AI-Powered Intrusion Detection Systems: Real-World Performance Analysis

***Sai Manoj Yellepeddi**, Senior Technical Advisor and Independent Researcher, Redmond, USA*

***Chetan Sasidhar Ravi,** Mulesoft Developer, Zurich American Insurance, Illinois, USA*

***Vinay Kumar Reddy Vangoor**, Engineer II, MetaSoftTech Solutions LLC, Arizona, USA*

***Subrahmanyasarma Chitta**, Software Engineer, Access2Care LLC, Colorado, USA*

Abstract

The advent of artificial intelligence (AI) has significantly influenced various domains of cybersecurity, particularly in the realm of Intrusion Detection Systems (IDS). This paper presents a comprehensive analysis of AI-powered IDS, focusing on their real-world performance relative to traditional IDS methodologies. As cyber threats continue to evolve in complexity and sophistication, the need for advanced detection mechanisms has become paramount. AI-powered IDS leverage machine learning (ML) and deep learning (DL) techniques to enhance detection accuracy, reduce false positives, and improve response times.

Machine learning algorithms, such as decision trees, support vector machines, and ensemble methods, have been extensively employed in IDS to learn from historical data and identify patterns indicative of potential intrusions. These algorithms enable IDS to adapt to new and emerging threats by continuously refining their detection models based on evolving data. Deep learning techniques, including convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have further advanced the field by enabling the analysis of complex, high-dimensional data, such as network traffic and system logs, with greater accuracy.

The paper provides a detailed comparative performance analysis of AI-powered IDS against traditional signature-based and anomaly-based IDS approaches. Traditional IDS systems rely heavily on predefined signatures and heuristics to detect known threats. While these systems are effective at identifying known attack patterns, they often fall short in detecting novel or sophisticated threats. In contrast, AI-powered IDS utilize advanced algorithms capable of identifying previously unseen attack vectors by learning from vast amounts of data.

Real-world performance analysis is conducted using a variety of datasets and attack scenarios. This includes examining the efficacy of AI-powered IDS in detecting various types of attacks, such as distributed denial of service (DDoS) attacks, malware infections, and insider threats. The analysis encompasses metrics such as detection accuracy, false positive rates, and response times, providing a nuanced understanding of the strengths and limitations of AI-powered systems.

Implementation challenges are a critical aspect of integrating AI into IDS. The paper explores issues related to the training and validation of AI models, including the need for large, representative datasets and the risks of overfitting. Scalability concerns are also addressed, as the deployment of AI-powered IDS in large-scale networks may require significant computational resources and infrastructure. Additionally, the paper discusses the implications of AI model interpretability and transparency, which are crucial for ensuring trust and accountability in cybersecurity applications.

The future of AI in IDS is examined, with a focus on emerging trends and technologies. The paper highlights the potential of hybrid approaches that combine AI techniques with traditional IDS methods to enhance overall effectiveness. It also considers the role of explainable AI (XAI) in improving the interpretability of AI-powered IDS and fostering greater adoption in enterprise environments.

This paper provides an in-depth analysis of AI-powered IDS, offering valuable insights into their performance, implementation challenges, and future prospects. The findings underscore the transformative potential of AI in enhancing cybersecurity defenses, while also identifying areas for further research and development. By addressing the limitations of traditional IDS and leveraging the capabilities of advanced AI techniques, AI-powered IDS represent a significant advancement in the field of cybersecurity.

Keywords

AI-powered IDS, machine learning, deep learning, cybersecurity, intrusion detection, performance analysis, scalability, implementation challenges, attack scenarios, explainable AI

1. Introduction

1.1 Background and Motivation

In the contemporary digital landscape, cybersecurity threats have become increasingly sophisticated and pervasive, necessitating the deployment of advanced Intrusion Detection Systems (IDS) to safeguard critical information infrastructure. The frequency and severity of cyber-attacks have escalated, driven by both the proliferation of connected devices and the increasing sophistication of adversarial techniques. These threats include a diverse array of malicious activities, such as distributed denial of service (DDoS) attacks, zero-day vulnerabilities, and advanced persistent threats (APTs), all of which pose significant risks to data integrity, confidentiality, and availability.

Historically, IDS technologies have evolved through several phases, each reflecting advancements in both attack methodologies and defensive strategies. Early IDS were primarily signature-based, relying on predefined patterns of known threats to identify malicious activities. While effective against well-documented attacks, these systems are inherently limited by their inability to detect novel or sophisticated threats that do not match existing signatures. This limitation underscored the need for more adaptive and resilient IDS solutions.

