks.

Supervised learning algorithms utilize labeled datasets to recognize previously identified attack categories, whereas unsupervised learning detects anomalies without requiring labeled data. Deep learning architectures, including convolutional neural networks (CNNs), recurrent neural networks (RNNs), long short-term memory (LSTM) networks, and hybrid neural models, further improve the detection of complex attack sequences by learning intricate behavioral relationships within large-scale datasets (Salem et al., 2024; Nay, 2024).

Hybrid AI models combine statistical analysis, machine learning, and neural networks to improve resilience against zero-day attacks and advanced persistent threats (APTs). These models continuously update detection capabilities as new attack patterns emerge.

Threat Classification Module

Following behavioral analysis, the classification module categorizes detected events into predefined attack classes such as malware, phishing, denial-of-service (DoS), distributed denial-of-service (DDoS), insider threats, ransomware, botnet activity, privilege escalation, and data exfiltration attacks.

Advanced classification engines employ ensemble learning and probabilistic decision-making techniques to assign confidence scores to each detected threat. Such prioritization enables cybersecurity teams to allocate resources effectively while reducing alert fatigue caused by excessive false positives (Madupati, 2024; Goswami, 2024).

Response and Mitigation Layer

Once an intrusion is detected, the response layer automatically initiates defensive actions to minimize potential damage. Depending on system configuration, mitigation strategies may include isolating compromised devices, blocking malicious IP addresses, terminating suspicious sessions, updating firewall rules, quarantining infected hosts, or notifying security analysts.

Modern Security Orchestration, Automation, and Response (SOAR) platforms further enhance AI-driven IDS by integrating automated incident response workflows with threat intelligence feeds and Security Information and Event Management (SIEM) systems, enabling rapid containment of cyber incidents (Sunkara, 2022; Rai et al., 2025).

Workflow of AI-Driven Intrusion Detection

The operational workflow of an AI-driven intrusion detection system follows a continuous analytical process that transforms raw network data into actionable security intelligence. Initially, traffic and system events are captured from multiple endpoints and communication channels. The collected information undergoes preprocessing to eliminate inconsistencies and extract meaningful security features. These processed datasets are then analyzed by AI models trained to recognize malicious behavioral patterns.

The detection engine evaluates each event against learned behavioral profiles and anomaly thresholds before classifying potential threats according to attack categories. Once malicious activity is confirmed, automated mitigation

mechanisms generate alerts, isolate affected systems, and implement predefined response policies. Feedback from security analysts and incident outcomes is subsequently incorporated into the training dataset, enabling continuous model refinement and adaptation to emerging attack techniques (Chauhan & Mekala, 2019; Salem et al., 2024).

This adaptive workflow allows AI-driven IDS to evolve alongside changing cyber threat landscapes while maintaining high detection performance in dynamic network environments.

Detection Lifecycle

The detection lifecycle within AI-driven IDS extends beyond simple attack identification by incorporating continuous learning and adaptive intelligence. The lifecycle typically consists of six interconnected stages:

- **Traffic Monitoring:** Continuous observation of network communications and endpoint activities.
- **Data Processing:** Cleaning, transformation, normalization, and feature extraction.
- **Behavioral Analysis:** AI algorithms evaluate network behavior for anomalies and attack signatures.
- **Threat Detection:** Classification of suspicious activities using machine learning or deep learning models.
- **Response and Recovery:** Automated or human-assisted mitigation procedures are initiated to contain attacks.
- **Model Updating:** Newly discovered attack behaviors are incorporated into retraining processes to improve future detection accuracy.

Continuous retraining significantly enhances system resilience against zero-day attacks, polymorphic malware, and evolving adversarial techniques, ensuring long-term detection effectiveness (Markevych & Dawson, 2023; Raja, 2025).

Performance Evaluation Metrics

Evaluating AI-driven intrusion detection systems requires multiple quantitative performance metrics that collectively measure detection capability, reliability, and computational efficiency.

Accuracy measures the proportion of correctly classified normal and malicious instances within the overall dataset. Although widely used, accuracy alone may be insufficient when dealing with highly imbalanced cybersecurity datasets.

Precision evaluates the proportion of detected attacks that are truly malicious, providing insight into false alarm reduction.

Recall, also referred to as the detection rate or sensitivity, measures the ability of the IDS to correctly identify actual attacks. High recall is particularly important for minimizing undetected intrusions.

F1-Score combines precision and recall into a single performance metric, offering balanced evaluation when datasets contain unequal class distributions.

False Positive Rate (FPR) quantifies the percentage of legitimate activities incorrectly classified as attacks. Lower false positive rates reduce unnecessary investigations and improve operational efficiency.

Receiver Operating Characteristic (ROC) Curve and Area Under the Curve (AUC) evaluate classification capability across multiple decision thresholds, providing comprehensive insight into model discrimination performance.

Additional evaluation criteria include detection latency, computational overhead, scalability, resource utilization, and

Figure 1

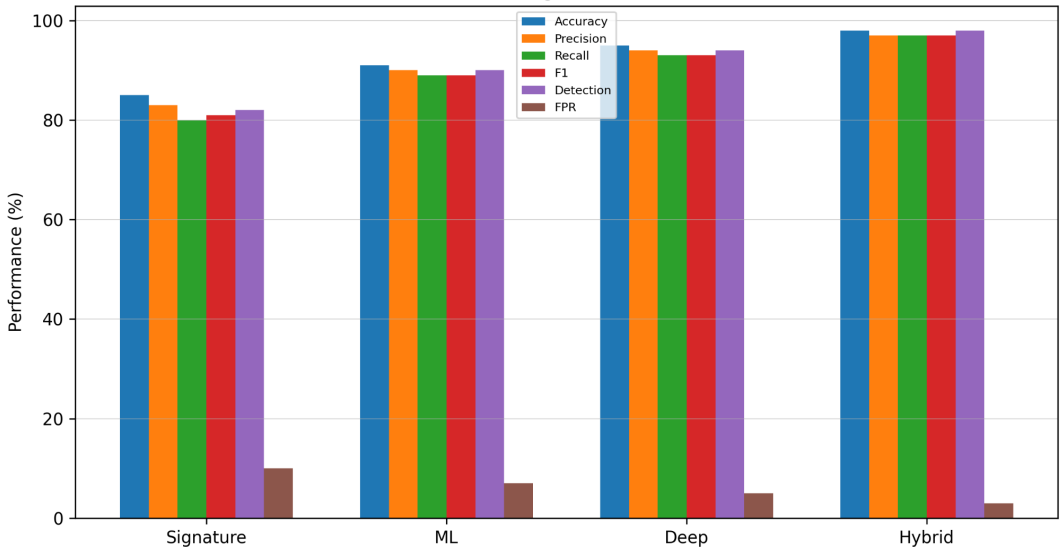

Figure 1: Compares Signature-Based IDS, Machine Learning IDS, Deep Learning IDS, and Hybrid AI IDS across Accuracy, Precision, Recall, F1-Score, Detection Rate, and False Positive Rate.

