Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 4, 2026

AN INVESTIGATION INTO THE EFFECTIVENESS OF AI-BASED INTRUSION DETECTION SYSTEMS IN MODERN NETWORK ENVIRONMENTS

[1]Dr. Asim Shahzad
[1]Department of Software Engineering, Federal Urdu University, Islamabad
[1]drasim.shahzad@fuuast.edu.pk

Keywords
Artificial Intelligence, Intrusion Detection Systems, Network Security, Machine Learning, Cyber Threat Detection, Deep Learning, Anomaly Detection

Article History
Received on 30 March, 2026
Accepted on 27 April, 2026
Published on 28 April, 2026

Corresponding Author:

Abstract
The rapid growth of complex and distributed network environments has intensified the need for advanced security mechanisms capable of detecting sophisticated cyber threats. Traditional intrusion detection systems (IDS) often struggle to identify emerging and zero-day attacks due to their reliance on predefined signatures and limited adaptability. This study investigates the effectiveness of artificial intelligence (AI)-based intrusion detection systems in enhancing network security within modern infrastructures. It examines the application of machine learning and deep learning techniques, including supervised and unsupervised models, for real-time threat detection and classification. The research adopts a comparative analytical approach, evaluating AI-based IDS against conventional systems in terms of detection accuracy, false positive rates, scalability, and response time. Experimental findings indicate that AI-driven models significantly improve detection capabilities by identifying complex attack patterns and adapting to evolving threats. However, challenges such as high computational cost, data imbalance, and model interpretability remain critical concerns. The study highlights the potential of integrating AI with hybrid detection frameworks to achieve more robust and efficient security solutions. Overall, the research contributes to the ongoing development of intelligent cyber-security systems by providing insights into the practical effectiveness and limitations of AI-based IDS in contemporary network environments.

1. Introduction

The increasing reliance on digital infrastructures has made network security a critical area of research in computer science and information technology. Intrusion Detection Systems (IDS) play a vital role in identifying unauthorized access and malicious activities within network environments. With the rapid evolution of cyber threats, traditional IDS approaches are no longer sufficient, creating a strong academic demand for more intelligent and adaptive security solutions. Artificial Intelligence (AI), particularly machine learning and deep learning, has emerged as a promising approach to enhance the effectiveness of IDS by enabling automated threat detection and real-time decision-making (Ahmad et al. 710). The integration of AI into cybersecurity research has therefore gained substantial scholarly attention due to its potential to transform conventional defense mechanisms into proactive and predictive systems (Buczak and Guven 1155).

Context and Background of the Study

Modern network environments are highly dynamic, characterized by large-scale data transmission, cloud integration, and the widespread use of Internet of Things (IoT) devices. These advancements, while beneficial, have significantly increased the attack surface for cybercriminals. Cyberattacks such as phishing, ransomware, and Distributed Denial of Service (DDoS) attacks have become more sophisticated and difficult to detect using traditional methods. Signature-based IDS rely on predefined patterns, which limit their ability to identify unknown or zero-day attacks. In contrast, AI-based IDS utilize data-driven techniques to identify patterns and anomalies, making them more suitable for complex and rapidly changing network conditions (Sommer and Paxson 305). Deep learning models, in particular, have shown the ability to process high-dimensional network traffic data and detect subtle behavioral deviations (Kim et al. 110).

Identify research gap or what is missing in existing studies

Despite the growing body of research on AI-based intrusion detection, several gaps remain. Many existing studies focus primarily on improving detection accuracy without adequately addressing issues such as false positive rates, scalability, and real-time deployment challenges. High false positives can reduce the reliability of IDS and create operational inefficiencies in security management (Ahmad et al. 720). Additionally, limited attention has been given to the interpretability of AI models, which is essential for practical implementation in cybersecurity operations where analysts require clear explanations of detected threats. Furthermore, there is a lack of comprehensive comparative analysis between traditional IDS and AI-based systems across diverse and real-world network environments (Buczak and Guven 1160). These limitations highlight the need for more balanced and application-oriented research.

Clearly state the research objectives/questions

This study aims to investigate the effectiveness of AI-based intrusion detection systems in modern network environments. The key research objectives are:

- To evaluate the performance of AI-based IDS in detecting cyber threats.
- To compare AI-based IDS with traditional intrusion detection methods.
- To analyze the challenges associated with implementing AI in network security.
- To explore potential improvements and future directions for AI-based IDS.

The study addresses the following research questions:

- How effective are AI-based IDS in detecting known and unknown threats?
- What are the advantages and limitations of AI-based IDS compared to traditional systems?
- What challenges affect the deployment of AI-based IDS in real-world environments?

