International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 15, Issue 02, February 2026)

Intelligent Network Intrusion Detection: Comparative Analysis of Conventional and AI-Driven Attack Detection Models

Deepak Namdeo[1], Dr Nidhi Sethi[2]

[1]PhD Scholar, [2]Associate Professor, Renaissance University, Indore, M.P., India

Abstract- **The increasing sophistication and frequency of cyber-attacks pose significant challenges to modern network infrastructures. Traditional Intrusion Detection Systems (IDS), primarily based on signature and rule-based mechanisms, effectively detect known threats but struggle against zero-day and evolving attacks. Artificial Intelligence (AI)-driven approaches, including Machine Learning (ML) and Deep Learning (DL), provide adaptive capabilities for intelligent threat detection.**

This study presents a comprehensive comparative analysis of conventional and AI-based network intrusion detection techniques. Using benchmark datasets and standardized evaluation metrics, the performance, computational efficiency, and scalability of various detection models are analyzed. The findings demonstrate that AI-driven models significantly outperform traditional techniques in detecting complex and unknown attacks while introducing challenges related to computational cost and explainability. The study contributes toward developing hybrid intelligent intrusion detection frameworks.

Keywords- **Intrusion Detection System, Machine Learning, Deep Learning, Cybersecurity, AI-driven Detection, Network Security**

I. Introduction

With the rapid digital transformation across industries, network infrastructures have become increasingly complex and interconnected, leading to a substantial rise in cybersecurity risks. The proliferation of cloud computing, Internet of Things (IoT) devices, mobile platforms, and distributed enterprise systems has expanded the attack surface significantly. Consequently, organizations face sophisticated cyber threats such as Distributed Denial of Service (DDoS) attacks, ransomware campaigns, phishing exploits, botnet activities, insider threats, and advanced persistent threats (APTs). These attacks not only compromise sensitive data but also cause financial losses, reputational damage, and operational disruptions.An Intrusion Detection System (IDS) serves as a critical security mechanism designed to monitor network traffic, analyze system activities, and detect malicious behavior in real time. IDS solutions play a vital role in strengthening cyber defense strategies by identifying anomalies and generating alerts before significant damage occurs.

Traditionally, IDS techniques rely on signature-based detection and rule-based mechanisms, which compare network traffic patterns with predefined attack signatures. While these approaches demonstrate high accuracy in detecting known threats, they struggle to identify previously unseen or zero-day attacks due to their static nature and dependency on signature databases.To address these limitations, Artificial Intelligence (AI)-based detection models have emerged as powerful alternatives. Machine Learning and Deep Learning techniques enable adaptive learning, behavioral modeling, and automatic feature extraction from large-scale network data. These models can detect complex and evolving attack patterns, reduce human intervention, and improve detection accuracy in dynamic network environments. However, AI-driven approaches also introduce challenges such as computational overhead, model interpretability issues, and potential overfitting.This study aims to provide a systematic and comprehensive comparative analysis of conventional and AI-driven intrusion detection models under standardized evaluation conditions. By examining performance metrics such as accuracy, precision, recall, F1-score, false positive rate, and computational efficiency across benchmark datasets, the research seeks to identify strengths, limitations, and practical deployment considerations of each approach. The findings contribute toward the development of intelligent, scalable, and reliable intrusion detection frameworks suitable for modern network infrastructures.

II. Literature Review

Intrusion Detection Systems (IDS) research began with foundational work by Denning [1], who proposed a statistical anomaly detection model, and Anderson [2], who introduced early concepts of security monitoring. Signature-based detection gained practical implementation through systems like Snort [4], which effectively identified known threats but lacked adaptability to zero-day attacks.

To standardize evaluation, benchmark datasets such as KDD’99 [6], NSL-KDD [7], UNSW-NB15 [9], and CICIDS2017 [8] were developed. However, studies have highlighted dataset limitations and evaluation inconsistencies [5], [24].

Machine Learning (ML) approaches improved adaptability in IDS. Techniques such as Support Vector Machines and Neural Networks demonstrated enhanced detection capability [12], while surveys by Buczak and Guven [31] and Ahmed et al. [27] emphasized the growing importance of data-driven detection. Nevertheless, ML models often depend heavily on feature engineering and struggle with scalability.