model adaptability under dynamic network conditions. These metrics collectively determine whether AI-driven IDS can satisfy the real-time performance requirements of enterprise environments, cloud infrastructures, IoT ecosystems, and critical infrastructure protection (Goswami, 2024; Khalaf et al., 2025; Wang & Xie, 2025).

Applications of AI-Driven Intrusion Detection Systems

Artificial Intelligence (AI)-driven Intrusion Detection Systems (IDS) have transformed cybersecurity by enabling intelligent, adaptive, and real-time detection of cyber threats across diverse computing environments. Unlike conventional intrusion detection solutions that primarily depend on predefined signatures and manually crafted rules, AI-powered IDS continuously learn from network traffic, system logs, and behavioral patterns to identify both known and previously unseen attacks. The integration of machine learning, deep learning, and hybrid AI techniques has significantly improved the detection accuracy, scalability, and responsiveness of intrusion detection systems, making them suitable for protecting modern digital infrastructures (Chauhan & Mekala, 2019; Salem et al., 2024).

As organizations increasingly adopt cloud computing, Internet of Things (IoT), enterprise applications, and distributed infrastructures, the attack surface continues to expand. Consequently, AI-driven IDS have become essential components of cybersecurity strategies across multiple domains. These intelligent systems not only detect malicious activities but also support automated threat analysis, predictive security, adaptive learning, and rapid incident response, thereby strengthening organizational cyber resilience (Khan et al., 2024; Sunkara, 2022).

Enterprise Network Security

Enterprise networks represent one of the primary deployment environments for AI-driven intrusion detection systems. Modern enterprises generate enormous volumes of network traffic from employee workstations, servers, cloud services, mobile devices, and remote access platforms. Traditional IDS often struggle to analyze such complex environments due to high traffic volumes and continuously evolving attack techniques.

AI-driven IDS improve enterprise security by applying machine learning algorithms to monitor network behavior continuously, identify anomalies, classify malicious traffic, and detect insider threats that may bypass conventional signature-based systems. These intelligent models learn normal organizational behavior and automatically recognize deviations associated with malware infections, privilege escalation, unauthorized access attempts, ransomware activities, and advanced persistent threats (APTs). Adaptive learning further enables the system to improve detection performance as new attack data become available (Chauhan & Mekala, 2019; Goswami, 2024).

Kamadi (2022) further emphasizes that AI-driven intrusion detection plays a vital role in securing enterprise APIs and distributed Java environments, where multiple interconnected services exchange sensitive information. Intelligent IDS can analyze API requests, authentication behaviors, and transaction patterns to detect malicious API abuse before significant damage occurs.

Cloud Computing Security

Cloud computing environments present unique cybersecurity challenges because of shared infrastructures, virtualized resources, dynamic workloads, and geographically distributed services. Traditional intrusion detection approaches often struggle to maintain visibility across cloud-native architectures, especially when workloads are continuously created, migrated, or scaled.

AI-driven IDS enhance cloud security by monitoring virtual machines, containers, application programming interfaces (APIs), cloud storage, and network communications simultaneously. Machine learning algorithms analyze large-scale cloud telemetry to identify abnormal resource utilization, unauthorized access, privilege misuse, lateral movement, data exfiltration, and distributed denial-of-service (DDoS) attacks in real time.

Deep learning models further improve cloud security by identifying subtle behavioral changes that may indicate sophisticated cyberattacks before they become critical incidents. Automated mitigation mechanisms integrated with AI-based IDS also enable rapid isolation of compromised resources while minimizing disruption to legitimate cloud services (Wang & Xie, 2025; Salem et al., 2024). The combination of AI-powered monitoring and automated incident response provides cloud providers with scalable protection against increasingly sophisticated cyber threats.

Internet of Things (IoT) Security

The rapid growth of IoT devices has significantly expanded organizational attack surfaces. Smart sensors, wearable devices, industrial controllers, connected healthcare equipment, and smart city infrastructures generate massive amounts of heterogeneous network traffic, making conventional intrusion detection increasingly ineffective.

AI-driven IDS provide intelligent monitoring of IoT ecosystems by learning the normal communication behavior of connected devices and identifying deviations that indicate cyberattacks. Hybrid machine learning models combining supervised learning with neural networks are particularly effective in detecting botnets, spoofing attacks, denial-of-service attacks, malware propagation, and unauthorized device communications.

Because IoT devices typically possess limited computational resources, lightweight AI models have become increasingly important for edge deployment. These models perform local intrusion detection while minimizing computational overhead and communication latency. Nay

(2024) demonstrates that hybrid machine learning and neural network architectures substantially improve intrusion detection accuracy while maintaining efficient operation within resource-constrained IoT environments. Similarly, Khan et al. (2024) highlight that AI enables continuous monitoring and adaptive threat detection for rapidly expanding IoT ecosystems.

Critical Infrastructure Protection

Critical infrastructure sectors including energy, transportation, healthcare, telecommunications, financial services, and water supply systems have become high-value targets for sophisticated cyberattacks. Successful attacks against these infrastructures may disrupt essential services and produce severe economic and societal consequences.

AI-driven IDS strengthen critical infrastructure protection by continuously analyzing operational technology (OT) networks, industrial control systems (ICS), and supervisory control and data acquisition (SCADA) environments. Machine learning algorithms detect deviations from normal industrial processes, identify malicious commands, recognize coordinated attacks, and provide early warning before operational disruptions occur.

