ISSN: 2455-6203
International Journal of Science Management & Engineering Research (IJSMER)
Volume: 10 | Issue: 01 | March - 2025 www.ejournal.rems.co.in
Date of Submission: 28/02/2025 Date of Acceptance: 15/11/2024 Date of Publish: 25/03/2025

AI-Based Intrusion Detection Systems for Network Security: A Review

[1]Monika Thakur, [2]Akanksha Jain, , [3]Saleha Khan, [4]Dr. Prashant Sen
[12&3] Research Scholar, Department of Computer Science & Engineering,
Eklavya University, Damoh, Madhya Pradesh
[4]Associate Professor & Head, Department of Computer Science & Engineering,
Eklavya University, Damoh, Madhya Pradesh

Abstract

The rapid increase in cyber threats and sophisticated attacks necessitates the development of advanced security mechanisms to safeguard networks. Traditional Intrusion Detection Systems (IDS) rely on signature-based and anomaly-based approaches, which often struggle with detecting new and evolving threats. AI-based IDS leverage Machine Learning (ML) and Deep Learning (DL) algorithms to enhance the detection of malicious activities, improve adaptability, and reduce false positives. This review provides a comprehensive analysis of AI-driven IDS, covering various methodologies such as supervised learning, unsupervised learning, and deep learning-based approaches. It also explores commonly used datasets, evaluation metrics, and the advantages of AI-driven detection mechanisms over traditional methods. Despite significant progress, AI-based IDS face challenges such as high false positive rates, adversarial attacks, scalability issues, and concept drift. We also discuss future research directions, including federated learning, explainable AI, hybrid models, and edge computing-based IDS, which can further improve the security and efficiency of intrusion detection systems. This review aims to serve as a valuable resource for researchers and practitioners in network security, highlighting the potential of AI-based IDS in mitigating cyber threats effectively.

Keywords: Intrusion Detection System (IDS), Cyber security, Deep Learning (DL), Machine Learning (ML), Cyber Threats, Supervised, Unsupervised, and reinforcement learning.

1. Introduction

With the increasing dependence on digital infrastructure, cyber threats have become more sophisticated, posing significant risks to governments, businesses, and individuals. Network security is crucial for protecting sensitive information and ensuring the integrity of data exchanges. One of the key components of network security is an Intrusion Detection System (IDS)**,** monitors which and analyzes network traffic to identify malicious activities.

Traditional IDS are primarily classified into **s**ignature-based IDS and anomaly-based IDS. Signature-based IDS relies on known attack patterns and is effective against previously identified threats. However,

ISSN: 2455-6203
International Journal of Science Management & Engineering Research (IJSMER)
Volume: 10 | Issue: 01 | March - 2025 www.ejournal.rems.co.in
Date of Submission: 28/02/2025 Date of Acceptance: 15/11/2024 Date of Publish: 25/03/2025

it struggles with detecting zero-day attacks—new and unknown vulnerabilities exploited by attackers (Buczak & Guven, 2016). Anomaly-based IDS, on the other hand, uses statistical and behavioral analysis to detect deviations from normal network behavior. While this approach enhances detection of unknown threats, it also results in high false positive rates.

To overcome these limitations, AI-driven IDS have gained prominence. Machine Learning (ML) and Deep Learning (DL) techniques enable IDS to learn from network traffic patterns, adapt to new attack strategies, and improve detection accuracy (Gao et al., 2020). Unlike traditional IDS, AI-based IDS can dynamically identify anomalies, reducing dependence on predefined attack signatures. These systems employ supervised, unsupervised, and reinforcement learning techniques to classify network activities as benign or malicious.

The key advantages of AI-based IDS include:

- **Enhanced detection accuracy** – AI models can analyze vast amounts of network data and recognize complex attack patterns.
- **Reduced false positives** – AI-based methods minimize the occurrence of false alarms compared to traditional anomaly detection systems.
- **Adaptability to evolving threats** – AI models can be trained continuously to adapt to new attack strategies.
- **Automated threat detection** – AI-driven IDS reduce the need for manual intervention, improving operational efficiency.