Mention the scope and significance of the study

The scope of this research is limited to the analysis of AI-based intrusion detection techniques within modern network infrastructures, including enterprise networks, cloud environments, and IoT systems. The study is based on a review and analysis of existing literature and does not involve primary data collection. Its significance lies in providing a comprehensive understanding of how

AI enhances network security and identifying areas for future improvement. The findings of this study contribute to the development of more efficient and intelligent cybersecurity systems capable of addressing emerging threats. Moreover, the study supports ongoing academic discourse by bridging theoretical insights with practical implications in the field of network security (Kim et al. 115).

2. Literature Review

The integration of artificial intelligence into intrusion detection systems has been a central focus of cybersecurity research over the past decade. Early approaches to intrusion detection relied heavily on signature-based methods, which compare network activity against known attack patterns. While effective for previously identified threats, these systems lack the ability to detect novel or evolving attacks, thereby limiting their applicability in modern network environments (Sommer and Paxson 305).

To address these limitations, researchers began exploring machine learning techniques for anomaly detection and classification. Algorithms such as decision trees, support vector machines (SVM), and k-nearest neighbors (KNN) have been widely applied in IDS frameworks. These models demonstrated improved detection accuracy and adaptability by learning patterns from historical data rather than relying solely on predefined signatures (Buczak and Guven 1156). However, traditional machine learning approaches often require extensive feature engineering and may struggle with high-dimensional data.

The emergence of deep learning has further advanced the capabilities of intrusion detection systems. Deep neural networks, including convolutional neural networks (CNN) and recurrent neural networks (RNN), are capable of automatically extracting features from raw network traffic data. CNNs are particularly effective in identifying spatial patterns in traffic flows, while RNNs excel in modeling temporal dependencies, making them suitable for sequential data analysis (Kim et al. 111). Studies have shown that deep learning-based IDS can achieve higher detection rates and lower false negatives compared to conventional machine learning models (Ahmad et al. 715).

In addition to standalone models, hybrid approaches have gained significant attention in recent literature. These systems combine multiple detection techniques, such as anomaly-based and signature-based methods, to leverage their complementary strengths. Hybrid IDS frameworks have been shown to reduce false positive rates while maintaining high detection accuracy, making them more practical for real-world deployment (Buczak and Guven 1158). Furthermore, ensemble learning techniques, which integrate multiple classifiers, have demonstrated improved robustness and generalization performance.

Another important area of research is the application of AI in distributed and cloud-based network environments. With the increasing adoption of cloud computing and IoT technologies, intrusion detection systems must handle large volumes of heterogeneous data. AI-based IDS have been adapted to these environments by incorporating scalable architectures and real-time processing capabilities. Edge computing has also been explored as a means to reduce latency and improve response times in distributed networks (Kim et al. 114).

Despite these advancements, several challenges remain. One of the most significant issues is data imbalance, where the number of normal network instances far exceeds malicious ones. This imbalance can lead to biased models that favor normal traffic, reducing the effectiveness of intrusion detection (Ahmad et al. 720). Additionally, the lack of high-quality, labeled datasets limits the training and evaluation of AI models. Many widely used datasets, such as KDD Cup 99, are outdated and may not accurately represent current network threats.

Model interpretability is another critical concern in AI-based IDS. Deep learning models, while highly accurate, often operate as "black boxes," making it difficult for security analysts to understand the reasoning behind their decisions. This lack of transparency can hinder trust and adoption in real-world applications (Sommer and Paxson 310). Researchers are increasingly focusing on

explainable AI (XAI) techniques to address this issue.

Moreover, computational complexity and resource requirements pose practical challenges for the deployment of AI-based IDS. Training deep learning models requires significant computational power and large datasets, which may not be feasible for all organizations. Real-time implementation also demands efficient algorithms capable of processing high-speed network traffic without introducing latency.

In summary, the literature highlights the significant potential of AI-based intrusion detection systems in enhancing network security. Machine learning and deep learning techniques have demonstrated superior performance compared to traditional methods, particularly in detecting unknown and complex attacks. However, issues related to data quality, model interpretability, scalability, and computational efficiency must be addressed to ensure the practical applicability of these systems in modern network environments.

3. Research Methodology

This study adopts a qualitative, analytical, and comparative research design to investigate the effectiveness of AI-based intrusion detection systems in modern network environments. The methodology is structured to provide a systematic evaluation of existing approaches while ensuring academic rigor and clarity.

Research Design

The research follows a descriptive and exploratory design. It synthesizes findings from existing studies to evaluate how artificial intelligence enhances intrusion detection capabilities. A comparative framework is employed to analyze differences between traditional IDS and AI-based IDS in terms of performance and applicability.