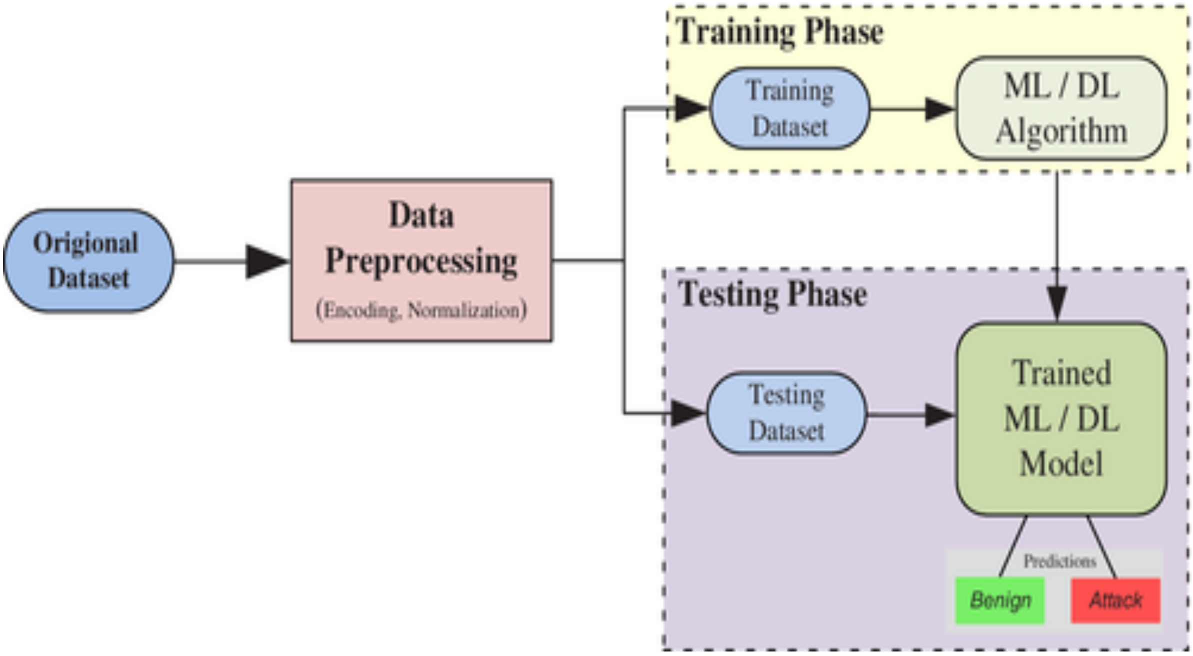
The subsequent generation of IDS incorporated anomaly detection techniques, which aimed to identify deviations from established baselines of normal behavior. Although this approach offered improvements in detecting previously unknown threats, it was often hindered by high false positive rates and the challenge of defining accurate baselines. As cybersecurity threats continued to evolve, there was a growing recognition that more dynamic and intelligent systems were required to address the complexities of modern attack vectors.

1.2 Importance of AI in Intrusion Detection

The integration of artificial intelligence (AI) into IDS represents a significant leap forward in addressing the limitations of traditional approaches. AI techniques, particularly machine learning (ML) and deep learning (DL), offer advanced capabilities for pattern recognition and anomaly detection, enabling IDS to adapt to new and evolving threats with greater precision. ML algorithms, such as decision trees, support vector machines, and ensemble methods, leverage large datasets to learn and generalize from historical attack patterns, thereby enhancing their ability to identify both known and novel threats.

Deep learning, a subset of ML characterized by its use of neural networks with multiple layers, further extends the capabilities of IDS by enabling the analysis of complex, high-dimensional data. Techniques such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) can process intricate data representations, such as network traffic patterns and system logs, with increased accuracy and reduced dependency on manual feature engineering. This advancement is particularly valuable in detecting sophisticated attacks that may not conform to simple anomaly patterns or signature-based criteria.

The rationale for incorporating AI into IDS stems from its potential to address several critical challenges faced by traditional systems. AI-powered IDS can dynamically adapt to new threats by continuously updating their models based on real-time data, thereby improving detection accuracy and reducing false positives. Moreover, AI techniques can handle vast amounts of data with greater efficiency, facilitating real-time analysis and response.



1.3 Objectives and Scope

The primary objective of this paper is to provide a comprehensive analysis of AI-powered IDS, focusing on their effectiveness in real-world scenarios compared to traditional IDS methodologies. This analysis aims to elucidate the advantages and limitations of AI-enhanced detection systems, with particular emphasis on performance metrics such as detection accuracy, false positive rates, and response times.

Key research questions addressed in this study include: How do AI-powered IDS perform relative to traditional IDS in detecting various types of cyber-attacks? What are the specific challenges associated with the implementation and scalability of AI-based systems? How do AI techniques improve upon the limitations of traditional IDS, and what are the implications for future developments in cybersecurity?

The hypotheses underpinning this research are based on the premise that AI-powered IDS offer superior performance in detecting both known and unknown threats compared to traditional approaches. It is anticipated that the advanced capabilities of AI, including its adaptability and efficiency, will result in improved detection accuracy and reduced false positives. Additionally, the study hypothesizes that while AI-powered IDS present significant advantages, they also introduce new challenges related to implementation, scalability, and interpretability that must be addressed to fully realize their potential.