Despite these benefits, AI-based IDS face several challenges, including scalability issues, adversarial attacks, and the need for large labeled datasets. Additionally, the computational complexity of deep learning models can hinder real-time intrusion detection.

This review explores the methodologies, datasets, evaluation metrics, challenges, and future research directions of AI-based IDS. We aim to provide a comprehensive understanding of how AI can revolutionize network security and improve the effectiveness of intrusion detection systems.

2. Types of Intrusion Detection Systems

Intrusion Detection Systems (IDS) are broadly classified into three categories based on their monitoring scope and detection mechanisms:

2.1 Host-Based Intrusion Detection Systems (HIDS)

ISSN: 2455-6203
International Journal of Science Management & Engineering Research (IJSMER)
Volume: 10 | Issue: 01 | March - 2025 www.ejournal.rems.co.in
Date of Submission: 28/02/2025 Date of Acceptance: 15/11/2024 Date of Publish: 25/03/2025

- HIDS operate on individual hosts or devices, monitoring system logs, file integrity, application activity, and unauthorized modifications.
- They provide granular security insights but may lack visibility into network-wide threats.
- Example: OSSEC (Open Source HIDS), Tripwire.

2.2 Network-Based Intrusion Detection Systems (NIDS)

- NIDS analyze network traffic at various points in a network, inspecting packet payloads and headers to identify suspicious activities.
- They can detect external attacks such as Denial-of-Service (DoS), port scanning, and network reconnaissance.
- Example: Snort, Suricata, Zeek (formerly Bro).

2.3 Hybrid Intrusion Detection Systems

- Hybrid IDS combine HIDS and NIDS capabilities, providing a holistic approach to threat detection.
- They leverage both network traffic analysis and host-level monitoring to improve detection accuracy and response time.
- Example: OSSEC combined with Snort, Security Information and Event Management (SIEM) solutions like Splunk and IBM QRadar.

2.4 Anomaly-Based IDS

- Anomaly-based IDS use AI/ML algorithms to detect deviations from normal behavior in network traffic or system activities.
- They are effective in identifying zero-day attacks but may suffer from high false positive rates.
- Example: AI-driven IDS solutions in modern SIEM platforms.

2.5 Signature-Based IDS

- These systems detect known attack patterns using predefined signatures, similar to antivirus databases.
- They are highly efficient against known threats but ineffective against novel or evolving cyberattacks.
- Example: Traditional IDS modules in Snort and Suricata.

2.6 Behavior-Based IDS

- Behavior-based IDS continuously analyze user and entity behavior to identify malicious activities.
- They utilize User and Entity Behavior Analytics (UEBA) for threat detection in enterprise environments.
- Example: IBM QRadar, Microsoft Defender for Endpoint.

By integrating AI and machine learning techniques, modern IDS solutions enhance the detection capabilities of these systems, making them more effective against evolving cyber threats.

ISSN: 2455-6203
International Journal of Science Management & Engineering Research (IJSMER)
Volume: 10 | Issue: 01 | March - 2025 www.ejournal.rems.co.in
Date of Submission: 28/02/2025 Date of Acceptance: 15/11/2024 Date of Publish: 25/03/2025

3. Machine Learning Techniques in IDS

Machine Learning techniques are widely employed in IDS to improve detection capabilities. The key ML techniques used in IDS are as follows:

3.1. Supervised Learning

Supervised learning requires labeled datasets for training models to classify network activities as normal or malicious.

- **Support Vector Machines (SVM)**: Used for binary classification, effective in detecting attack patterns (Wang et al., 2018).
- **Decision Trees (DT)**: A rule-based approach that provides interpretable classification of threats (Zhang et al., 2019).
- **Random Forest (RF)**: An ensemble method that improves accuracy by combining multiple decision trees (Kumar et al., 2021).
- **Artificial Neural Networks (ANN)**: Multi-layered networks that learn complex attack patterns for intrusion detection.