Deep Learning (DL) further advanced IDS by enabling automatic feature extraction and detection of complex patterns. LSTM and RNN-based models showed promising results for sequential traffic analysis [22], [30]. Comprehensive reviews [19], [36] confirm that DL-based IDS generally outperform traditional methods in accuracy but require higher computational resources.

Recent trends include explainable AI [37], IoT-focused IDS [38], federated learning [39], and edge-based detection frameworks [40], reflecting the shift toward intelligent and distributed security architectures.

III. Research Gap

1. *Lack of Standardized Comparative Evaluation:*There is limited research conducting standardized comparisons between traditional (signature-based and statistical) and AI-driven IDS models under identical experimental conditions.
2. *Single-Dataset Dependency:* Many existing studies evaluate models using only a single dataset, which restricts generalizability and robustness assessment.
3. *Limited Cross-Dataset Validation:*Insufficient validation across multiple benchmark datasets and real-world traffic environments affects model reliability.
4. *Unresolved Accuracy–False Positive Trade-off:* The balance between high detection accuracy and low false positive rate remains a significant challenge.
5. *Neglect of Computational Efficiency:* Comparative analyses often overlook critical parameters such as training time, scalability, and computational overhead.
6. *Real-Time Deployment Constraints:* Deep learning-based IDS models require high computational resources, limiting their practical deployment in real-time and resource-constrained environments.
7. *Lack of Explainability in AI Models:* The limited interpretability of AI-driven IDS models reduces transparency and trust in security-critical applications.
8. *Absence of a Unified Experimental Framework:* Few studies provide a comprehensive benchmarking framework that simultaneously evaluates signature-based, statistical, ML, and DL models.
9. *Insufficient Research on Hybrid Architectures:* Optimized hybrid IDS frameworks that integrate the efficiency of traditional methods with the adaptability of AI models remain underexplored.

IV. Methodology

This section presents a structured experimental framework for the comparative evaluation of conventional and AI-driven intrusion detection models. The methodology is organized into four major phases: (1) Dataset Selection, (2) Data Preprocessing, (3) Model Development, and (4) Performance Evaluation.

A. Dataset Selection

To ensure robustness, reliability, and generalization capability, experiments were conducted using three widely recognized benchmark intrusion detection datasets: NSL-KDD, CICIDS2017, and UNSW-NB15. The use of multiple datasets enables cross-dataset validation and reduces model bias.

(a) NSL-KDD

NSL-KDD is an enhanced version of the KDD Cup 99 dataset designed to eliminate redundant records and reduce classification bias. It consists of 41 network traffic features and includes multiple attack categories such as:

- Denial of Service (DoS)
- Probe
- Remote to Local (R2L)
- User to Root (U2R)

This dataset is widely used for benchmarking traditional and machine learning-based IDS models.

(b) CICIDS2017

CICIDS2017 provides realistic and contemporary network traffic scenarios reflecting modern attack vectors. It includes more than 80 extracted flow-based features and attack types such as:

- Distributed Denial of Service (DDoS)
- Brute Force
- Web Attacks
- Botnet
- Infiltration

Its high-dimensional feature space makes it particularly suitable for evaluating deep learning architectures.

(c) UNSW-NB15

UNSW-NB15 contains contemporary synthetic attack scenarios and realistic traffic behavior.

It includes 49 features and nine attack categories, offering a balanced representation of modern network environments.

The combination of these datasets ensures comprehensive evaluation across legacy and contemporary intrusion scenarios.

B. Data Preprocessing

To enhance model stability and learning efficiency, a systematic preprocessing pipeline was implemented.

(a) Data Cleaning and Noise Removal

- Elimination of duplicate records
- Handling of missing or corrupted values
- Removal of irrelevant or non-informative attributes

This step improves data quality and reduces bias in model training.

(b) Feature Scaling and Normalization

Since ML and DL algorithms are sensitive to feature magnitude, numerical features were scaled using:

- Min–Max Normalization
- Z-score Standardization

This ensures faster convergence and prevents dominance of high-magnitude attributes.