Real-time AI-powered threat detection enables infrastructure operators to respond proactively rather than reactively. Predictive analytics further improve cyber resilience by identifying attack precursors and estimating future attack likelihood based on evolving threat intelligence. Khalaf et al. (2025) demonstrate that AI-driven real-time threat detection systems significantly improve the protection of critical infrastructure by enabling rapid identification of sophisticated cyber threats. Likewise, Al Abdulwahid (2025) emphasizes the growing importance of predictive AI models capable of identifying attack precursors before exploitation occurs.

API Security

Modern organizations increasingly rely on APIs to facilitate communication among cloud services, enterprise applications, mobile platforms, and third-party systems. While APIs improve interoperability, they also introduce numerous security vulnerabilities, including authentication bypass, injection attacks, excessive data exposure, credential theft, and API abuse.

AI-driven intrusion detection systems provide intelligent API security by continuously monitoring request patterns, authentication behaviors, transaction frequencies, payload structures, and user interactions. Machine learning algorithms distinguish legitimate API usage from malicious activities by identifying unusual access patterns and behavioral anomalies.

Kamadi (2022) explains that AI-driven IDS deployed within distributed Java environments effectively detect API attacks that traditional rule-based security systems frequently overlook. Continuous behavioral learning enables these systems to recognize evolving attack techniques while reducing false-positive alerts that commonly affect conventional intrusion detection systems.

Host-Based Intrusion Detection

Host-based intrusion detection systems (HIDS) monitor activities occurring directly on individual computing devices, including servers, workstations, laptops, and virtual machines. AI-driven HIDS analyze operating system logs, process execution, memory utilization, registry modifications, file integrity, user behavior, and application activities to detect malicious behavior.

Unlike traditional host-based IDS that primarily rely on predefined attack signatures, AI-powered anomaly detection continuously learns normal host behavior and identifies suspicious deviations associated with malware infections, ransomware, privilege escalation, insider threats, and zero-day attacks. Hybrid detection models combining signature-based detection with machine learning provide comprehensive protection by identifying both previously known and unknown attack patterns.

Rehman et al. (2024) demonstrate that integrating signature-based methods with AI-driven anomaly detection substantially improves detection capability while reducing false positives. Similarly, Rai et al. (2025) highlight that advanced AI-powered intrusion detection protocols significantly enhance endpoint security by enabling intelligent behavioral analysis and continuous adaptation to emerging cyber threats.

Comparative Analysis of AI-Driven IDS Applications

The applicability of AI-driven intrusion detection varies according to deployment environments, attack characteristics, and operational requirements. Enterprise networks emphasize behavioral analytics and insider threat detection, while cloud environments prioritize scalability and virtualization security. IoT deployments require lightweight AI models capable of operating under resource constraints, whereas critical infrastructure demands highly reliable real-time threat detection with predictive capabilities. API security focuses on transaction analysis and behavioral authentication, while host-based intrusion detection emphasizes endpoint behavior monitoring and anomaly detection.

Overall, AI-driven intrusion detection systems have become indispensable across modern cybersecurity domains because they provide adaptive, scalable, and intelligent protection against increasingly sophisticated cyber threats. By integrating advanced machine learning techniques with continuous behavioral analysis, these systems enable organizations to detect both known and unknown attacks more accurately than traditional rule-based approaches. As AI technologies continue to mature, intrusion detection systems are expected to become increasingly autonomous, predictive, and resilient, supporting proactive cybersecurity

Table 2: Applications of AI-Driven Intrusion Detection Systems Across Cybersecurity Domains

Application Domain	*Primary Threats*	*AI Techniques Employed*	*Major Benefits*	*Key References*
Enterprise Networks	Insider threats, malware, ransomware, APTs	Machine Learning, Deep Learning	Behavioral analytics, adaptive detection, reduced false positives	Chauhan & Mekala (2019); Goswami (2024); Kamadi (2022)
Cloud Computing	Data breaches, DDoS, privilege escalation, lateral movement	Deep Learning, Neural Networks	Scalable monitoring, automated threat mitigation, real-time detection	Wang & Xie (2025); Salem et al. (2024)
Internet of Things (IoT)	Botnets, spoofing, malware, device compromise	Hybrid ML, Neural Networks	Lightweight detection, adaptive learning, edge intelligence	Nay (2024); Khan et al. (2024)
Critical Infrastructure	ICS attacks, SCADA attacks, APTs, sabotage	Predictive AI, Machine Learning	Early warning, predictive analytics, operational resilience	Khalaf et al. (2025); Al Abdulwahid (2025)
Enterprise APIs	API abuse, injection attacks, credential theft	Machine Learning, Behavioral Analytics	Intelligent API monitoring, reduced false alarms	Kamadi (2022)
Host-Based Systems	Malware, ransomware, insider threats, zero-day attacks	Signature-Based + AI Anomaly Detection	Endpoint protection, improved detection accuracy	Rehman et al. (2024); Rai et al. (2025)

strategies across enterprise, cloud, IoT, critical infrastructure, and endpoint environments (Madupati, 2024; Raja, 2025; Markevych & Dawson, 2023).

Challenges and Emerging Trends

The rapid advancement of Artificial Intelligence (AI)-driven Intrusion Detection Systems (IDS) has significantly improved the ability of organizations to identify, analyze, and respond to increasingly sophisticated cyber threats. By leveraging machine learning, deep learning, and hybrid AI models, modern IDS can detect both known and unknown attack patterns with higher accuracy than traditional signature-based approaches. Despite these advancements, AI-driven intrusion detection systems continue to face numerous technical, operational, and security challenges that affect their reliability, scalability, and deployment across heterogeneous computing environments. Simultaneously, ongoing research has introduced emerging technologies that promise to enhance the adaptability, intelligence, and resilience of AI-powered cybersecurity frameworks.