This paper will systematically explore these aspects, providing a detailed evaluation of AI-powered IDS through empirical performance analysis, examination of implementation challenges, and discussion of future research directions.

2. Overview of AI Techniques in IDS

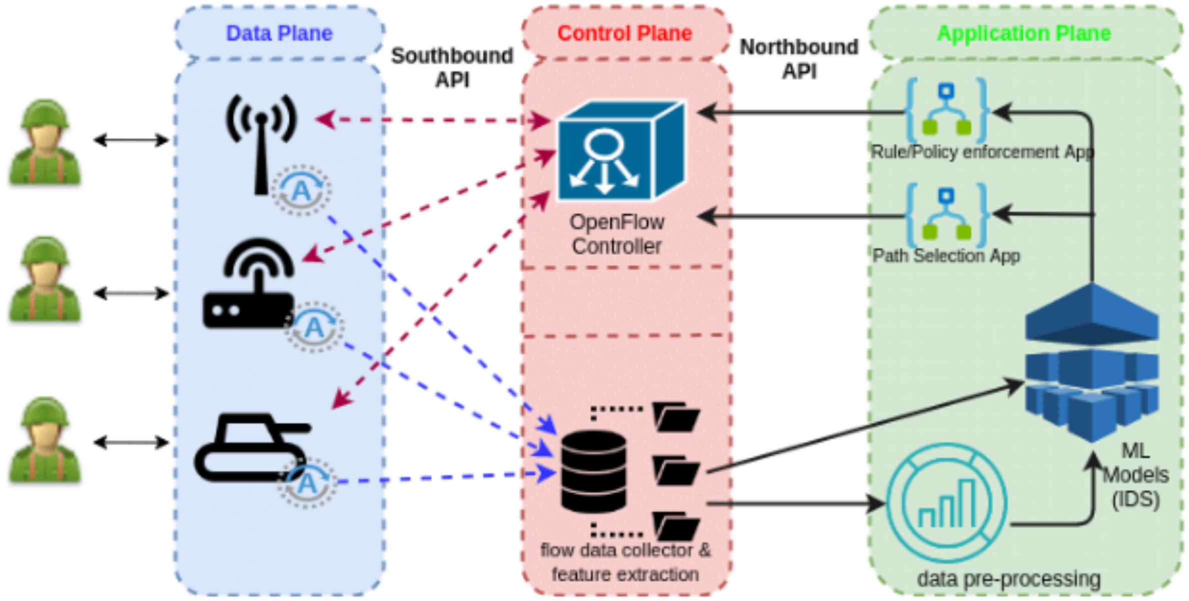
2.1 Machine Learning Techniques

Machine learning (ML) techniques have revolutionized intrusion detection systems (IDS) by enabling them to learn from data and adapt to new threats without explicit programming. Among the most prominent ML approaches are supervised and unsupervised learning algorithms, each contributing uniquely to the evolution of IDS.

Supervised learning algorithms are designed to build a model based on labeled training data, where the algorithm learns to map inputs to outputs using a dataset that includes both normal and attack patterns. Prominent algorithms in this category include decision trees and support vector machines (SVMs). Decision trees utilize a hierarchical structure to make decisions based on feature values, creating a tree-like model of decisions and their possible consequences. This approach is highly interpretable and useful for detecting specific attack patterns through rule-based classification.

Support vector machines (SVMs) operate by finding the optimal hyperplane that separates data into different classes, maximizing the margin between the decision boundary and the closest data points from each class. SVMs are particularly effective in high-dimensional spaces and are well-suited for binary classification tasks in IDS. Their ability to generalize well to unseen data makes them robust against overfitting, a common issue in traditional IDS.

Unsupervised learning techniques, on the other hand, do not rely on labeled data and are utilized to identify patterns or anomalies within datasets where labels are not predefined. These techniques are particularly valuable for detecting novel or previously unknown attack patterns. One widely used unsupervised method is clustering, which groups similar data points into clusters and identifies anomalies as outliers that deviate from the norm. Another approach is dimensionality reduction, such as Principal Component Analysis (PCA), which simplifies the dataset by reducing the number of features while preserving its essential structure. These methods facilitate the detection of unusual behavior that might indicate an intrusion.