3.2. Unsupervised Learning

Unsupervised learning does not require labeled data and is useful for detecting novel attacks.

- **K-Means Clustering**: Groups similar network behaviors, identifying outliers as potential threats (Aminanto & Kim, 2018).
- **Autoencoders**: Neural networks trained to reconstruct normal traffic, detecting anomalies as deviations (Shone et al., 2018).
- **Principal Component Analysis (PCA)**: Reduces dimensionality to identify unusual patterns in network traffic.

3.3. Deep Learning Approaches

Deep Learning models extract high-level features from network traffic to improve detection accuracy.

- **Convolutional Neural Networks (CNN)**: Applied to IDS for feature extraction from packet data (Javaid et al., 2016).
- **Recurrent Neural Networks (RNN)**: Suitable for analyzing sequential network traffic data (Kim et al., 2020).
- **Long Short-Term Memory (LSTM) Networks**: Specialized RNNs that learn temporal dependencies in attack patterns (Tang et al., 2019).
- **Generative Adversarial Networks (GANs)**: Used for adversarial training to detect sophisticated cyber threats.

ISSN: 2455-6203
International Journal of Science Management & Engineering Research (IJSMER)
Volume: 10 | Issue: 01 | March - 2025 www.ejournal.rems.co.in
Date of Submission: 28/02/2025 Date of Acceptance: 15/11/2024 Date of Publish: 25/03/2025

By leveraging these techniques, AI-based IDS enhance cybersecurity, improving threat detection while reducing false positives.

4. Datasets for AI-Based IDS

The effectiveness of AI-based IDS largely depends on the availability of high-quality datasets for training and evaluation. Several benchmark datasets have been used in intrusion detection research to assess the performance of different AI models. Below are some of the most commonly used datasets:

1. KDD Cup 1999

- One of the earliest and most widely used IDS datasets, created for the **KDD Cup 1999** competition.
- Contains **4.9 million records** of network traffic, categorized into **normal** and **attack types** (e.g., DoS, Probe, R2L, U2R).
- Despite its extensive use, it has **redundancy issues**, making it less suitable for modern IDS research.

2. NSL-KDD

- An improved version of **KDD'99**, addressing data redundancy and bias.
- Features **balanced class distribution**, making it more suitable for ML model evaluation.
- Still criticized for not representing modern network traffic accurately.

3. CICIDS2017

- Developed by the **Canadian Institute for Cybersecurity (CIC)**, this dataset contains realistic attack scenarios.
- Includes diverse attack types such as **DDoS, Brute Force, Botnet, Web attacks**, and **Infiltration**.
- Features **labeled data with over 80 network traffic attributes**, making it one of the most comprehensive datasets.

4. UNSW-NB15

- Created by the **Australian Centre for Cyber Security (ACCS)** to overcome the limitations of KDD datasets.
- Contains **normal and attack traffic**, generated using a real network environment.
- Offers a wide range of **network flow-based features**, making it suitable for modern IDS evaluations.

5. TON_IoT

- A modern dataset designed for **Intrusion Detection in IoT environments**.
- Covers **network traffic, telemetry data, and system logs**, enabling the evaluation of IoT security threats.
- Provides insights into **real-time cyber-physical system security**.

ISSN: 2455-6203
International Journal of Science Management & Engineering Research (IJSMER)
Volume: 10 | Issue: 01 | March - 2025 www.ejournal.rems.co.in
Date of Submission: 28/02/2025 Date of Acceptance: 15/11/2024 Date of Publish: 25/03/2025

6. CSE-CIC-IDS2018

- An **extended version of CICIDS2017**, offering more attack scenarios.
- Includes **Windows and Linux traffic**, making it suitable for **cross-platform IDS evaluations**.
- Widely used for **deep learning-based IDS research**.