Figure 2

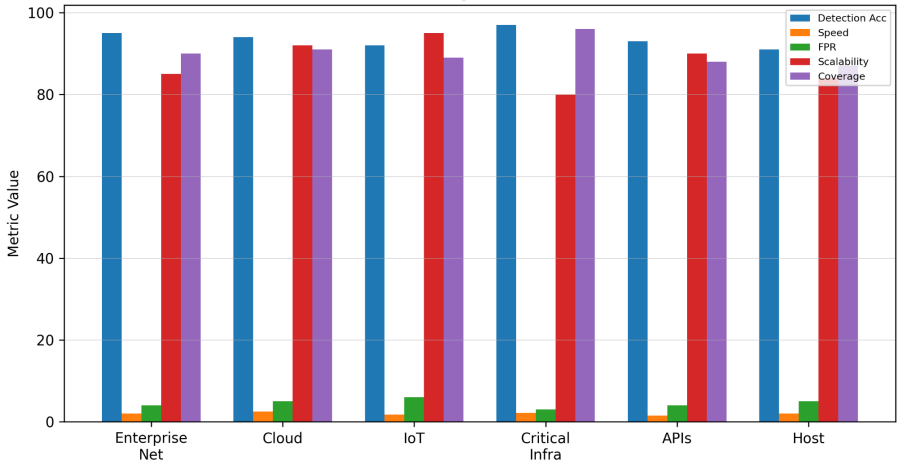

Figure 2: Compares six application domains using Detection Accuracy, Detection Speed, False Positive Rate, Scalability Score, and Threat Coverage Score

Challenges of AI-Driven Intrusion Detection Systems

High False Positive and False Negative Rates

One of the most persistent challenges facing AI-driven IDS is maintaining a balance between detection sensitivity and accuracy. Although AI algorithms are capable of recognizing complex attack behaviors, they often generate false positive alerts by incorrectly classifying legitimate network activities as malicious. Excessive false positives increase alert fatigue among security analysts and consume valuable incident response resources. Conversely, false negatives allow sophisticated attacks to bypass detection mechanisms, thereby exposing organizations to significant security risks. Improving feature engineering, optimizing learning algorithms, and employing ensemble learning models have been identified as effective strategies for reducing classification errors while maintaining high detection performance (Chauhan & Mekala, 2019; Goswami, 2024).

Limited Availability and Quality of Training Data

The effectiveness of supervised AI models depends heavily on the availability of high-quality labeled datasets. However, cybersecurity datasets are frequently incomplete, imbalanced, outdated, or contain redundant traffic patterns that limit the ability of machine learning algorithms to generalize to real-world environments. Emerging attack vectors evolve rapidly, making existing benchmark datasets insufficient for training robust intrusion detection models. Researchers therefore advocate continuous dataset updating, synthetic data generation, and data augmentation techniques to improve model robustness and adaptability (Salem et al., 2024; Markevych & Dawson, 2023).

Adversarial AI Attacks

As AI becomes increasingly integrated into cybersecurity systems, attackers have begun exploiting vulnerabilities within AI models themselves. Adversarial attacks manipulate input data to deceive machine learning algorithms into misclassifying malicious activities as legitimate traffic. Poisoning attacks can corrupt training datasets, while evasion attacks exploit weaknesses during model inference. These emerging threats challenge the reliability of AI-driven IDS and necessitate the development of adversarially robust learning techniques capable of maintaining detection accuracy under hostile conditions (Madupati, 2024; Raja, 2025).

Computational Complexity and Scalability

Deep learning architectures require substantial computational resources for both training and inference. Enterprise networks, cloud infrastructures, and Internet of Things (IoT) ecosystems generate massive volumes of network traffic that must be analyzed continuously in real time. Processing such large-scale data streams often results in increased latency, higher memory consumption, and significant infrastructure costs. Consequently, researchers are exploring lightweight AI models, distributed computing architectures, and edge-based deployment strategies to improve scalability without sacrificing detection performance (Nay, 2024; Wang & Xie, 2025).

Explainability and Model Transparency

Many advanced AI algorithms, particularly deep neural networks, operate as "black-box" systems whose decision-making processes are difficult for security analysts to interpret. The lack of transparency complicates incident investigation, reduces user trust, and creates compliance challenges for highly regulated industries. Explainable Artificial Intelligence (XAI) has therefore become an important research area focused on providing interpretable threat classifications while maintaining predictive accuracy (Salem et al., 2024; Khan et al., 2024).

Privacy and Regulatory Compliance

Modern intrusion detection systems continuously monitor user activities, application logs, and network traffic, potentially exposing sensitive personal or organizational information. Privacy regulations require organizations to implement secure data handling practices while ensuring effective threat detection. Privacy-preserving machine learning approaches, including federated learning and secure multi-party computation, are increasingly investigated as mechanisms for protecting confidential information without compromising cybersecurity performance (Wang & Xie, 2025; Al Abdulwahid, 2025).

Zero-Day and Advanced Persistent Threat Detection

Zero-day exploits and Advanced Persistent Threats (APTs) remain among the most difficult attacks to detect because they exploit previously unknown vulnerabilities and exhibit stealthy behaviors over extended periods. Although AI-based anomaly detection significantly improves the identification of unknown threats compared to signature-based systems, distinguishing malicious anomalies from legitimate behavioral variations remains a major challenge. Continuous learning mechanisms and predictive AI models are increasingly adopted to improve early attack identification (Sunkara, 2022; Rai et al., 2025).

Emerging Trends in AI-Driven Intrusion Detection Systems

Explainable Artificial Intelligence (XAI)

Explainable AI has become a major research direction aimed at improving transparency in intrusion detection. Rather than producing only classification outputs, XAI provides understandable explanations for detected threats, enabling cybersecurity professionals to validate AI-generated

Table 3: Major Challenges, Impacts, AI-Based Solutions, and Future Directions of AI-Driven Intrusion Detection Systems

Challenge	*Impact on cybersecurity*	*Ai-based solution*	*Future research direction*	*References*
False Positives and False Negatives	Reduced detection reliability and alert fatigue	Ensemble learning and hybrid AI models	Adaptive learning algorithms	Chauhan & Mekala (2019); Goswami (2024)
Poor Training Data Quality	Reduced model generalization	Data augmentation and synthetic datasets	Automated dataset generation	Salem et al. (2024); Markevych & Dawson (2023)
Adversarial AI Attacks	Model manipulation and detection evasion	Adversarial training	Robust AI security frameworks	Madupati (2024); Raja (2025)
Computational Complexity	High processing overhead	Edge AI and distributed computing	Lightweight deep learning models	Nay (2024); Wang & Xie (2025)
Lack of Explainability	Limited analyst trust	Explainable AI (XAI)	Interpretable neural networks	Khan et al. (2024); Salem et al. (2024)
Privacy and Compliance	Data protection risks	Federated learning	Privacy-preserving AI	Al Abdulwahid (2025); Wang & Xie (2025)
Zero-Day Attacks	Difficult detection of novel threats	Predictive anomaly detection	Autonomous adaptive IDS	Sunkara (2022); Rai et al. (2025)

decisions and enhance organizational trust in automated security systems (Salem et al., 2024).

