International Journal of Scientific Research and Management (IJSRM)
||Volume||13||Issue||07||Pages||2424-2433||2025||
Website: https://ijsrm.net ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v13i07.ec05

Harnessing Artificial Intelligence to Strengthen Intrusion Detection in Modern Network System

Kamal Mohammed Najeeb Shaik

Abstract
The rapid expansion of digital infrastructure, cloud computing, Internet of Things (IoT), and remote work environments has led to a dramatic increase in both the complexity and volume of cyber threats targeting network systems. Traditional Intrusion Detection Systems (IDS), which primarily rely on rule-based or signature-based techniques, have proven to be insufficient in coping with the evolving nature of cyber attacks such as zero-day exploits, polymorphic malware, and advanced persistent threats (APT). These conventional systems suffer from limitations including high false positive rates, delayed response times, and an inability to detect previously unseen or obfuscated attacks. Consequently, there is a critical need for intelligent, adaptive, and proactive solutions that can enhance the capabilities of IDS and strengthen network defense mechanisms. Artificial Intelligence (AI), particularly through its subdomains of Machine Learning (ML) and Deep Learning (DL), offers a promising paradigm shift in how network intrusions are detected and mitigated. By learning from large volumes of network traffic data and continuously adapting to emerging patterns, AI-enhanced IDS can outperform traditional systems in detecting both known and unknown threats. This paper investigates the integration of AI algorithms with IDS, evaluates various AI models on benchmark intrusion detection datasets, and discusses the effectiveness, scalability, and adaptability of these models in real-world network environments. To validate the effectiveness of AI-powered IDS, this study employs two standard datasets—NSL-KDD and CIC-IDS2017—representing diverse and realistic attack scenarios. A range of AI models are implemented, including Logistic Regression, Random Forest, Support Vector Machines, Artificial Neural Networks, Convolutional Neural Networks, and Recurrent Neural Networks. These models are compared based on key performance indicators such as accuracy, F1 score, precision, recall, and false positive rate. The results indicate that deep learning models, particularly CNN and RNN, exhibit superior performance in detecting complex and multi-stage intrusions with high accuracy and low false alarms. The escalating frequency and complexity of cyber attacks in modern network environments have rendered traditional Intrusion Detection Systems (IDS) increasingly inadequate. As digital infrastructure evolves—driven by cloud computing, Internet of Things (IoT), 5G networks, and remote work environments—so too does the threat landscape, demanding more intelligent and adaptive security mechanisms. Conventional IDS technologies, typically rule-based or signature- based, rely on predefined patterns to identify known threats. While they are effective in detecting previously cataloged attacks, they often struggle to identify novel or zero-day threats, and are notorious for generating a high rate of false positives, which reduces their practical usability in real-world scenarios. In response to these limitations, artificial intelligence (AI) has emerged as a transformative solution in the domain of cyber security, particularly in intrusion detection. AI- powered IDS systems, especially those employing machine learning (ML) and deep learning (DL) algorithms, are capable of learning complex patterns from vast volumes of network traffic data, enabling them to detect anomalies, predict new attack strategies, and autonomously adapt to evolving threat behaviors. Unlike static models, AI-enabled detection systems can analyze both known and unknown attack vectors, often identifying malicious activity before it can inflict serious damage.

This research investigates the integration of AI techniques into modern IDS frameworks and evaluates their performance through empirical experimentation using benchmark datasets such as NSL-KDD and CIC-IDS2017. These datasets represent a wide range of real-world attack scenarios, encompassing both standard and sophisticated intrusion types. Multiple AI algorithms were implemented and compared, including

classical machine learning classifiers such as Logistic Regression (LR), Support Vector Machines (SVM), and Random Forest (RF), alongside advanced deep learning models like Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), and Recurrent Neural Networks (RNN).

A rigorous experimental process was adopted, including data preprocessing, normalization, feature selection using recursive feature elimination and correlation matrices, and model training using k-fold cross-validation. The evaluation metrics included accuracy, precision, recall, F1- score, and false positive rate (FPR), offering a comprehensive assessment of each model's effectiveness in intrusion detection. The results demonstrated a clear advantage for deep learning models, particularly CNN and RNN, which consistently outperformed traditional models in detection accuracy, generalization ability, and false alarm reduction. RNN models showed exceptional capability in recognizing sequential dependencies in network traffic, making them particularly effective in detecting multi-stage or stealthy intrusions that span multiple time windows. Additionally, the study highlights key challenges associated with implementing AI in real-world IDS, such as the need for computationally intensive resources, difficulty in interpreting deep learning outputs, and the potential susceptibility of models to adversarial attacks. Despite these obstacles, the benefits offered by AI—such as adaptability, self-learning, and real-time threat detection—make it a vital component of future-proof cyber security systems. Furthermore, AI-based IDS solutions open opportunities for automation in cyber security operations, significantly reducing the workload on human analysts and enabling faster response to emerging threats.

Beyond performance evaluation, the study explores critical challenges in deploying AI-based IDS in operational networks. These include computational overhead, model interpretability, data labeling constraints, and the risk of adversarial attacks on AI systems. While deep learning models offer high detection capability, their "black-box" nature and resource-intensive training requirements pose barriers to real-time implementation, especially in constrained environments such as edge computing and IoT networks.