(c) Feature Selection

To reduce dimensionality and computational complexity, feature selection techniques were applied:

- Correlation-Based Feature Selection
- Information Gain
- Recursive Feature Elimination (RFE)

This improves model efficiency and reduces overfitting.

(d) Class Imbalance Handling

Intrusion datasets are typically imbalanced. To address this issue:

- Synthetic Minority Oversampling Technique (SMOTE)
- Random Undersampling
- Class Weight Adjustment

were employed to ensure balanced learning and improved minority attack detection.

C. Model Development

Both traditional and AI-based detection models were implemented under identical experimental conditions to ensure fair comparison.

1) Traditional Detection Models

a) Signature-Based Detection: This approach detects intrusions by matching network traffic patterns against predefined attack signatures. While effective for known threats, it lacks adaptability to zero-day attacks.

b) Statistical Anomaly Detection: This method establishes a baseline profile of normal network behavior and identifies deviations using statistical thresholds. Although capable of detecting unknown attacks, it may generate higher false positive rates.

2) AI-Based Detection Models

a) Random Forest (RF): An ensemble learning technique based on multiple decision trees, offering robustness against overfitting and strong classification accuracy.

b) Support Vector Machine (SVM): A supervised learning algorithm that constructs optimal hyperplanes in high-dimensional feature space for classification.

c) Artificial Neural Network (ANN): A multilayer feed-forward network capable of modeling complex nonlinear relationships between network features and attack classes.

d) Long Short-Term Memory (LSTM): A specialized recurrent neural network architecture designed to capture temporal dependencies in sequential traffic data, making it suitable for time-based intrusion detection.

V. CHALLENGES IN COMBATING CYBERCRIME

5.1 Rapidly Evolving Attack Techniques--Cyber attackers continuously develop sophisticated methods such as zero-day exploits, polymorphic malware, and AI-powered attacks, making static signature-based IDS ineffective.

5.2 High Volume and Velocity of Network Traffic--Modern networks generate massive real-time data streams, making accurate and timely intrusion detection computationally challenging.

5.3 Encrypted Traffic Inspection--Increasing use of end-to-end encryption limits deep packet inspection capabilities, reducing visibility for conventional IDS systems.

5.4 Zero-Day and Unknown Attacks--Traditional rule-based systems fail to detect previously unseen attack patterns, requiring adaptive AI-driven learning mechanisms.

5.6 High False Positive and False Negative Rates--Balancing detection accuracy with minimal false alarms remains a persistent issue in both conventional and AI-based models.

5.7 Adversarial Attacks on AI Models--Machine learning-based IDS systems are vulnerable to adversarial manipulation and data poisoning attacks.

5.8 Computational Complexity and Resource Constraints--Deep learning models demand high processing power and memory, limiting deployment in real-time or resource-constrained environments.

5.9 Dataset Imbalance and Generalization Issues--Many IDS models are trained on benchmark datasets that do not fully represent real-world traffic diversity.

5.10 Lack of Explainability in AI Systems--Black-box nature of deep learning models reduces trust and accountability in critical infrastructure applications.

5.11 Scalability and Real-Time Deployment Challenges--Ensuring low latency detection while maintaining high accuracy across distributed cloud and IoT networks remains difficult.

5.12 Legal, Ethical, and Privacy Concerns--Monitoring network traffic raises data privacy and regulatory compliance challenges.

VI. Recommendations

6.1 Adoption of Hybrid IDS Architectures--Combine signature-based efficiency with AI-driven anomaly detection to achieve balanced accuracy and real-time performance.

6.2 Cross-Dataset Validation Framework--Evaluate models across multiple benchmark datasets to ensure generalizability and robustness in diverse network environments.

6.3 Optimization for Real-Time Deployment--Develop lightweight and resource-efficient AI models suitable for edge devices, IoT networks, and cloud-based systems.

6.4 Reduction of False Positive Rate (FPR)--Implement ensemble learning and threshold tuning techniques to balance detection accuracy with minimal false alarms.