Federated Learning for Distributed Security

Federated learning enables multiple organizations to collaboratively train intrusion detection models without sharing sensitive network data. This decentralized learning approach enhances privacy protection while enabling continuous model improvement across distributed environments such as healthcare systems, financial institutions, and government agencies (Al Abdulwahid, 2025).

Edge AI for Internet of Things Security

The rapid expansion of IoT devices has increased demand for intrusion detection systems capable of performing local threat analysis with minimal latency. Edge AI allows machine learning models to operate directly on edge devices, reducing bandwidth consumption and enabling real-time detection of attacks occurring within resource-constrained IoT environments (Nay, 2024).

AI-Driven Predictive Cybersecurity

Traditional IDS primarily detect attacks after malicious activities begin. Emerging predictive cybersecurity models seek to identify attack precursors before system compromise occurs by analyzing behavioral indicators, threat intelligence, and historical attack patterns. Predictive AI enhances proactive defense capabilities and reduces incident response time (Al Abdulwahid, 2025).

Autonomous Cyber Defense

Modern research increasingly focuses on autonomous intrusion detection systems capable of continuously monitoring network environments, identifying attacks, and initiating automated mitigation strategies without requiring human intervention. Such systems integrate reinforcement learning, adaptive decision-making, and intelligent orchestration to provide continuous cybersecurity protection (Khalaf et al., 2025; Rai et al., 2025).

Cloud-Native AI Security

As organizations migrate critical services to cloud infrastructures, AI-driven IDS are being integrated into cloud-native architectures to provide scalable, distributed, and real-time protection. Cloud-based AI platforms leverage elastic computing resources to process high-volume traffic while supporting dynamic threat intelligence and automated incident response (Wang & Xie, 2025).

Hybrid Intrusion Detection Models

Current research demonstrates increasing adoption of hybrid intrusion detection architectures that combine signature-based detection with anomaly-based AI techniques. These integrated models improve detection coverage by identifying both known attacks and previously unseen threats while minimizing false alarm rates (Rehman et al., 2024; Kamadi, 2022).

Overall, while AI-driven intrusion detection systems have substantially improved cybersecurity through intelligent threat detection and adaptive defense mechanisms, several technical and operational challenges continue to limit their full potential. Emerging technologies such as explainable AI, federated learning, predictive cybersecurity, autonomous cyber defense, cloud-native AI, and edge intelligence are expected to address many of these limitations. Continued research into trustworthy, scalable, and privacy-preserving AI models will play a pivotal role in developing the next generation of intelligent intrusion detection systems capable of defending increasingly complex digital infrastructures against evolving cyber threats (Chauhan & Mekala, 2019; Salem et al., 2024; Raja, 2025).

Table 3: Major Challenges, Impacts, AI-Based Solutions, and Future Directions of AI-Driven Intrusion Detection Systems

Challenge	*Impact on cybersecurity*	*Ai-based solution*	*Future research direction*	*References*
False Positives and False Negatives	Reduced detection reliability and alert fatigue	Ensemble learning and hybrid AI models	Adaptive learning algorithms	Chauhan & Mekala (2019); Goswami (2024)
Poor Training Data Quality	Reduced model generalization	Data augmentation and synthetic datasets	Automated dataset generation	Salem et al. (2024); Markevych & Dawson (2023)
Adversarial AI Attacks	Model manipulation and detection evasion	Adversarial training	Robust AI security frameworks	Madupati (2024); Raja (2025)
Computational Complexity	High processing overhead	Edge AI and distributed computing	Lightweight deep learning models	Nay (2024); Wang & Xie (2025)
Lack of Explainability	Limited analyst trust	Explainable AI (XAI)	Interpretable neural networks	Khan et al. (2024); Salem et al. (2024)
Privacy and Compliance	Data protection risks	Federated learning	Privacy-preserving AI	Al Abdulwahid (2025); Wang & Xie (2025)
Zero-Day Attacks	Difficult detection of novel threats	Predictive anomaly detection	Autonomous adaptive IDS	Sunkara (2022); Rai et al. (2025)

Discussion

The growing sophistication of cyber threats has transformed intrusion detection systems (IDS) from traditional rule-based mechanisms into intelligent, adaptive platforms capable of identifying both known and unknown attacks. The literature consistently demonstrates that Artificial Intelligence (AI) has become a fundamental enabler of modern cybersecurity by improving detection accuracy, reducing response time, and enabling continuous adaptation to evolving attack patterns. Compared with conventional signature-based IDS, AI-driven systems leverage machine learning and deep learning algorithms to analyze large volumes of network traffic, identify anomalous behaviors, and detect previously unseen threats with greater efficiency (Chauhan & Mekala, 2019; Salem et al., 2024).

One of the most significant findings across the reviewed studies is the superiority of AI-based detection techniques over conventional intrusion detection approaches. Traditional IDS primarily rely on predefined attack signatures, making them highly effective against known threats but ineffective against zero-day exploits and polymorphic malware. AI-driven IDS overcome this limitation by learning behavioral patterns from historical and real-time network data, enabling anomaly detection that can identify malicious activities without relying solely on existing signatures. Markevych and Dawson (2023) emphasize that integrating artificial intelligence into intrusion detection substantially enhances system adaptability, while Khan et al. (2024) further argue that machine learning algorithms improve threat classification through continuous learning and automated decision-making. These capabilities significantly reduce manual intervention and enable organizations to respond more effectively to increasingly sophisticated cyberattacks.

The discussion also highlights the growing importance of hybrid AI models that combine multiple analytical techniques to improve detection performance. Rather than depending on a single machine learning algorithm, hybrid systems integrate supervised learning, unsupervised learning, neural networks, and ensemble models to achieve higher detection rates while minimizing false alarms. Nay (2024) demonstrates that hybrid machine learning and neural network architectures significantly improve IoT security by identifying complex attack behaviors that conventional approaches often fail to detect. Similarly, Salem et al. (2024) report that combining multiple AI methodologies produces more robust detection capabilities across heterogeneous computing environments, particularly where network traffic exhibits dynamic and unpredictable characteristics.