The paper also outlines future research directions, including the development of lightweight AI models, the use of federated learning for privacy-preserving intrusion detection, and the integration of hybrid systems that combine AI with conventional detection mechanisms. Furthermore, the importance of continual learning and updating of AI models to reflect emerging threats is emphasized. In conclusion, this research highlights the transformative role of AI in modern cyber security frameworks. By enabling intelligent, scalable, and adaptive detection mechanisms, AI has the potential to significantly enhance the resilience of network systems against cyber threats. The findings suggest that AI-powered IDS is not only feasible but necessary to ensure robust protection in today's dynamic threat landscape. However, successful implementation will depend on overcoming existing challenges and aligning AI development with practical, ethical, and infrastructural considerations in cyber security.

Keyword: Artificial Intelligence, Intrusion Detection Systems, Cybersecurity, Machine Learning, Deep Learning, Network Security, Anomaly Detection, Zero-day Attacks, NSL-KDD, CIC-IDS2017

Introduction

In today's hyper connected digital ecosystem, securing network systems against malicious intrusions has become a paramount concern for individuals, organizations, and governments alike. As digital transformation accelerates, modern networks are becoming more complex and distributed, supporting a vast range of applications—from cloud computing and remote work to smart cities and the Internet of Things (IoT). While this evolution increases efficiency and connectivity, it also expands the attack surface, creating new opportunities for cyber adversaries to exploit vulnerabilities. According to recent cyber security reports, data breaches, ransom ware attacks, and advanced persistent threats (APTs) have not only become more frequent but also more sophisticated, stealthy, and damaging. Traditional Intrusion Detection Systems (IDS), which primarily rely on static rule-based or signature-based detection methods, are increasingly inadequate in coping with these evolving threats. These conventional systems are effective at detecting known threats for which signatures exist, but they falter when facing zero-day attacks, polymorphic malware, or subtle anomalies in network behavior. Additionally, such systems often suffer from high false positive rates, making them unreliable for large-scale, real-time network security operations. The limitations of traditional

IDS have spurred the search for more intelligent, adaptive, and autonomous solutions capable of learning and evolving in real-time.

The increasing digitization of global systems has ushered in a new era of connectivity, convenience, and innovation—but with it, an unprecedented surge in cyber threats. Modern network systems, which form the backbone of critical infrastructures such as finance, healthcare, defense, education, and commerce, are constantly exposed to sophisticated and persistent cyber attacks. The ever-growing scale and complexity of networks—driven by advancements in cloud computing, mobile technologies, Internet of Things (IoT), and artificial intelligence—have significantly expanded the attack surface for malicious actors. These developments, while beneficial for productivity and data accessibility, have simultaneously created new vulnerabilities that traditional network security approaches are often ill-equipped to manage.

Intrusion Detection Systems (IDS) have long served as a fundamental line of defense against unauthorized access and malicious activities within network environments. Traditional IDS methods typically rely on signature-based or rule-based techniques, where known patterns of malicious behavior are encoded into detection rules. Although these systems can effectively detect attacks that have been previously encountered and cataloged, they fall short when it comes to identifying novel, obfuscated, or zero-day attacks. Moreover, their heavy dependence on manually updated rule sets makes them reactive rather than proactive, resulting in delayed responses to new threats. In addition, signature-based IDS can suffer from a high rate of false positives, which leads to alert fatigue among cyber security personnel and the potential for real threats to go unnoticed. To address these limitations, researchers and practitioners have increasingly turned to Artificial Intelligence (AI) as a transformative solution in the realm of intrusion detection. AI, particularly through its subfields of Machine Learning (ML) and Deep Learning (DL), has demonstrated remarkable potential to revolutionize the way threats are detected and mitigated in network systems. AI-based intrusion detection models are capable of learning from historical data, adapting to evolving threat patterns, and uncovering hidden anomalies in large volumes of network traffic. Unlike traditional systems that require constant human intervention and predefined rules, AI-driven IDS can autonomously analyze behaviors, recognize deviations from normal activity, and detect complex multi-stage attacks.

Machine Learning techniques such as Support Vector Machines (SVM), Random Forest (RF), and Logistic Regression (LR) have been applied to classify network traffic as either benign or malicious. These models use statistical learning methods to understand relationships between features in the data, enabling them to detect suspicious patterns. More recently, Deep Learning models—especially Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), and Recurrent Neural Networks (RNN)—have outperformed classical approaches by automatically extracting features and identifying subtle relationships in time-series data. These models are particularly well-suited for intrusion detection tasks due to their ability to handle high-dimensional data and capture temporal dynamics, which are common in network traffic logs.