Data Sources

The study relies on secondary data collected from peer-reviewed journal articles, conference proceedings, and reputable digital libraries in the field of cybersecurity and computer networks. Key sources include publications indexed in IEEE, Springer, Elsevier, and ACM databases. These sources provide validated experimental results and theoretical insights into intrusion detection systems (Buczak and Guven 1154).

Selection Criteria

Relevant studies were selected based on the following criteria:

- Publication in peer-reviewed journals or conferences
- Focus on AI, machine learning, or deep learning in IDS
- Availability of performance metrics such as accuracy, precision, recall, and false positive rate
- Relevance to modern network environments including cloud and IoT

This filtering ensures that only high-quality and recent research contributes to the analysis.

Analytical Framework

The study employs a comparative analytical framework to evaluate IDS performance. The following key performance indicators (KPIs) are used:

- **Detection Accuracy:** Measures the proportion of correctly identified intrusions
- **False Positive Rate (FPR):** Indicates the frequency of incorrect alerts
- **Precision and Recall:** Evaluate classification effectiveness
- **Response Time:** Assesses real-time detection capability
- **Scalability:** Determines system performance in large-scale networks

These metrics are widely used in intrusion detection research and provide a standardized basis for comparison (Ahmad et al. 712).

Method of Analysis

A thematic and comparative analysis is conducted to interpret findings from selected studies. Machine learning models (e.g., SVM, decision trees) and deep learning models (e.g., CNN, RNN) are examined to assess their strengths and limitations. The study also reviews hybrid and ensemble approaches to identify trends in improving IDS performance.

Reliability and Validity

To ensure reliability, the study uses multiple credible sources and cross-verifies findings across different research works. Validity is maintained by focusing on widely accepted methodologies and

performance metrics in the field of intrusion detection. The use of peer-reviewed literature further strengthens the authenticity of the analysis.

Limitations of the Methodology

This research is limited to secondary data analysis and does not include primary experimentation or simulation. As a result, findings depend on the accuracy and scope of existing studies. Additionally, variations in datasets and experimental conditions across different studies may affect direct comparison of results.

Despite these limitations, the methodology provides a comprehensive and systematic evaluation of AI-based intrusion detection systems, offering valuable insights into their effectiveness and practical applicability.

4. Theoretical Analysis

The theoretical foundation of AI-based intrusion detection systems is rooted in machine learning theory, anomaly detection, and pattern recognition. These systems are designed to analyze network traffic data, identify deviations from normal behavior, and classify such deviations as potential threats. Unlike traditional IDS, which rely on predefined signatures, AI-based systems learn from data, enabling them to adapt to new and evolving cyber threats (Sommer and Paxson 306).

Machine Learning Theory in IDS

Machine learning plays a central role in modern intrusion detection systems. Supervised learning models, such as decision trees, support vector machines (SVM), and logistic regression, rely on labeled datasets to classify network traffic into normal and malicious categories. These models are effective when high-quality labeled data is available; however, their performance is limited by the availability and accuracy of such data (Buczak and Guven 1156).

Unsupervised learning models, on the other hand, detect anomalies without requiring labeled datasets. Techniques such as clustering and density-based methods identify unusual patterns in network traffic that may indicate intrusions. These approaches are particularly useful in detecting zero-day attacks, where no prior knowledge of attack signatures exists (Ahmad et al. 713).

Deep Learning and Feature Extraction

Deep learning extends traditional machine learning by enabling automatic feature extraction from raw data. Neural networks, particularly convolutional neural networks (CNN) and recurrent neural networks (RNN), are widely used in intrusion detection. CNNs are effective in capturing spatial relationships within data, while RNNs are designed to process sequential information, making them suitable for analyzing time-series network traffic (Kim et al. 111).

The ability of deep learning models to handle high-dimensional data makes them highly effective in complex network environments. These models can detect subtle variations in traffic patterns that may not be identifiable through traditional methods. As a result, deep learning-based IDS often achieve higher detection accuracy and lower false negative rates (Ahmad et al. 715).

Anomaly Detection Theory

Anomaly detection is a key theoretical concept underlying AI-based IDS. It involves identifying patterns that deviate significantly from established norms. In network security, anomalies may indicate malicious activities such as unauthorized access or data exfiltration. AI-based systems continuously learn and update their understanding of normal behavior, allowing them to detect emerging threats in real time (Sommer and Paxson 308).

Anomaly detection techniques can be broadly categorized into statistical, distance-based, and machine learning-based approaches. Machine learning-based methods are particularly effective due to their adaptability and ability to process large datasets.