7. Bot-IoT

- Designed for **IoT security research**, addressing the increasing cyber threats in IoT networks.
- Contains a mix of **benign and attack traffic**, with attack types including **DDoS, Data Exfiltration, and Reconnaissance**.
- Helps evaluate the performance of AI-based IDS in **resource-constrained environments**.

8. IoT-23

- A recent dataset for **IoT-based intrusion detection**, containing **malicious and benign IoT network traffic**.
- Collected from various real-world IoT devices, providing realistic attack patterns.
- Supports **behavior-based intrusion detection research**.

These datasets play a critical role in benchmarking AI-based IDS models, allowing researchers to compare different methodologies effectively. The choice of dataset depends on the specific use case, network type, and attack scenario being analyzed.

5. Evaluation Metrics for AI-Based IDS

The performance of AI-based IDS is assessed using various evaluation metrics to measure detection accuracy, efficiency, and reliability. The most commonly used evaluation metrics are:

1. Accuracy (ACC)

- Measures the overall correctness of the IDS model.
- Defined as: Accuracy = $\frac{TP+TN}{TP+TN+FP+FN}$

where TP = True Positives, TN = True Negatives, FP = False Positives, and FN = False Negatives.

- High accuracy indicates that the IDS correctly distinguish between normal and malicious traffic.

2. Precision (Positive Predictive Value - PPV)

- Measures how many of the instances classified as attacks are actual attacks.
- Defined as: Precision = $\frac{TP}{TP+FP}$
- A high precision score means fewer false positives.

ISSN: 2455-6203
International Journal of Science Management & Engineering Research (IJSMER)
Volume: 10 | Issue: 01 | March - 2025 www.ejournal.rems.co.in
Date of Submission: 28/02/2025 Date of Acceptance: 15/11/2024 Date of Publish: 25/03/2025

3. Recall (True Positive Rate - TPR, Sensitivity)

- Measures how well the IDS detect actual attacks.
- Defined as: Recall = $\frac{TP}{TP+FN}$
- High recall ensures that most attacks are detected, but it must be balanced with precision to reduce false alarms.

4. F1-Score

- A harmonic mean of precision and recall, providing a balanced measure of model performance.
- Defined as: F1 = 2 X $\frac{\text{Precision x Recall}}{\text{Precision+ Recall}}$
- Useful when the dataset is imbalanced, as it considers both false positives and false negatives.

5. False Positive Rate (FPR)

- Measures how often normal traffic is incorrectly classified as an attack.
- Defined as: FPR = $\frac{FP}{FP+TN}$
- A lower FPR is desirable to minimize false alarms.

6. False Negative Rate (FNR)

- Measures the proportion of actual attacks missed by the IDS.
- Defined as: FNR = $\frac{FN}{FN+TP}$
- A lower FNR is crucial for ensuring no attacks go undetected.

7. Receiver Operating Characteristic (ROC) Curve & Area Under the Curve (AUC)

- ROC curve plots TPR against FPR, showing the trade-off between detection rate and false positives.
- **AUC** measures the area under the ROC curve, with a higher AUC indicating better performance.

8. Matthews Correlation Coefficient (MCC)

- A more balanced metric for evaluating classification performance, especially with imbalanced datasets.
- Defined as: MCC = $\frac{(TP\ X\ TN)-(FP\ X\ FN)}{\sqrt{(TP+FP)(TP+FN)(TN+FP(TN+FN)}}$
- Ranges from -1 (worst) to +1 (best), with 0 indicating random classification.

9. Detection Rate (DR)

- Measures the ability of the IDS to correctly identify intrusions.
- Defined as: DR =$\frac{TP}{TP+FN}$
- A higher detection rate indicates better intrusion detection capabilities.