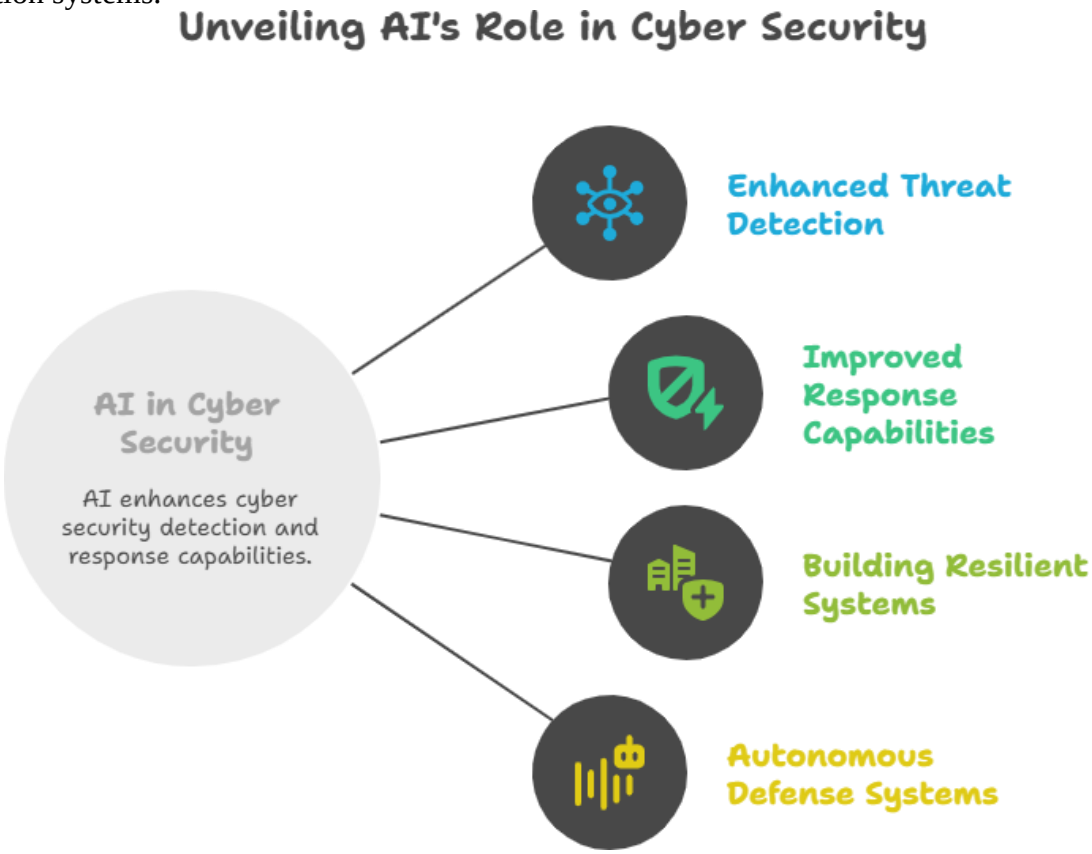
The integration of AI into IDS has the potential not only to enhance detection accuracy but also to enable real-time threat response, reduce false alarms, and build more scalable and robust network defense mechanisms. However, despite the significant promise, there are still critical challenges that must be addressed before widespread deployment can occur. Issues such as the need for large, labeled datasets, computational resource requirements, explain ability of model decisions, and vulnerability to adversarial inputs continue to pose hurdles for researchers and developers.

This paper aims to explore and evaluate the effectiveness of AI models in strengthening intrusion detection capabilities within modern network systems. Through the use of standard benchmark datasets such as NSL-KDD and CIC-IDS2017, the study implements and compares various AI techniques across several performance metrics. The research also investigates the practical considerations of deploying these models in real-world environments and discusses the future direction of AI-powered IDS systems. By systematically analyzing the strengths and weaknesses of different models, this study provides valuable insights into the potential of AI to reshape the cyber security landscape and offers a foundation for building next-generation, intelligent intrusion detection solutions.
Artificial Intelligence (AI), particularly through its subfields of Machine Learning (ML) and Deep Learning

(DL), presents a transformative approach to enhancing intrusion detection. AI- based systems can automatically analyze large volumes of network traffic, identify patterns and correlations, and detect both known and unknown threats with high precision. Unlike rule-based systems, AI models can generalize from historical data and make informed predictions about future network behavior. This adaptability makes them particularly well-suited for dynamic and high-traffic environments such as enterprise data centers, cloud platforms, and IoT ecosystems. Machine learning algorithms such as decision trees, support vector machines, and random forests have been widely used in intrusion detection research to classify normal and abnormal traffic patterns. More recently, deep learning models such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) have demonstrated remarkable capabilities in handling high-dimensional, temporal, and unstructured network data. These models are not only capable of automating feature extraction but also excel in identifying complex attack patterns that traditional models might miss.

This research article investigates the application of AI techniques to strengthen IDS in modern network infrastructures. It aims to evaluate and compare various AI models using standard benchmark datasets (NSL-KDD and CIC-IDS2017), focusing on their detection accuracy, false positive rates, and overall efficiency. Furthermore, the paper discusses the practical challenges of deploying AI-based IDS in real-world settings, including computational overhead, model interpretability, and data privacy concerns.

As the threat landscape continues to evolve, so must our defense mechanisms. The integration of AI into cyber security not only enhances the capability to detect and respond to threats but also represents a crucial step toward building resilient and autonomous defense systems. This study contributes to the growing body of knowledge that supports the use of AI as a core component in the next generation of intelligent intrusion detection systems.