Another important observation concerns the expanding deployment of AI-driven intrusion detection systems across diverse cybersecurity domains. Enterprise environments increasingly utilize AI-based IDS to protect distributed applications, cloud services, and organizational networks against advanced persistent threats and insider attacks. Kamadi (2022) illustrates how AI-driven intrusion detection strengthens enterprise API security by providing continuous behavioral analysis within distributed Java environments. Likewise, Wang and Xie (2025) discuss the growing relevance of AI-powered IDS in cloud computing, where scalable machine learning models enable continuous monitoring of virtualized infrastructures while supporting automated mitigation strategies. These findings demonstrate that AI technologies are no longer limited to research environments but have become practical cybersecurity solutions across multiple operational settings.

The literature also emphasizes the importance of AI-driven intrusion detection in securing emerging technologies such as the Internet of Things (IoT) and critical infrastructure. IoT environments generate massive volumes of heterogeneous data while operating under significant resource constraints,

creating challenges for conventional intrusion detection mechanisms. AI-based IDS address these limitations through intelligent feature extraction and adaptive anomaly detection capable of identifying attacks against connected devices in real time (Nay, 2024). Similarly, Khalaf et al. (2025) demonstrate that AI-enabled threat detection systems significantly strengthen cybersecurity resilience within critical infrastructure by providing continuous monitoring, predictive analytics, and rapid incident response capabilities that reduce operational risks associated with cyberattacks.

Host-based intrusion detection has likewise benefited from the integration of artificial intelligence. Conventional host-based systems typically depend on static signature databases, limiting their ability to detect sophisticated attacks targeting system processes and user behaviors. Rehman et al. (2024) demonstrate that combining signature-based detection with AI-driven anomaly detection substantially improves host protection by identifying both known malware and previously unseen malicious activities. This hybrid approach enhances overall detection coverage while reducing false positives that commonly affect purely anomaly-based detection systems.

Despite these advancements, several implementation challenges remain. One recurring concern involves the computational complexity associated with training and deploying advanced AI models. Deep learning architectures often require substantial computational resources, large training datasets, and specialized hardware, which may limit their adoption among organizations with constrained resources. Goswami (2024) notes that maintaining high detection accuracy while ensuring real-time processing remains a critical engineering challenge. Similarly, Madupati (2024) highlights that balancing detection performance with computational efficiency continues to be an active area of cybersecurity research, particularly as enterprise networks continue to expand in size and complexity.

Another significant challenge concerns adversarial machine learning and the robustness of AI models against manipulation. Attackers increasingly develop adversarial techniques designed to evade AI-based detection systems by generating malicious inputs that resemble legitimate network behavior. Such attacks expose vulnerabilities within machine learning models and may reduce overall detection reliability. Raja (2025) argues that strengthening model robustness through adversarial training, continuous model updating, and explainable AI techniques will become increasingly important as cyber adversaries adopt AI technologies themselves. Likewise, Al Abdulwahid (2025) emphasizes the need for predictive cybersecurity models capable of identifying attack precursors before malicious activities fully materialize, thereby enabling proactive rather than reactive defense strategies.

The discussion further reveals that explainability and trust remain essential considerations for future AI-driven intrusion detection systems. Although deep learning models frequently achieve superior detection performance, their decision-making processes often lack transparency, making it difficult for cybersecurity analysts to interpret alerts and validate automated responses. Salem et al. (2024) suggest that integrating explainable AI into intrusion detection will improve user confidence, regulatory compliance, and operational decision-making by providing interpretable reasoning behind threat classifications. This development is expected to facilitate greater collaboration between automated AI systems and human cybersecurity professionals.

Collectively, the reviewed literature demonstrates that AI-driven intrusion detection systems represent a transformative advancement in cybersecurity by combining intelligent data analysis, adaptive learning, and automated threat detection. Machine learning, deep learning, hybrid AI models, and predictive analytics collectively improve the capability of IDS to detect sophisticated attacks across enterprise networks, cloud platforms, IoT ecosystems, host environments, and critical infrastructure (Sunkara, 2022; Rai et al., 2025). However, realizing the full potential of AI-enabled cybersecurity requires continued research addressing adversarial robustness, explainability, computational efficiency, privacy preservation, and scalable deployment architectures. Future innovations that integrate predictive intelligence, autonomous response mechanisms, and trustworthy AI frameworks are expected to further strengthen intrusion detection systems and enhance cyber resilience against increasingly complex and evolving threat landscapes.

Conclusion

Artificial Intelligence (AI)-driven Intrusion Detection Systems (IDS) have become a fundamental component of modern cybersecurity by providing intelligent, adaptive, and scalable mechanisms for identifying increasingly sophisticated cyber threats. Unlike traditional signature-based intrusion detection approaches, AI-powered IDS leverage machine learning, deep learning, neural networks, and hybrid analytical models to detect both known and previously unseen attacks with greater accuracy and speed. This capability enables organizations to strengthen their security posture while reducing response times and improving the overall resilience of digital infrastructures (Chauhan & Mekala, 2019; Salem et al., 2024).

The review demonstrates that AI-driven intrusion detection systems have significantly improved threat detection across diverse environments, including enterprise networks, cloud computing platforms, Internet of Things (IoT) ecosystems, host-based systems, distributed application programming interfaces (APIs), and critical infrastructure. Intelligent detection models continuously learn from evolving network behavior, allowing them to identify anomalies that conventional security solutions may overlook. The integration of AI techniques into cybersecurity has also

enhanced automated threat analysis, adaptive defense mechanisms, and real-time monitoring capabilities, making IDS more effective against advanced persistent threats, malware, distributed denial-of-service attacks, insider threats, and zero-day exploits (Sunkara, 2022; Kamadi, 2022; Nay, 2024; Khalaf et al., 2025).