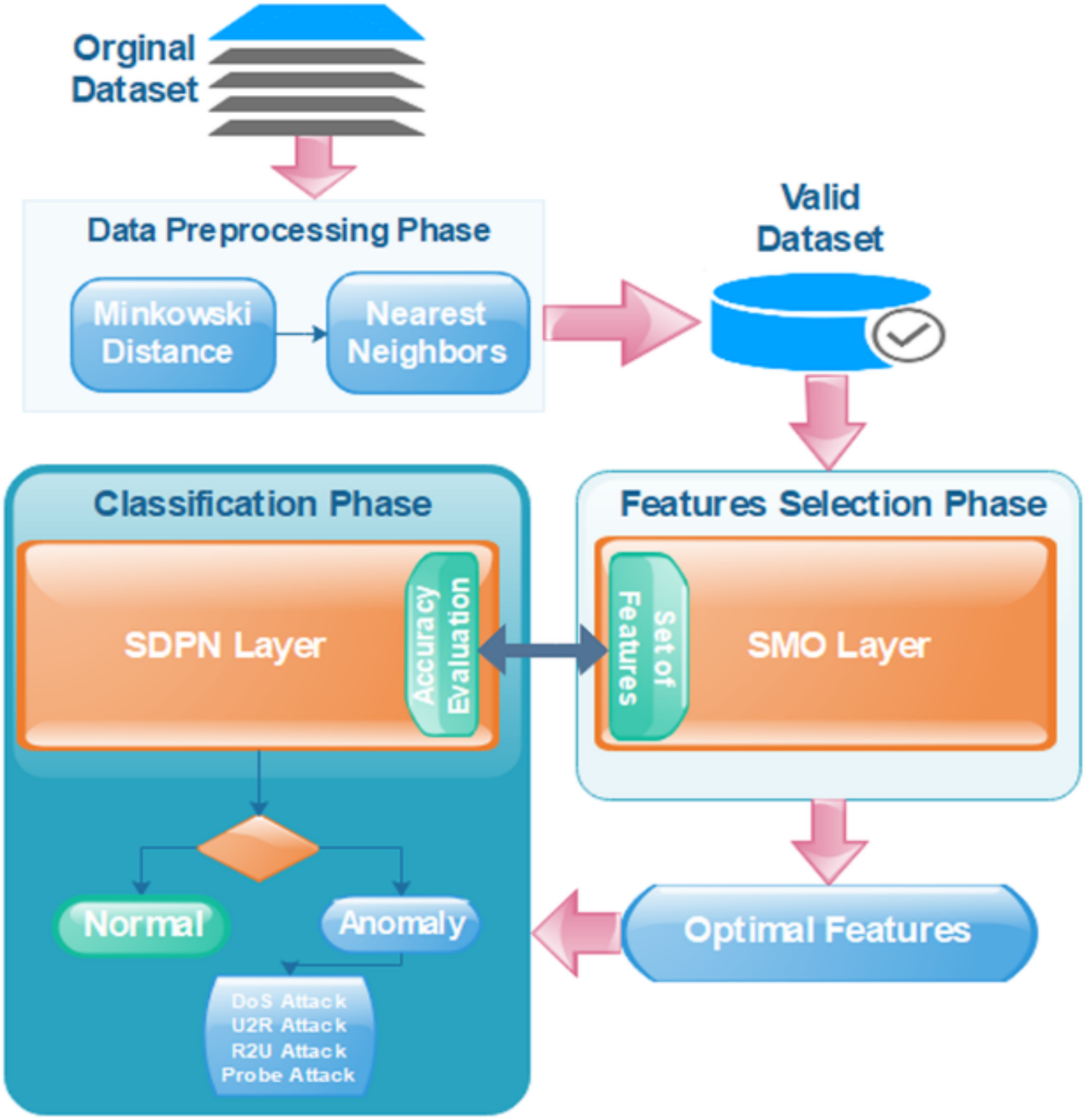
2.2 Deep Learning Approaches

Deep learning, a subset of machine learning, involves the use of neural networks with multiple layers, enabling the model to learn complex representations of data. Two prominent deep learning architectures are convolutional neural networks (CNNs) and recurrent neural networks (RNNs), each offering distinct advantages for analyzing complex data in IDS.

Convolutional neural networks (CNNs) are particularly effective for processing grid-like data structures, such as images or time-series data. In the context of IDS, CNNs can be applied to analyze network traffic patterns or system logs, identifying intricate patterns and relationships that might be indicative of an intrusion. CNNs operate by applying convolutional filters to input data, capturing local patterns and progressively learning higher-level abstractions through multiple layers of convolutions and pooling operations. This capability allows CNNs to detect subtle and complex attack signatures that might be missed by traditional methods.

Recurrent neural networks (RNNs), including Long Short-Term Memory (LSTM) networks, are designed to handle sequential data by maintaining a form of memory through their recurrent connections. This makes RNNs particularly suited for analyzing time-series data, such as network traffic logs or system event sequences. RNNs can model temporal dependencies and identify deviations in behavior over time, which is crucial for detecting sophisticated attacks that involve sequential patterns or delayed activation.

The application of deep learning in IDS enables the handling of vast amounts of high-dimensional data with greater accuracy and efficiency. By learning hierarchical features and capturing intricate patterns, deep learning models can enhance detection capabilities and reduce reliance on manual feature extraction.