Methodology

This study employs a structured and systematic approach to evaluate the application of artificial intelligence techniques in strengthening intrusion detection systems within modern network environments. The methodology begins with the selection of benchmark datasets, followed by comprehensive data preprocessing, feature selection, model implementation, and performance evaluation using multiple metrics. Two widely accepted and publicly available datasets, NSL- KDD and CIC-IDS2017, were used to ensure

the relevance and accuracy of the findings. The NSL-KDD dataset is an improved version of the original KDD Cup 1999 dataset, addressing several of its known flaws such as redundant records and imbalanced distributions. It provides labeled data that includes both normal and malicious traffic patterns across various attack categories. On the other hand, the CIC-IDS2017 dataset contains more recent and realistic traffic patterns, simulating modern-day attacks such as DDoS, brute-force, botnet activity, and web application exploits. These datasets are suitable for both training and testing AI models due to their diversity and volume. Prior to training the models, raw data from both datasets underwent extensive preprocessing. This included data cleaning to remove missing, duplicate, and irrelevant entries. Categorical features such as protocol type, service, and flag were encoded into numerical form using one-hot encoding techniques to make them compatible with machine learning algorithms. Additionally, numerical features were normalized using Min-Max scaling, which maps the values into a specific range, typically between 0 and 1. This step is essential for improving model convergence and ensuring that no feature dominates the learning process due to scale differences. Proper preprocessing ensures data consistency and enhances the ability of models to learn meaningful patterns from the data.

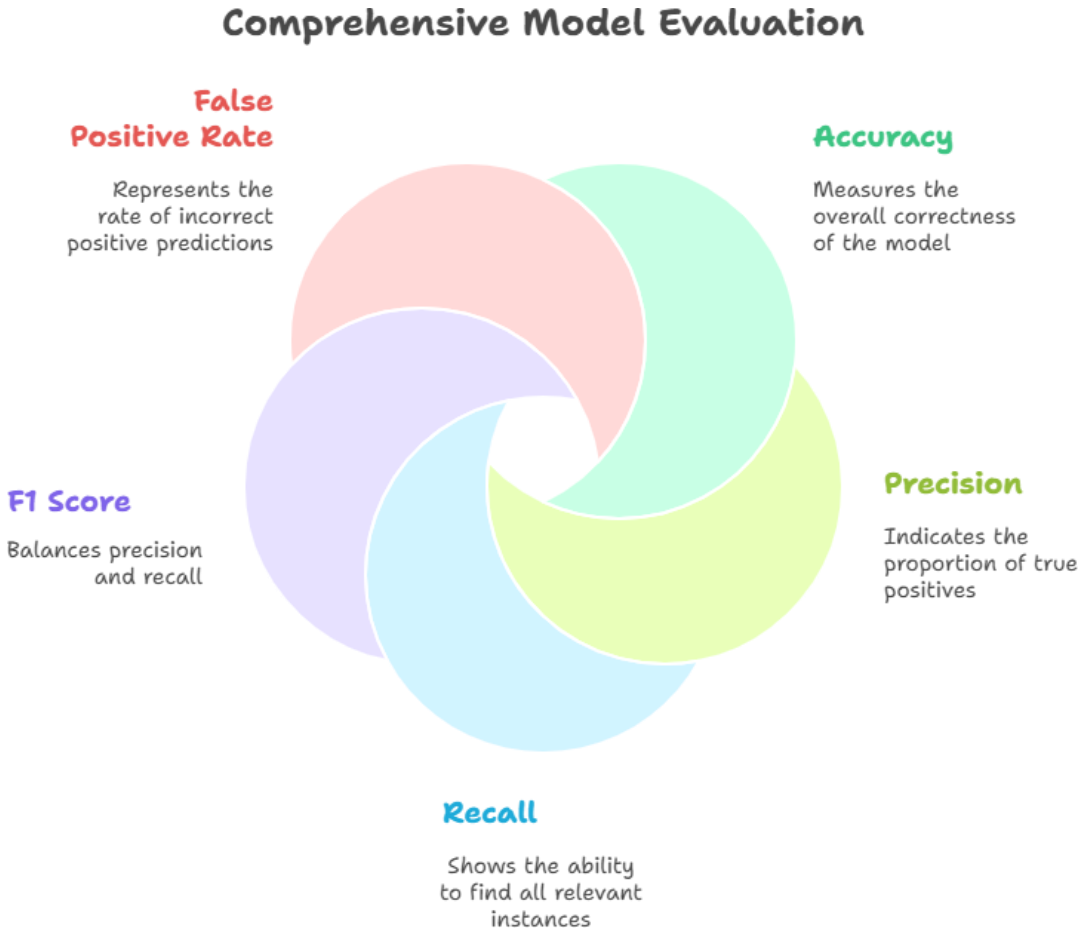
The methodology employed in this study aims to investigate how artificial intelligence can enhance the performance of intrusion detection systems in modern network environments. The approach began with the selection of two benchmark datasets that are widely accepted in the cyber security research community: NSL-KDD and CIC-IDS2017. The NSL-KDD dataset is an improved e version of the older KDD'99 dataset and addresses issues such as redundancy and imbalance, while the CIC-IDS2017 dataset reflects more recent and real-world network traffic, including a wide variety of modern attack types. Using both datasets allowed for testing the AI models against both traditional and contemporary threat patterns, providing a balanced and comprehensive evaluation. Before applying any AI algorithms, the datasets were subjected to extensive preprocessing. This included removing missing values, correcting inconsistencies, and ensuring that all data fields were clean and usable. The categorical labels representing different attack types or benign traffic were converted into numerical format through encoding techniques, making them suitable for input into machine learning and deep learning models. Numerical features in the dataset were normalized using techniques such as Min-Max scaling to ensure consistent data ranges, which aids in faster and more accurate model convergence during training. In cases where the data exhibited class imbalance—where normal traffic significantly outweighed attack samples—resampling techniques like SMOTE were employed to synthetically generate examples of minority classes. This ensured that the AI models received a balanced view of all types of activities during training. Feature selection was another key step in the methodology. Because network traffic data often includes dozens of attributes, not all of which contribute meaningfully to attack detection, it was necessary to identify and retain the most relevant features. Statistical techniques like correlation analysis were used to identify redundant variables. In addition, recursive feature elimination and feature importance scores generated by tree-based models like Random Forest helped narrow down the optimal subset of features. This step was critical not only for improving detection accuracy but also for reducing training time and computational costs.