The analysis further indicates that supervised, unsupervised, and hybrid machine learning models each contribute unique strengths to intrusion detection depending on data availability and operational requirements. Deep learning architectures have demonstrated remarkable effectiveness in recognizing complex attack patterns, while hybrid AI approaches combine multiple algorithms to improve detection accuracy and reduce false positives. These advancements have enabled cybersecurity systems to evolve from reactive monitoring tools into proactive defense platforms capable of predicting and mitigating emerging threats before significant damage occurs (Markevych & Dawson, 2023; Khan et al., 2024; Goswami, 2024).

Despite these advancements, several challenges continue to influence the practical deployment of AI-driven IDS. High computational requirements, adversarial machine learning attacks, model interpretability, data privacy concerns, imbalanced training datasets, and the continuous evolution of cyber threats remain important obstacles to widespread implementation. Furthermore, maintaining detection accuracy while minimizing false alarms and ensuring scalability across heterogeneous computing environments requires continuous model refinement and robust security governance (Madupati, 2024; Raja, 2025).

Overall, AI-driven intrusion detection systems represent a transformative advancement in cybersecurity by combining intelligent analytics with adaptive learning to improve threat detection, incident response, and network resilience. As organizations increasingly adopt digital transformation initiatives, cloud services, edge computing, and interconnected IoT environments, AI-enabled IDS will continue to play an essential role in protecting critical information assets and supporting proactive cybersecurity strategies (Rehman et al., 2024; Wang & Xie, 2025; Rai et al., 2025).

Future Research

Future research should focus on developing more explainable and transparent AI models that improve the interpretability of intrusion detection decisions while maintaining high detection performance. Explainable Artificial Intelligence (XAI) can help build user trust, enable regulatory compliance, and assist cybersecurity analysts in making sense of the findings of complex detections (Salem et al., 2024).

Another area of research is enhancing the adversarial machine learning attacks that aim to fool AI-based IDS systems. AI-powered cybersecurity solutions will be more reliable if strong learning algorithms are developed that can effectively withstand data poisoning, model evasion, and adversarial perturbations (Raja, 2025; Madupati, 2024).

With the rise in cloud, edge and IoT technologies too, lightweight and distributed intrusion detection frameworks are becoming a reality. The federated learning, edge AI, and collaborative intelligence models, which allow for privacy-preserving learning and real-time threat detection in decentralized environments, should be explored in future studies (Nay, 2024; Wang & Xie, 2025).

Other research is required to develop predictive cybersecurity models that are able to detect attack indicators prior to security events. The combination of behavioral analytics, threat intelligence, and predictive machine learning algorithms can greatly improve proactive cyber-defense efforts and minimize the risk of an organization being exposed to new attack vectors (Al Abdulwahid, 2025).

Furthermore, future research is needed on the integration of AI-based IDS, ZTA, Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR) and Autonomous Cyber Defense. This integration can enhance automated decision-making, incident response coordination, and adaptable security management within ever-evolving enterprise settings (Khalaf et al., 2025; Rai et al., 2025).

Lastly, a common set of benchmark datasets, evaluation frameworks, and performance metrics will enable fair comparisons of AI-based intrusion detection methods. To create secure, scalable, trustworthy, and resilient intrusion detection systems that can tackle the ever-changing face of cybersecurity, continued interdisciplinary collaboration between cybersecurity researchers, AI experts, industry practitioners, and policymakers will be crucial (Chauhan & Mekala, 2019; Markevych & Dawson, 2023; Khan et al., 2024; Goswami, 2024).

References

[1] Chauhan, G. S., & Mekala, R. (2019). AI-driven intrusion detection systems: Enhancing cybersecurity with machine learning algorithms. *International Journal of Multidisciplinary and Current Research*, *7*(2), 131-139.

[2] Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data*, *11*(1), 105.

[3] Markevych, M., & Dawson, M. (2023, June). A review of enhancing intrusion detection systems for cybersecurity using artificial intelligence (ai). In *International conference knowledge-based organization* (Vol. 29, No. 3, pp. 30-37).

[4] Nay, T. (2024). Enhancing iot security with ai-driven hybrid machine learning and neural network-based intrusion detection system. *Babylonian Journal of Artificial Intelligence*, *2024*, 158-167.

[5] Khan, M. I., Arif, A., & Khan, A. R. A. (2024). AI-driven threat detection: a brief overview of AI techniques in cybersecurity. *BIN: Bulletin of Informatics*, *2*(2), 248-61.

[6] Sunkara, G. (2022). AI-driven cybersecurity: Advancing intelligent threat detection and adaptive network security in the era of sophisticated cyber attacks. *Well Testing Journal*, *31*(1), 185-198.