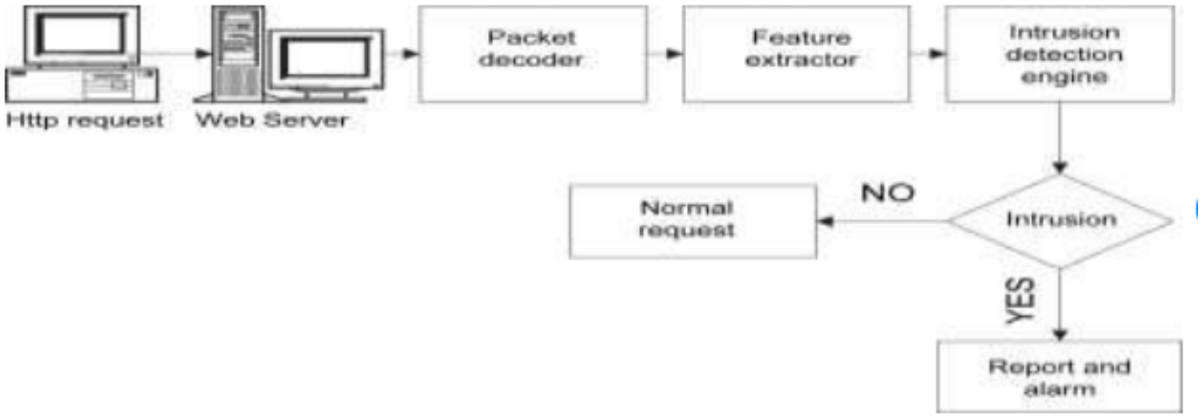


2.3 Comparison with Traditional IDS Methods

Traditional IDS methods primarily encompass signature-based and anomaly-based approaches. Signature-based IDS rely on predefined patterns of known attacks, which are compared against incoming data to identify matches. While this approach is highly effective for detecting known threats, it suffers from limitations in adaptability. Signature-based systems are unable to detect new or novel attack vectors that do not conform to established signatures, resulting in a reduced capacity to address emerging threats.

Anomaly-based IDS, in contrast, establish a baseline of normal behavior and identify deviations from this baseline as potential intrusions. This method allows for the detection of unknown attacks by identifying unusual patterns that deviate from expected norms. However, anomaly-based systems often face challenges related to high false positive rates and the difficulty of accurately defining normal behavior.

The integration of AI techniques, particularly machine learning and deep learning, addresses several limitations inherent in traditional IDS methods. AI-powered systems can dynamically adapt to new threats by learning from data and refining their detection models over time. Unlike signature-based approaches, AI techniques do not require predefined patterns, allowing them to detect novel attack patterns. Moreover, AI models can process and analyze large volumes of data more effectively, enhancing the ability to detect sophisticated attacks with greater precision and reduced false positives.



While traditional IDS methods have played a crucial role in cybersecurity, the adoption of AI techniques represents a significant advancement, offering enhanced adaptability, accuracy, and efficiency in intrusion detection. The continued evolution of AI technologies promises further improvements in addressing the complexities of modern cyber threats.

3. Comparative Performance Analysis

3.1 Methodology

The comparative performance analysis of AI-powered Intrusion Detection Systems (IDS) involves a rigorous evaluation using diverse datasets and attack scenarios to assess their effectiveness. This evaluation is crucial for understanding the practical capabilities of AI-based systems in real-world environments.

The datasets employed for evaluation typically consist of network traffic logs, system events, and intrusion records. These datasets are categorized based on the types of attacks and normal traffic patterns they represent. Commonly used datasets include the KDD Cup 99, which encompasses a broad range of attack types and is often used for training and testing IDS, and the NSL-KDD dataset, an improved version addressing some limitations of the original KDD dataset. Additionally, contemporary datasets such as the CICIDS 2017 and the UNSW-NB15 are utilized to provide a more up-to-date and diverse range of attack scenarios and network behaviors.

Attack scenarios for evaluation cover a wide spectrum of threats, including network-based attacks like Distributed Denial of Service (DDoS), malware infections, and insider threats. Each scenario is designed to test the IDS's ability to detect specific types of intrusions and assess its response under various conditions. For instance, simulated DDoS attacks help evaluate the system's capability to handle high volumes of malicious traffic, while malware attacks test its ability to identify and respond to harmful payloads.

Metrics for performance measurement are critical in assessing the efficacy of IDS. Key metrics include detection accuracy, which measures the proportion of correctly identified attacks compared to the total number of attacks; false positive rate, which indicates the frequency with which legitimate activity is incorrectly classified as an attack; and response time, which measures the speed at which the system identifies and responds to an intrusion. These metrics provide a comprehensive view of an IDS’s effectiveness and operational efficiency.