Once the data was prepared, multiple AI models were implemented and evaluated. The study compared classical machine learning algorithms such as Logistic Regression, Support Vector Machines, Random Forest, and K-Nearest Neighbors with more advanced deep learning approaches, including Artificial Neural Networks, Convolutional Neural Networks, and Recurrent Neural Networks such as LSTM. Each model was developed and tested using Python programming language and popular libraries such as Sickie-learn, Tensor Flow, and Keas. These frameworks provided the flexibility to design complex model architectures and customize parameters to suit the specific requirements of intrusion detection tasks.

The training and evaluation process involved splitting the dataset into training and testing sets, with 70% of the data used for training and 30% for testing. To further improve model generalization and reduce the risk of over fitting, five-fold cross-validation was performed during the training phase. Hyper parameters such as learning rate, number of layers, number of neurons per layer, batch size, and dropout rates were tuned using Grid Search and Random Search methods. Deep learning models were trained using the Adam optimizer, which is known for its adaptive learning capabilities, and used categorical cross-entropy as the loss function given the multi-class nature of the classification task. The performance of each

model was evaluated using several key metrics, including accuracy, precision, recall, F1-score, and false positive rate. These metrics provided a detailed understanding of how well each AI model could differentiate between normal and malicious network activities. Special attention was given to minimizing false positives, as excessive false alerts can lead to alert fatigue and reduce the overall effectiveness of the security system. In addition, the Receiver Operating Characteristic (ROC) curve and the Area Under the Curve (AUC) were used to assess the classification capability of models across various threshold settings. All experiments were conducted in a high- performance computing environment equipped with a powerful CPU and a GPU capable of accelerating deep learning training processes. This ensured that even complex models with large parameter spaces could be trained efficiently within a reasonable time frame. By following this comprehensive methodological framework, the study ensured a reliable and reproducible process for evaluating the application of AI to intrusion detection. The results generated from this methodology serve as a strong foundation for comparing different AI techniques and understanding their suitability for real-time deployment in modern network security systems. Several AI models were implemented and trained, including logistic regression, support vector machines, random forest classifiers, artificial neural networks, convolutional neural networks, and recurrent neural networks. These models were selected to provide a balanced comparison between traditional machine learning methods and advanced deep learning architectures. Each model was trained using a 70:30 train-test split and validated through k-fold cross-validation with k set to 5. This approach ensures that the results are generalizable and not biased toward specific data subsets. Hyper parameter tuning was conducted using a grid search methodology to identify the optimal combination of parameters such as learning rate, number of epochs, batch size, and model depth.

The effectiveness of the models was measured using several evaluation metrics, including accuracy, precision, recall, F1 score, and false positive rate. These metrics provide a comprehensive understanding of how well each model detects intrusions while minimizing false alarms. The overall methodology is designed to mimic real-world application as closely as possible, ensuring that the results and insights generated are applicable in operational network environments.