ISSN: 2455-6203
International Journal of Science Management & Engineering Research (IJSMER)
Volume: 10 | Issue: 01 | March - 2025 www.ejournal.rems.co.in
Date of Submission: 28/02/2025 Date of Acceptance: 15/11/2024 Date of Publish: 25/03/2025

10. Computational Efficiency (Time Complexity)

- Measures the processing time required for the IDS to analyze network traffic.
- Important for real-time IDS where quick threat detection is required.

11. Scalability and Robustness Metrics

- Evaluate the performance of the IDS in handling large-scale network traffic and unknown attack variations.
- Includes factors like adaptability to new attack patterns and performance degradation over time.

By using these evaluation metrics, researchers and security analysts can assess the strengths and weaknesses of AI-based IDS models and optimize them for better performance in real-world network security applications.

Conclusion

AI-based Intrusion Detection Systems (IDS) represent a significant advancement in network security, offering improved detection accuracy, adaptability, and automation over traditional methods. By leveraging Machine Learning (ML) and Deep Learning (DL) techniques, IDS can identify complex attack patterns, detect zero-day vulnerabilities, and enhance cybersecurity defenses.

Despite their advantages, AI-based IDS face several challenges, including high false positive rates, adversarial attacks, and computational complexity. The reliance on high-quality labeled datasets for training remains a limitation, necessitating the development of more robust, self-learning models capable of adapting to evolving threats. Additionally, issues such as explainability and transparency in AI decision-making require further research to ensure trust and reliability in security applications.

Future research in AI-driven IDS should focus on developing hybrid models that combine signature-based, anomaly-based, and behavior-based detection approaches. Technologies like federated learning can enhance IDS efficiency while preserving data privacy, and explainable AI (XAI) can improve the interpretability of AI decisions. Furthermore, advancements in edge computing can enable real-time threat detection without the need for extensive cloud-based processing.

In conclusion, AI-powered IDS have the potential to revolutionize network security by improving real-time threat detection and response. However, continuous innovation and research are required to overcome current limitations and ensure robust, scalable, and interpretable AI-driven cybersecurity solutions. By addressing these challenges, AI-based IDS can significantly strengthen the defense mechanisms of modern digital infrastructures against sophisticated cyber threats.

ISSN: 2455-6203
International Journal of Science Management & Engineering Research (IJSMER)
Volume: 10 | Issue: 01 | March - 2025 www.ejournal.rems.co.in
Date of Submission: 28/02/2025 Date of Acceptance: 15/11/2024 Date of Publish: 25/03/2025

References

1. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cybersecurity intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153-1176.

2. Gao, J., Liu, Z., & Dai, Y. (2020). An overview of machine learning-based intrusion detection technology. *Future Internet, 12*(9), 156.

3. Wang, J., Lu, P., & Zhang, H. (2018). An efficient intrusion detection model based on machine learning. *Computers & Security, 78*, 1-13.

4. Zhang, C., Luo, J., & Liu, P. (2019). Deep learning-based anomaly detection in network traffic. *IEEE Transactions on Network and Service Management, 16*(3), 1031-1042.

5. Kumar, R., Raj, J., & Singh, A. (2021). A hybrid IDS model using machine learning techniques. *Journal of Cyber Security and Mobility, 10*(1), 1-20.

6. Aminanto, M. E., & Kim, K. (2018). Deep learning in intrusion detection system: A comprehensive review. *Journal of Information Security and Applications, 41*, 79-98.

7. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence, 2*(1), 41-50.

8. Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system. *EAI Endorsed Transactions on Security and Safety, 3*(9), e2.

9. Kim, T., Won, D., & Lee, S. (2020). LSTM-based anomaly detection for network security. *IEEE Transactions on Information Forensics and Security, 15*, 2598-2612.

10. Tang, T., Li, J., & Zhang, X. (2019). An LSTM-based model for network anomaly detection. *Security and Communication Networks, 2019*, 1-10.

11. Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology (TIST), 10*(2), 1-19.