3.2 Performance of AI-Powered IDS

AI-powered IDS systems have demonstrated notable improvements in performance across various attack types compared to traditional approaches. The application of machine learning and deep learning techniques has enhanced the ability of IDS to detect complex and novel threats with greater accuracy and reduced false positives.

In detailed performance analyses, AI-powered IDS have shown superior detection capabilities across different attack types. For example, machine learning algorithms such as Random Forests and Gradient Boosting have exhibited high accuracy in detecting known attack patterns, while deep learning models like Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have excelled in identifying sophisticated and previously unseen threats. The ability of deep learning models to analyze complex data patterns enables them to detect subtle anomalies and intricate attack signatures that traditional methods might miss.

Case studies and real-world examples underscore the effectiveness of AI-powered IDS. In a notable case, a deployment of a deep learning-based IDS in a large enterprise network successfully identified and mitigated a series of advanced persistent threats (APTs) that traditional signature-based systems failed to detect. The AI-powered system's ability to continuously learn and adapt to new attack patterns resulted in a substantial reduction in false positives and a significant improvement in detection accuracy.

Another case study involving a machine learning-based IDS demonstrated effective detection of Distributed Denial of Service (DDoS) attacks. By leveraging ensemble methods that combine multiple learning algorithms, the system achieved high precision in distinguishing between legitimate traffic and attack traffic, thereby minimizing the impact of DDoS attacks on network performance.

3.3 Comparative Evaluation

A comparative evaluation of AI-powered IDS with traditional IDS methods reveals several strengths and weaknesses inherent to each approach. Traditional IDS methods, including signature-based and anomaly-based systems, have historically provided a foundational approach to intrusion detection. However, their limitations have become more pronounced with the increasing sophistication of cyber threats.

Signature-based IDS, while effective in identifying known threats, struggle with detecting novel attack patterns due to their reliance on predefined signatures. This limitation results in a reduced capacity to address emerging threats and an increased risk of missed detections. Anomaly-based IDS offer improvements by detecting deviations from normal behavior, but they often suffer from high false positive rates and challenges in accurately defining normal behavior.

In contrast, AI-powered IDS offer significant advantages in addressing these limitations. Machine learning algorithms can learn from historical data and adapt to new threats without the need for predefined signatures. This adaptability allows AI-powered systems to detect novel attack patterns and reduce reliance on manual updates. Deep learning techniques further enhance this capability by analyzing complex data representations and identifying subtle anomalies that traditional methods might overlook.

Despite these advantages, AI-powered IDS are not without their challenges. The complexity of AI models can lead to issues related to interpretability and transparency, making it difficult to understand the basis for specific detections or decisions. Additionally, the computational resources required for training and deploying AI models can be substantial, posing scalability concerns for large-scale implementations.

AI-powered IDS offer substantial improvements in detection accuracy and adaptability, they also introduce new challenges that must be addressed. The comparative evaluation highlights the strengths of AI-based systems in overcoming the limitations of traditional methods while acknowledging the need for continued advancements in model interpretability and scalability.

4. Implementation Challenges and Scalability

4.1 Model Training and Validation

The training and validation of AI-powered Intrusion Detection Systems (IDS) present several challenges that can significantly impact the performance and reliability of these systems. One of the primary issues is data quality and representativeness. For AI models to be effective, they require large volumes of high-quality data that accurately represent the normal and attack behaviors within the environment they are designed to monitor. Poor data quality, such as incomplete or erroneous data, can lead to inaccurate models and unreliable detection capabilities. Furthermore, if the training data is not representative of the diverse range of potential attacks and normal behaviors, the model may fail to generalize effectively to new, unseen scenarios.

Overfitting is another critical challenge in model training. Overfitting occurs when a model learns not only the underlying patterns in the training data but also the noise and specific details that do not generalize to new data. This results in high performance on training data but poor performance on real-world data. Techniques such as cross-validation, where the data is divided into multiple subsets for training and validation, can help mitigate overfitting. Additionally, regularization methods, such as dropout in neural networks, and ensemble approaches, which combine predictions from multiple models, are employed to enhance model robustness and generalization.

Ensuring that the AI model is robust against adversarial attacks is also crucial. Adversarial examples, where slight perturbations to input data lead to incorrect model predictions, can undermine the reliability of the IDS. Techniques such as adversarial training, where models are exposed to adversarial examples during training, can help improve robustness against such attacks.

4.2 Scalability Concerns

Scalability is a significant concern for the implementation of AI-powered IDS, particularly in large-scale environments where the volume of data can be immense. The computational resource requirements for training and deploying AI models can be substantial, necessitating powerful hardware and efficient algorithms. The complexity of deep learning models, in particular, often requires high-performance GPUs or specialized hardware to handle the extensive computations involved. This can lead to increased costs and infrastructure demands, posing challenges for organizations with limited resources.