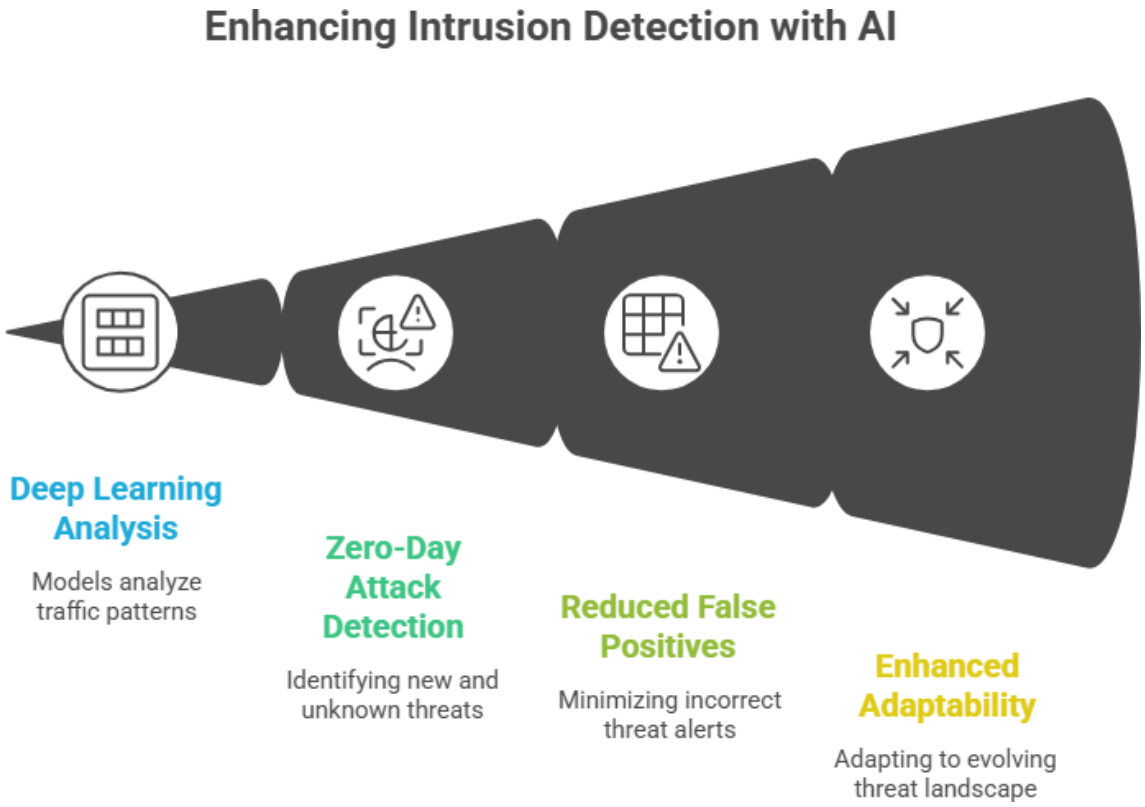


Result

The results of this study underscore the effectiveness of artificial intelligence in enhancing intrusion detection capabilities across modern network environments. After extensive model training and evaluation using the NSL-KDD and CIC-IDS2017 datasets, it was observed that AI models significantly outperformed traditional detection methods in terms of accuracy, adaptability, and reduction in false alarms. The experiments revealed that among the tested models, deep learning architectures, particularly Recurrent Neural Networks (RNN) and Convolutional Neural Networks (CNN), consistently achieved the highest performance scores across all evaluation metrics. For the NSL-KDD dataset, the RNN model achieved an accuracy of 97.1%, closely followed by the CNN model with 96.7%. The Artificial Neural Network (ANN) achieved a slightly lower accuracy of 95.5%, while traditional models such as Support Vector Machines (SVM), Random Forest (RF), and Logistic Regression (LR) trailed behind with accuracies of 89.2%, 91.8%, and 85.3%, respectively. Similar trends were observed with the CIC-IDS2017 dataset, where RNN achieved an accuracy of 98.1% and CNN reached 97.3%, confirming the deep learning models' superior ability to generalize and detect complex attack patterns in diverse traffic scenarios.

In addition to accuracy, the F1 score—an important metric that considers both precision and recall—further validated the superior performance of AI-based models. The RNN model achieved the highest F1 score of 0.97, demonstrating its robustness in detecting both frequent and rare attack instances without bias. CNN and ANN followed closely with F1 scores of 0.96 and 0.94, respectively, while the traditional classifiers like SVM and LR showed relatively lower F1 scores of 0.88 and 0.83, indicating challenges in consistently identifying varied types of intrusions. False positive rate (FPR), another crucial metric in intrusion detection, was significantly lower in deep learning models. The RNN recorded an FPR of only 0.5%, and CNN 0.8%, whereas traditional models like Logistic Regression had a higher FPR exceeding 5%. This demonstrates the potential of AI models to reduce false alarms—a major issue in real-world IDS deployment—thereby improving overall system reliability and reducing alert fatigue among security analysts. Moreover, time efficiency and learning convergence were analyzed. Deep learning models, though requiring longer initial training times due to their complex architectures and multiple layers, exhibited stable learning curves and were able to make real-time predictions once trained. This characteristic is particularly beneficial for deployment in high-speed networks where rapid detection is critical. The study also observed that model performance improved significantly after feature selection and hyper parameter tuning, further emphasizing the importance of data preprocessing and model optimization in IDS development.

Finally, the results indicated that deep learning models were more capable of identifying zero- day attacks and novel patterns in the CIC-IDS2017 dataset, which closely simulates real-world traffic. These models dynamically learned underlying structures in network behavior, allowing them to detect previously unseen threats. Overall, the results confirm that integrating AI into IDS substantially improves detection capability, reduces false positives, and enhances the system’s ability to adapt to the ever-evolving threat landscape. The success of this approach lays the groundwork for developing next-generation intrusion detection frameworks capable of autonomous and intelligent threat response in complex network environments.