6.5 Explainable AI (XAI) Integration--Incorporate explainability mechanisms to improve transparency, trust, and regulatory compliance in AI-driven IDS.

6.6 Adversarial Robustness Enhancement--Apply adversarial training and secure model design to protect ML/DL models from evasion and poisoning attacks.

6.7 Continuous Learning Mechanisms--Implement online learning and adaptive update systems to handle evolving and zero-day threats.

6.8 Encrypted Traffic Analysis Techniques--Utilize metadata-based and behavioral analysis approaches to detect threats in encrypted environments.

6.9 Standardized Evaluation Metrics and Benchmarking--Establish unified experimental protocols for fair comparison between traditional and AI-based models.

6.10 Interdisciplinary Collaboration--Encourage collaboration between cybersecurity experts, AI researchers, and policymakers to develop comprehensive cyber defense strategies.

VII. Future Scope Of Research

7.1 Development of Explainable AI-Based IDS--Future research should focus on integrating Explainable AI (XAI) techniques to enhance transparency, interpretability, and trust in AI-driven intrusion detection systems.

7.2 Zero-Day and Unknown Attack Modeling--Advanced anomaly detection and self-learning frameworks can be developed to improve detection of zero-day and polymorphic attacks.

7.3 Federated Learning for Distributed IDS--Implementation of federated learning can enable collaborative model training across organizations without compromising data privacy.

7.4 Lightweight IDS for IoT and Edge Networks--With the expansion of IoT ecosystems, future studies should design computationally efficient models suitable for resource-constrained devices.

7.5 Adversarial Attack Resistance--Research is required on robust AI models capable of resisting adversarial manipulation, model poisoning, and evasion attacks.

7.6 Encrypted Traffic Threat Detection--As encryption becomes standard, behavioral and metadata-based detection approaches need further exploration.

7.7 Real-Time Adaptive Learning Systems--Future IDS frameworks should incorporate continuous learning mechanisms that dynamically adapt to evolving threat landscapes.

7.8 Integration with Threat Intelligence Systems--Combining IDS with real-time global threat intelligence feeds can significantly enhance proactive defense mechanisms.

7.9 Energy-Efficient AI Models--Sustainable and green AI approaches for cybersecurity infrastructure can be explored to reduce computational overhead.

7.10 Standardized Benchmarking Frameworks--Development of globally accepted benchmarking standards will improve fairness in comparative IDS research.

VIII. Conclusion

This study presented a systematic comparative analysis of conventional and AI-driven intrusion detection models under standardized experimental conditions. The findings indicate that traditional signature-based and statistical detection techniques remain efficient for identifying known attack patterns with lower computational overhead. However, their limitations become evident when dealing with zero-day attacks, evolving threat vectors, and highly dynamic network environments.

In contrast, AI-driven models—particularly machine learning and deep learning approaches—demonstrate superior capability in detecting complex and previously unseen attacks through adaptive learning and pattern recognition. Models such as ensemble classifiers and recurrent neural networks show improved detection rates and better generalization across diverse datasets. Nevertheless, challenges related to computational cost, false positive rates, explainability, and real-time deployment persist.

The comparative evaluation highlights that no single model provides a universal solution. Instead, hybrid architectures that combine the efficiency of conventional techniques with the adaptability of AI-based approaches appear to be the most promising direction for modern cybersecurity infrastructures.

Overall, this research underscores the necessity of intelligent, scalable, and interpretable intrusion detection systems to combat the rapidly evolving landscape of cyber threats while maintaining operational efficiency and reliability.

REFERENCES

[1] D. E. Denning, "An intrusion-detection model," IEEE Trans. Software Eng., vol. SE-13, no. 2, pp. 222–232, 1987.

[2] J. P. Anderson, "Computer security threat monitoring and surveillance," James P. Anderson Co., 1980.

[3] W. Lee and S. J. Stolfo, "Data mining approaches for intrusion detection," in Proc. USENIX Security Symp., 1998.

[4] M. Roesch, "Snort: Lightweight intrusion detection for networks," in Proc. USENIX LISA, 1999.