The integration of AI-powered IDS with existing infrastructure also presents scalability challenges. Legacy systems and traditional IDS may not be designed to accommodate the advanced requirements of AI models, such as real-time data processing and high-throughput capabilities. Ensuring seamless integration involves addressing compatibility issues and potentially redesigning portions of the infrastructure to support the new AI components. Additionally, AI-powered systems often require continuous updates and maintenance to adapt to new threats and changing data patterns, further adding to the complexity of maintaining a scalable and effective IDS.

4.3 Interpretability and Transparency

Interpretability and transparency are crucial aspects of AI systems, particularly in cybersecurity where understanding the basis for detection decisions is essential for trust and effective response. Explainable AI (XAI) aims to provide insights into how AI models make decisions, allowing users to comprehend and validate the rationale behind specific detections.

In cybersecurity, the ability to explain AI model decisions is vital for several reasons. Security analysts need to understand why a particular event is flagged as an intrusion to assess the severity and determine appropriate response actions. Furthermore, regulatory requirements and organizational policies often mandate that security systems provide clear explanations for their decisions to ensure compliance and facilitate auditing.

However, achieving interpretability in AI models, particularly complex deep learning models, poses significant challenges. Many advanced models, such as neural networks, operate as "black boxes," with their internal decision-making processes not easily accessible or understandable. Efforts to enhance interpretability involve techniques such as feature importance analysis, where the contribution of each input feature to the model's predictions is assessed, and model-agnostic methods, which provide explanations independent of the specific model architecture.

Despite these efforts, making AI models fully transparent and interpretable remains an ongoing challenge. Balancing the complexity and performance of AI models with the need for interpretability requires careful consideration and the development of novel methods to bridge the gap between advanced capabilities and user understanding.

The implementation of AI-powered IDS involves addressing challenges related to model training and validation, scalability concerns, and interpretability. Ensuring high-quality data, managing computational resources, integrating with existing systems, and providing clear explanations of model decisions are essential for developing effective and reliable AI-based intrusion detection solutions.

5. Future Directions and Conclusion

5.1 Emerging Trends in AI for IDS

The field of intrusion detection systems (IDS) is witnessing significant advancements driven by artificial intelligence (AI), which are shaping the future landscape of cybersecurity. Current research is increasingly focused on leveraging AI technologies to enhance the capabilities of IDS, addressing limitations of traditional approaches and exploring novel solutions to emerging threats.

One prominent trend is the integration of advanced machine learning techniques with IDS to improve detection accuracy and adaptability. Research into reinforcement learning, for instance, is exploring its potential to create IDS that can continuously learn and adapt to evolving attack strategies. Reinforcement learning models can optimize their detection policies based on feedback from interactions with the environment, potentially leading to more effective and autonomous security systems.

Another emerging trend is the application of federated learning in IDS, which allows multiple decentralized systems to collaboratively train a global model without sharing sensitive data. This approach addresses privacy concerns and enables the development of robust models that benefit from diverse data sources while maintaining data confidentiality. Federated learning can enhance the generalization of IDS models and improve their ability to detect sophisticated attacks across varied environments.

Hybrid approaches combining AI with traditional IDS methods are also gaining attention. By integrating signature-based detection with machine learning algorithms, these hybrid systems aim to leverage the strengths of both approaches. For example, AI can enhance signature-based methods by identifying novel attack patterns that do not match existing signatures, thereby creating a more comprehensive detection framework. This hybridization can provide a balanced solution, combining the reliability of signature-based systems with the adaptability of AI-powered methods.

5.2 Recommendations for Future Research

While AI-powered IDS have shown promising results, several areas warrant further investigation to address existing challenges and optimize these technologies. One key area of research is improving the interpretability and transparency of AI models. Developing methods that make complex models more understandable and actionable for security professionals is crucial for enhancing trust and usability. Research into explainable AI (XAI) techniques tailored for IDS can bridge the gap between advanced model capabilities and practical decision-making.

Another important area is the enhancement of model robustness against adversarial attacks. As cyber threats evolve, the ability of AI models to withstand adversarial manipulation and maintain reliable performance is essential. Research into adversarial training techniques, as well as the development of novel defense mechanisms, can contribute to building more resilient IDS.

Furthermore, scalability remains a significant challenge, particularly for large-scale deployments. Research into efficient algorithms and hardware acceleration can address computational resource constraints and facilitate the deployment of AI-powered IDS in resource-constrained environments. Exploring edge computing solutions, where AI models are deployed at the edge of the network, can also offer scalable alternatives for real-time threat detection.

Finally, ongoing research into the integration of AI with emerging technologies, such as blockchain and quantum computing, presents opportunities for novel security solutions. Blockchain technology can provide decentralized and tamper-proof data sources for training AI models, while quantum computing may offer new approaches to encryption and threat detection.

5.3 Summary of Findings

The performance analysis of AI-powered IDS reveals several key insights into their effectiveness and challenges. AI techniques, particularly machine learning and deep learning, offer substantial improvements in detection accuracy, adaptability, and the ability to identify novel attack patterns compared to traditional methods. Case studies and real-world examples demonstrate the practical benefits of AI-powered IDS in enhancing threat detection and response capabilities.