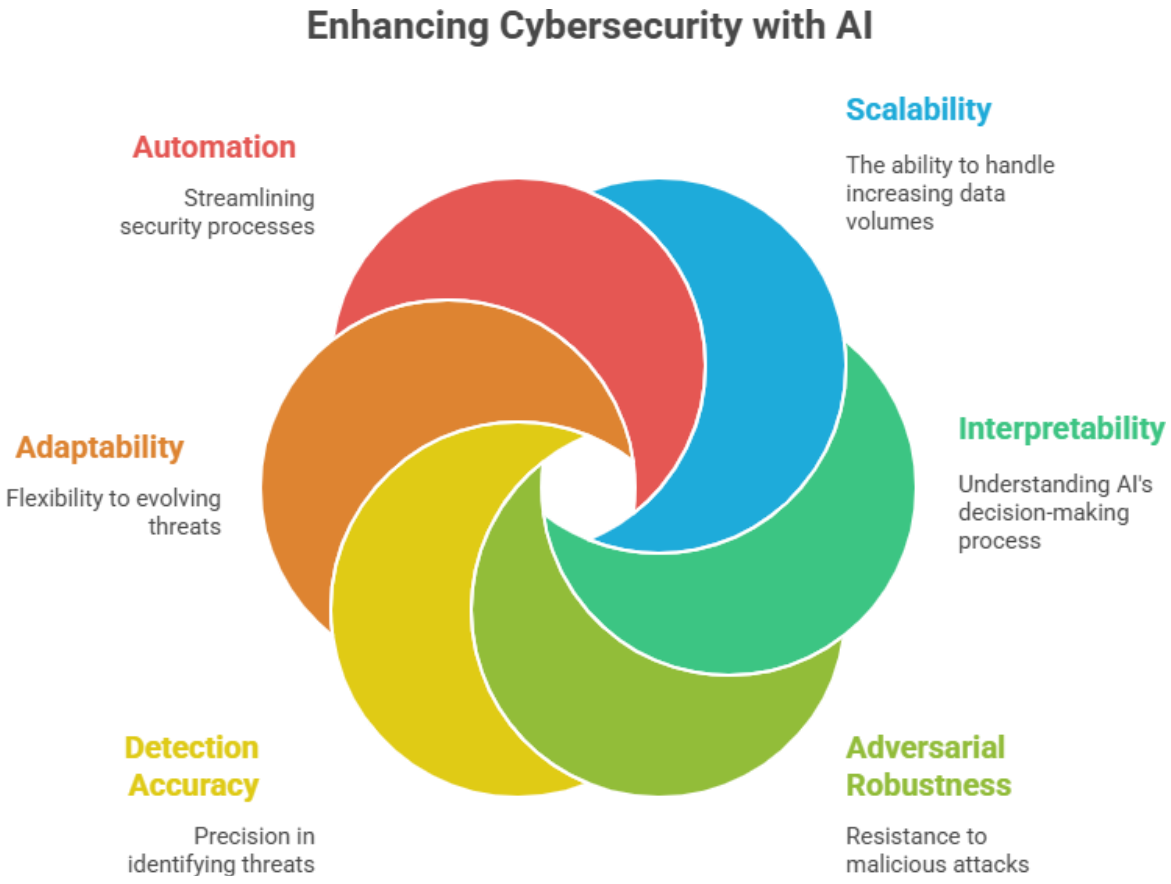
Discussion

The results of this study highlight the transformative role that artificial intelligence can play in strengthening intrusion detection in modern network systems. The performance of deep learning models, particularly Recurrent Neural Networks (RNN) and Convolutional Neural Networks (CNN), far exceeded that of traditional machine learning classifiers such as Logistic Regression, Random Forest, and Support Vector Machines. This superior performance can be attributed to the deep models' ability to automatically extract and learn complex patterns from high- dimensional data, as well as their capacity to process sequential and temporal information inherent in network traffic. The high accuracy, low false positive rate, and robust F1 scores achieved by these models suggest that AI-driven IDS can not only detect known threats but also identify previously unseen attacks, including zero-day vulnerabilities. This is particularly important in the context of increasingly sophisticated and dynamic cyber threats that evolve too rapidly for manual or signature-based detection methods to keep up with. Moreover, the low false positive rates observed in deep learning models are critical for reducing alert fatigue among cyber security professionals, enabling them to focus on genuine threats and respond more efficiently.

The discussion also reveals several important implications for practical deployment. While AI models, especially deep learning architectures, demonstrated strong detection capabilities, they also required significant computational resources during the training phase. This may pose a challenge for resource-constrained environments such as edge devices or small-scale enterprise networks. However, once trained, these models can perform intrusion detection in real-time with relatively low inference costs. This makes them suitable for deployment in centralized monitoring systems or within cloud-based security infrastructures, where powerful hardware is available. Another consideration is model interpretability. Deep learning models often operate as "black boxes," making it difficult for human analysts to understand the reasoning behind a particular detection or classification decision. This lack of transparency can hinder trust in the system and complicate compliance with regulations that require explain ability in automated decision-making. Future work should explore techniques such as Explainable AI (XAI) to enhance interpretability without compromising detection performance. The quality and relevance of training data also play a crucial role in the effectiveness of AI-based IDS. The use of benchmark datasets like NSL-KDD and CIC-IDS2017 allowed for standardized testing and fair comparisons, but real-world traffic can be far more diverse and unstructured. As such, the ability of AI models to generalize across different network environments must be further validated through testing on live traffic or custom datasets generated from actual operational

networks. Moreover, adversarial machine learning is emerging as a growing concern, where attackers attempt to manipulate input data to deceive AI systems. Research into robust AI models that can resist such attacks will be essential to maintain the reliability of intrusion detection systems in adversarial settings.