[7] Goswami, M. (2024). Enhancing network security with ai-driven intrusion detection systems. *International Journal of Open Publication and Exploration (IJOPE)*, *12*(1), 29-35.
[8] Kamadi, S. (2022). Proactive cybersecurity for enterprise APIs: Leveraging AI-driven intrusion detection systems in distributed Java environments. *IJRCAIT*, *5*(1), 34-52.
[9] Khalaf, N. Z., Barazanchi, A., Ibraheem, I., Radhi, A. D., Shah, P., & Sekhar, R. (2025). Development of real-time threat detection systems with AI-driven cybersecurity in critical infrastructure. *Mesopotamian Journal of CyberSecurity*, *5*(2), 501-513.
[10] Wang, F., & Xie, S. (2025). Cybersecurity in cloud computing ai-driven intrusion detection and mitigation strategies. *IEEE Access*, *13*, 108051-108058.
[11] Rehman, F., Mushtaq, F., & Zaman, H. (2024, October). A host-based intrusion detection: using signature-based and AI-driven anomaly detection for enhanced cybersecurity. In *2024 4th International Conference on Digital Futures and Transformative Technologies (ICoDT2)* (pp. 1-7). IEEE.
[12] Mukherjee, C. Ai-Driven Personalization of Power System Learning Modules Using Student Personas based on Behavioral Analysis of Grid Performance.
[13] Nadia, N. Y., Rabby, H. R., Arif, M. H., Tanvir, M. I. M., Ahmed, M., & Firdaus, S. (2025, October). Scalable RNN-Based Transfer Learning for Patient Sentiment Monitoring in Telehealth Platforms. In *2025 IEEE 2nd International Conference on Computing, Applications and Systems (COMPAS)* (pp. 1-6). IEEE.
[14] Takon, A. (2025). Explainable AI for Threat Modelling and Decision Support in Engineering Assets. *Journal of Cyber-Physical Security and Robotics*, *1*(02), 46-52.
[15] Mukherjee, C. (2025). Combating digital media piracy with agentic ai: Leveraging video transcription and character recognition for automated enforcement. *Authorea Preprints*.
[16] Anifowose, K. (2025). Development and Validation of AI-Assisted Analytical Methods for Biochemical Compound Detection in Pharmaceutical Chemistry. *Journal of Applied Pharmaceutical Sciences and Research*, *8*(4), 41-52.
[17] Mukherjee, C. (2025). Use of Agentic AI with OpenAI and Prompt Engineering and State-of-the Art Machine Learning Algorithm to detect the patterns in IOT Device Network Intrusion Attacks. *Authorea Preprints*.
[18] Ravikumar, V. (2025). Therapeutic Bot: Ethical Concerns in AI therapy for Neurodivergence. *J Int Scient Re Rep*.
[19] Mukherjee, C. (2025). Use of Agentic AI with LLM and Prompt Engineering and State-of-the Art Machine Learning Algorithm to detect the patterns in IOT Device Network Intrusion Attacks. *TechRxiv. August*, *6*.
[20] Takon, A. (2025). 3D Object Detection and Localization for Industrial Threat Monitoring. *Well Testing Journal*, *34*(S3), 850-880.
[21] Mukherjee, C. (2025). Harnessing large language models and ai agents for child behavior analytics in day care: a proof of concept for next-generation parental insight using simulated data. *Machinery and Production Engineering*, *174*(2870), 26-34.
[22] Mukherjee, C. (2025). Combating digital media piracy with agentic ai: Leveraging video transcription and character recognition for automated enforcement. *Authorea Preprints*.
[23] Mukherjee, C. (2026). AI-Based Detection of Deepfakes and Misinformation on Social Media. *Euro Vantage journals of Artificial intelligence*, *3*(2), 9-30.
[24] Anifowose, K. (2026). Advanced Chromatographic and Spectroscopic Method Development for Biomarker Identification and Validation in Clinical Biochemistry. *Journal of Drug Discovery and Health Sciences*, *3*(02), 1-8.
[25] Rai, H. M., Pal, A., Ergash o'g'li, R. A., Ugli, B. A. K., & Shokirovich, Y. S. (2025). Advanced AI-powered intrusion detection systems in cybersecurity protocols for network protection. *Procedia Computer Science*, *259*, 140-149.
[26] Madupati, B. (2024). AI-Driven Threat Detection in Cybersecurity. *J Artif Intell Mach Learn & Data Sci 2024*, *2*(2), 1163-1167.
[27] Al Abdulwahid, A. (2025). Ai-driven identification of attack precursors: A machine learning approach to predictive cybersecurity. *Computers, Materials & Continua*, *85*(1), 1751-1777.
[28] Al Kalach, N. (2025). AI-Driven Customer Relationship Management: Enhancing Salesforce Efficiency Through Predictive Analytics. *International Journal of Advance Industrial Engineering*, *13*(01), 22-35.
[29] Al Kalach, N. (2025). Salesforce Security Architecture for Zero-Trust, Encryption & Compliance. *Journal of Data Analysis and Critical Management*, *1*(04), 63-77.
[30] Khan, H. A. (2024). DATA-DRIVEN EPIDEMIOLOGICAL MODELING USING MACHINE LEARNING FOR DISEASE SPREAD FORECASTING AND PUBLIC HEALTH DECISION SUPPORT IN THE UNITED STATES. *International Journal of Applied Mathematics*, *37*(6s), 178-192.
[31] Ferdus, M. Z., Monsur, M. H., Akhtar, M. J., & Islam, S. (2024). Secured Auto Encryption and Authentication Process for Cloud Computing Security. *Valley International Journal Digital Library*, 1040-1044.
[32] Hossain, M. D., Kashem, M. A., Sadeq, M. J., Mustary, S., & Ferdus, M. Z. (2024, September). IoT Enabled Soil Fertilizer Monitoring and Recommendation System in the Context of Bangladeshi Agriculture. In *2024 IEEE International Conference on Power, Electrical, Electronics and Industrial Applications (PEEIACON)* (pp. 416-421). IEEE.
[33] Ferdus, M. Z., Anjum, N., Nguyen, T. N., Jisan, A. H., & Raju, M. A. H. (2024). The influence of social media on stock market: A transformer-based stock price forecasting with external factors. *Journal of Computer Science and Technology Studies*, *6*(1), 189-194.
[34] Arif, M. H. (2024). Optimizing Hospital Logistics and Healthcare Supply Chains Using Machine Learning and Artificial Intelligence Techniques. *J. Electrical Systems*, *20*(7s), 4209-4217.
[35] Goel, N. (2025). Federated Learning for Secure AI Models: Enhancing Privacy and Robustness in Decentralized Environments.
[36] Abul Kashem, M., Hossain, D., Hasan Shuvo, M., Mustary, S., Ferdus, M. Z., & Uddin, J. (2025). An Explainable AI-Based Crop Recommendation Framework Leveraging IoT-Driven Environmental Data.
[37] Ferdus, M. Z., Bhuiyan, R. J., Brydie, D., Monsur, M. H., Shafi, A. H., Sani, Z. U., ... & Tabassum CN, M. (2025). AI-Driven Predictive Analytics for Early Diagnosis and Healthcare Cost Reduction. *International Journal of Medical and Health Research*, *3*(4), 96-101.
[38] Goel, N. Privacy Risks and Protection in the Digital World of IoT. *Panamerican Mathematical Journal*, *33*(1), 2023.
[39] Verma, A. CONTINUOUS THREAT EXPOSURE MANAGEMENT (CTEM) WITHIN SASE FRAMEWORKS.
[40] Williams, M. O. (2024). DEVELOPMENT OF REACTIVE HEAT EXCHANGERS FOR ENHANCED GEOTHERMAL ENERGY RECOVERY. *Power System Protection and Control*, *52*(2), 18-37.
[41] Raja, M. S. R. S. (2025). The rise of ai-driven network intrusion detection systems: Innovations, challenges, and future directions. *International Journal of AI, BigData, Computational and Management Studies*, *6*(1), 1-9.