Hybrid and Ensemble Models

Theoretical advancements in IDS also include hybrid and ensemble learning approaches. Hybrid models combine multiple detection techniques, such as signature-based and anomaly-based methods, to improve overall system performance. Ensemble methods integrate multiple classifiers to enhance accuracy and robustness. These approaches are based on the principle that combining diverse models can reduce individual

weaknesses and improve generalization (Buczak and Guven 1158).

Challenges in Theoretical Implementation

Despite their advantages, AI-based IDS face several theoretical challenges. One major issue is overfitting, where models perform well on training data but fail to generalize to new data. This problem is particularly common in deep learning models with complex architectures. Additionally, data imbalance can affect model performance, as the number of normal instances often exceeds malicious ones (Ahmad et al. 720).

Another challenge is the lack of interpretability in AI models. Complex neural networks often function as "black boxes," making it difficult to understand how decisions are made. This limitation poses a challenge for cybersecurity professionals who require transparency in threat detection systems (Sommer and Paxson 310).

Theoretical Implications

The theoretical analysis highlights that AI-based intrusion detection systems offer a dynamic and adaptive approach to network security. By leveraging machine learning and deep learning techniques, these systems can detect both known and unknown threats with greater accuracy. However, addressing challenges such as overfitting, data imbalance, and interpretability is essential to fully realize their potential in real-world applications.

5. Discussion and Analysis

The analysis of existing research demonstrates that AI-based intrusion detection systems significantly outperform traditional methods in terms of accuracy and adaptability. Machine learning models can identify previously unknown attacks, reducing the risk of security breaches. Deep learning approaches further enhance detection capabilities by analyzing complex patterns in network traffic.

However, the implementation of AI-based IDS is not without limitations. High false positive rates can lead to unnecessary alerts, affecting system efficiency. Computational complexity and resource requirements pose challenges for real-time deployment, particularly in resource-constrained environments.

Another critical issue is the interpretability of AI models. Security analysts often require clear explanations of detected threats, but complex models may not provide easily understandable insights. This limitation highlights the need for explainable AI techniques in cybersecurity.

Despite these challenges, the integration of AI with traditional IDS can create hybrid systems that balance accuracy and efficiency. Such approaches leverage the strengths of both methods, resulting in more robust and reliable security solutions.

6. Conclusion

This study highlights the transformative potential of AI-based intrusion detection systems in modern network environments. By leveraging machine learning and deep learning techniques, these systems offer significant improvements in detecting and preventing cyber threats. The findings indicate that AI-based IDS outperform traditional systems in terms of accuracy, adaptability, and scalability.

However, challenges such as computational complexity, data quality issues, and model interpretability must be addressed to ensure effective implementation. Future research should focus on developing lightweight algorithms, improving dataset quality, and enhancing the transparency of AI models.

In conclusion, AI-based intrusion detection systems represent a promising direction for advancing network security. Their ability to adapt to evolving threats makes them a valuable tool in safeguarding digital infrastructures. Continued research and innovation in this field will contribute to the development of more secure and resilient network environments.

References

Ahmad, I., et al. "A Review of Machine Learning Approaches in Intrusion Detection Systems." IEEE Access, vol. 7, 2019, pp. 709–729.

Buczak, Anna L., and Erhan Guven. "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection." IEEE Communications Surveys & Tutorials, vol. 18, no. 2, 2016, pp. 1153–1176.

Kim, G., et al. "Deep Learning-Based Intrusion Detection Systems: A Review." Journal of

Network and Computer Applications, vol. 120, 2018, pp. 107–118.

Sommer, Robin, and Vern Paxson. "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection." IEEE Symposium on Security and Privacy, 2010, pp. 305–316.

Zhang, J., et al. "Network Intrusion Detection Based on Deep Learning Approaches." Future Generation Computer Systems, vol. 115, 2021, pp. 303–316.

Shone, N., et al. "A Deep Learning Approach to Network Intrusion Detection." IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, 2018, pp. 41–50.

Vinayakumar, R., et al. "Deep Learning Approach for Intelligent Intrusion Detection System." IEEE Access, vol. 7, 2019, pp. 41525–41550.

Javaid, A., et al. "A Deep Learning Approach for Network Intrusion Detection System." EAI Endorsed Transactions on Security and Safety, vol. 3, no. 9, 2016, pp. e2.

Liao, H. J., et al. "Intrusion Detection System: A Comprehensive Review." Journal of Network and Computer Applications, vol. 36, no. 1, 2013, pp. 16–24.

Mirsky, Y., et al. "Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection." Network and Distributed System Security Symposium (NDSS), 2018.