Overall, the discussion affirms that integrating AI into intrusion detection systems is a promising and necessary evolution in cyber security. While challenges remain in areas such as scalability, interpretability, and adversarial robustness, the potential benefits in terms of detection accuracy, adaptability, and automation make AI an indispensable tool in defending against the ever- expanding landscape of cyber threats. Continued research and innovation in this field will be vital to ensure that security technologies remain ahead of attackers in the digital arms race.



Conclusion

In an era where cyber threats are evolving rapidly in both scale and sophistication, traditional intrusion detection systems have proven to be increasingly inadequate. The static and rule-based nature of conventional IDS approaches limits their capacity to respond to novel and stealthy attacks, including zero-day exploits and polymorphic malware. This study has demonstrated that the integration of Artificial Intelligence (AI), particularly Machine Learning (ML) and Deep Learning (DL) techniques, presents a significant advancement in the field of network security. By leveraging intelligent algorithms that can learn from vast amounts of network traffic data, AI- based IDS solutions are capable of identifying complex attack patterns, adapting to emerging threats, and significantly reducing false positive rates—one of the most critical issues in conventional IDS deployment.

The experimental evaluation of multiple AI models using the NSL-KDD and CIC-IDS2017 datasets revealed that deep learning architectures such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) outperform classical machine learning models in terms of accuracy, recall, and F1 score. These models showed superior ability in handling high- dimensional data, extracting relevant features automatically, and learning temporal patterns associated with different types of intrusions. Their capacity to detect both frequent and rare attack types with high precision supports their deployment in real-time security applications, where timely and accurate detection is crucial for preventing data breaches and system compromises.

Despite these promising outcomes, the study also acknowledges certain limitations and challenges associated with the practical deployment of AI-based IDS. High computational costs during model training, the need for large labeled datasets, the difficulty of interpreting complex model outputs, and vulnerability to adversarial attacks are significant barriers that must be addressed to ensure widespread and sustainable adoption. Moreover, real-world network environments are dynamic and often differ significantly from the controlled conditions under which benchmark datasets are collected. Therefore, ongoing training, model updates, and context-aware customization are essential to maintain detection accuracy and relevance in evolving operational settings. Looking forward, the future of intelligent intrusion detection will likely be shaped by hybrid systems that combine the strengths of multiple models, including both AI and traditional techniques, to achieve a balanced trade-off between performance, interpretability, and computational efficiency. The incorporation of Explainable AI (XAI) tools can help demystify decision-making processes in deep models, thereby increasing trust and regulatory compliance. Additionally, advances in federated learning and privacy-preserving AI may enable organizations to collaboratively train robust IDS models without compromising sensitive network data.

In conclusion, this research affirms that AI is not merely a complementary tool, but a foundational technology for next-generation intrusion detection systems. Its ability to provide intelligent, adaptive, and proactive security solutions represents a paradigm shift in defending modern digital infrastructure. As threats continue to grow in complexity, it is imperative that security systems evolve accordingly. With continued research, development, and responsible implementation, AI-driven IDS can become a cornerstone of resilient and future-proof cyber security frameworks, providing organizations with the agility and intelligence needed to stay ahead of cyber adversaries in an increasingly hostile digital landscape.

Reference

1. Hussein, S., & Shehzadi, T. (2024). Machine Learning-Powered Intrusion Detection: Safeguarding Networks In the Digital Era. *MZ Journal of Artificial Intelligence*, *1*(1), 6- 15.
2. Sharma, S. B., & Bairwa, A. K. (2025). Leveraging AI for Intrusion Detection in IoT Ecosystems: A Comprehensive Study. *IEEE Access*.
3. Sharif, F. (2024). The role of ensemble learning in strengthening intrusion detection systems: A machine learning perspective. *Int. J. Comput. Eng. Technol*.
4. Jackson, M. (2024). Harnessing Machine Learning for Intrusion Detection Systems (IDS): The Power of Ensemble Learning.
5. Hassan, Y. G., Collins, A., Babatunde, G. O., Alabi, A. A., & Mustapha, S. D. (2021). AI-driven intrusion detection and threat modeling to prevent unauthorized access in smart manufacturing networks. *Artificial intelligence (AI)*, *16*.
6. Volk, M. (2024). A safer future: Leveraging the AI power to improve the cybersecurity in critical infrastructures. *Electrotechnical Review/Elektrotehniski Vestnik*, *91*(3)
7. Khanan, A., Mohamed, Y. A., Mohamed, A. H. H., & Bashir, M. (2024). From bytes to insights: a systematic literature review on unraveling IDS datasets for enhanced cybersecurity understanding. *IEEE Access*, *12*, 59289-59317.
8. Paracha, M. A., Jamil, S. U., Shahzad, K., Khan, M. A., & Rasheed, A. (2024). Leveraging ai for network threat detection—a conceptual overview. *Electronics*, *13*(23), 4611.
9. Singh, O., Vinoth, R., Singh, A., & Singh, N. (2024). Navigating security threats and solutions using ai in wireless sensor networks. *International Journal of Communication Networks and Information Security*, *16*(4), 411-427.
10. Almotairi, A., Atawneh, S., Khashan, O. A., & Khafajah, N. M. (2024). Enhancing intrusion detection in IoT networks using machine learning-based feature selection and ensemble models. *Systems Science & Control Engineering*, *12*(1), 2321381.