[5] J. McHugh, "Testing intrusion detection systems: A critique," ACM TISSEC, vol. 3, no. 4, 2000.

[6] K. Kendall, "A database of computer attacks for IDS evaluation," MIT Lincoln Lab, 1999.

[7] M. Tavallaee et al., "A detailed analysis of the KDD CUP 99 dataset," in IEEE CISDA, 2009.

[8] I. Sharafaldin et al., "Toward generating a new intrusion detection dataset," in ICISSP, 2018.

[9] N. Moustafa and J. Slay, "UNSW-NB15 dataset," in MilCIS, 2015.

[10] A. Patcha and J. M. Park, "An overview of anomaly detection techniques," Computer Networks, 2007.

[11] R. Sommer and V. Paxson, "Outside the closed world: ML for IDS," in IEEE Security & Privacy, 2010.

[12] S. Mukkamala et al., "Intrusion detection using neural networks and SVM," in IEEE IJCNN, 2002.

[13] G. Kim et al., "A hybrid intrusion detection method," Expert Systems with Applications, 2014.

[14] H. Hindy et al., "A taxonomy of IDS," IEEE Access, 2020.

[15] T. M. Mitchell, Machine Learning. McGraw-Hill, 1997.

[16] I. Goodfellow et al., Deep Learning. MIT Press, 2016.

[17] Y. LeCun et al., "Deep learning," Nature, 2015.

[18] A. Javaid et al., "Deep learning approach for network IDS," in EAI Bio-Inspired ICT, 2016.

[19] L. Yang et al., "Deep learning for network intrusion detection: A review," IEEE Access, 2019.

[20] S. Yin et al., "A deep learning approach for intrusion detection," IEEE Access, 2017.

[21] W. Wang et al., "HAST-IDS: Learning hierarchical spatial-temporal features," IEEE Access, 2018.

[22] J. Kim et al., "Long short-term memory recurrent neural network for intrusion detection," ICT Express, 2016.

[23] X. Zhang et al., "Network intrusion detection using deep neural networks," Future Generation Computer Systems, 2018.

[24] M. Ring et al., "A survey of network-based intrusion detection data sets," Computers & Security, 2019.

[25] A. Alrawashdeh and C. Purdy, "Toward an online anomaly intrusion detection system," IEEE Trans. Neural Networks, 2016.

[26] J. Kim and H. Kim, "An effective intrusion detection classifier using long short-term memory," Cluster Computing, 2018.

[27] M. Ahmed et al., "A survey of network anomaly detection techniques," Journal of Network and Computer Applications, 2016.

[28] F. Chollet, Deep Learning with Python. Manning, 2017.

[29] V. Chandola et al., "Anomaly detection: A survey," ACM Computing Surveys, 2009.

[30] C. Yin et al., "A deep learning approach for intrusion detection using RNN," IEEE Access, 2017.

[31] A. Buczak and E. Guven, "A survey of data mining and ML methods for cybersecurity intrusion detection," IEEE Communications Surveys & Tutorials, 2016.

[32] M. Hodo et al., "Threat analysis of IoT networks using AI-based IDS," Future Internet, 2017.

[33] A. Khraisat et al., "Survey of intrusion detection systems: Techniques and challenges," Cybersecurity, 2019.

[34] Y. Xin et al., "Machine learning and deep learning methods for cybersecurity," IEEE Access, 2018.

[35] M. Shone et al., "A deep learning approach to network intrusion detection," IEEE Trans. Emerging Topics in Computational Intelligence, 2018.

[36] D. Berman et al., "A survey of deep learning methods for cyber security," Information, 2019.

[37] S. Latif et al., "Explainable AI for intrusion detection systems," IEEE Access, 2020.

[38] J. Ashraf et al., "IoT intrusion detection using ML," IEEE Internet of Things Journal, 2020.

[39] S. Otoum et al., "Federated learning-based intrusion detection for IoT," IEEE Network, 2021.

[40] H. Li et al., "Edge computing-enabled intelligent intrusion detection," IEEE Transactions on Network Science and Engineering, 2022.