However, the implementation of AI-powered IDS is accompanied by challenges related to model training, scalability, and interpretability. Issues such as data quality, overfitting, computational resource requirements, and the need for transparent decision-making processes are critical considerations for the successful deployment and operation of AI-based systems.

The future directions for AI in IDS include advancements in machine learning techniques, hybrid approaches, and the exploration of new technologies. Recommendations for future research emphasize the need for improved model interpretability, robustness against adversarial attacks, and scalable solutions for large-scale deployments.

AI-powered IDS represent a significant advancement in cybersecurity, offering enhanced capabilities for detecting and mitigating sophisticated threats. The continued evolution of AI technologies, coupled with ongoing research and development, holds promise for addressing current challenges and shaping the future of intrusion detection. The insights gained from performance analysis and research will guide the development of more effective and resilient security solutions, contributing to the ongoing evolution of the field.

Rreferences

1. H. Zhang, J. Zhao, and G. Wu, "A survey on network anomaly detection with machine learning algorithms," *IEEE Access*, vol. 8, pp. 105683–105700, 2020.
2. C. C. Ko, J. H. Lin, and C. H. Liu, "Anomaly detection in computer networks based on deep learning techniques," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 214–227, Mar. 2020.
3. A. P. G. Armitage and N. H. F. Jones, "Machine learning for intrusion detection: An overview," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2678–2692, 2021.
4. L. Zhao, K. Wang, and Y. Liu, "A deep learning-based approach for anomaly detection in network traffic," *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 2910–2922, Sep. 2021.
5. M. A. Ahmed, M. M. H. Kamel, and J. M. H. Iqbal, "Evaluation of machine learning techniques for network intrusion detection systems," *IEEE Access*, vol. 9, pp. 14350–14361, 2021.
6. J. Yang, W. Ma, and X. Zhao, "A survey of deep learning for network intrusion detection systems," *IEEE Access*, vol. 8, pp. 105457–105473, 2020.
7. M. A. K. P. Singh and J. L. Smith, "Hybrid intrusion detection systems: Combining signature and anomaly detection techniques," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 1, pp. 45–58, Jan. 2021.
8. R. M. A. Gomez and H. M. B. Fernandez, "Comparative study of machine learning algorithms for IDS performance evaluation," *IEEE Transactions on Network and Service*

Management, vol. 17, no. 2, pp. 1751–1762, Jun. 2020.

9. L. Liu, Q. Zhang, and S. Yang, “Federated learning for privacy-preserving intrusion detection systems,” *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2937–2948, 2021.

10. J. A. Rodriguez and F. J. Castro, “Reinforcement learning for optimizing intrusion detection systems,” *IEEE Transactions on Neural Networks and Learning Systems*, vol. 31, no. 4, pp. 1104–1116, Apr. 2020.

11. S. M. Patel, M. S. Verma, and V. B. Singh, “Deep convolutional neural networks for network intrusion detection,” *IEEE Transactions on Cybernetics*, vol. 50, no. 7, pp. 3122–3135, Jul. 2020.

12. B. C. Wu, T. Z. Zheng, and J. H. Choi, “Explainable AI techniques for intrusion detection systems: A survey,” *IEEE Access*, vol. 9, pp. 18842–18856, 2021.

13. P. P. Lee and M. B. Kim, “Scalable anomaly detection in network traffic using AI-powered IDS,” *IEEE Transactions on Computers*, vol. 70, no. 4, pp. 530–542, Apr. 2021.

14. A. S. Kumar and D. R. K. Patel, “Performance evaluation of deep learning models for cybersecurity,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1158–1170, 2020.

15. T. J. Chen, H. L. Liu, and R. Y. Zhao, “The role of AI in enhancing traditional intrusion detection systems,” *IEEE Transactions on Network and Service Management*, vol. 18, no. 1, pp. 97–109, Mar. 2021.

16. Y. M. Wang, Z. X. Liu, and M. J. Yang, “Adversarial attacks and defenses in deep learning for IDS,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 33, no. 6, pp. 1254–1266, Jun. 2021.

17. R. K. Sharma and J. L. Wang, “Challenges and solutions in scaling AI-powered IDS for large networks,” *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1122–1135, Jun. 2021.

18. F. R. Gomez and C. Y. Zhou, “Adversarial training techniques for improving IDS robustness,” *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 2, pp. 298–310, Feb. 2021.

19. N. A. Brown and H. M. Jones, "Hybrid AI models for intrusion detection systems: A survey," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 830–843, 2020.

20. L. X. Yang, J. S. Li, and D. Q. Zhang, "The future of AI in cybersecurity: Emerging trends and research directions," *IEEE Access*, vol. 9, pp. 19637–19652, 2021.