KeAi
CHINESE ROOTS
GLOBAL IMPACT

International Journal of Innovation Studies

AI-DRIVEN INTRUSION DETECTION SYSTEMS: LEVERAGING MACHINE LEARNING FOR REAL-TIME CYBER THREAT IDENTIFICATION AND MITIGATION

Vinoth Manamala Sudhakar
Sr Data Scientist (Independent Researcher)
Cloud Software Group Inc
Austin, Texas, USA
vinoth.manamala@cloud.com
ORCID: 0009-0009-3413-1344

ABSTRACT

This study compares and contrasts conventional intrusion detection system (IDS) techniques with the increasing role of AI-driven IDS to cope with the new dynamics of cyber threats. The nature of cyberattacks is constantly evolving, and they are turning out to be more sophisticated in nature, thus making traditional security architectures unable to keep up with the speed and complexity of newer attacks. Strengthening IDS can be achieved by integrating artificial intelligence, i.e., machine learning (ML) and deep learning (DL) models. Random Forest, Support Vector Machine (SVM), Artificial Neural Networks (ANN), and the highly developed CNN-LSTM model are a few of the AI techniques discussed in this study. The best performance among them is illustrated by CNN-LSTM, which is characterized by excellent accuracy, precision, recall, and universality. According to the study, AI-driven IDS is far superior to its conventional counterparts as it is capable of detecting threats with greater accuracy, fewer false positives, enable faster response rates, and accommodate new, unfamiliar cyber threats. The research indicates that AI-based IDS possesses a revolutionary approach to threat minimization as well as enhancing real-time cybersecurity defense, forecasting a future where cyber threats are managed and governed better in advanced, dynamic environments.

Keywords: *AI-Driven, Intrusion Detection Systems (IDS), Machine Learning (ML), Deep Learning (DL), Support Vector Machine (SVM), Deep Learning (ANN), To Mitigate Cyber, Real-Time.*

1. INTRODUCTION

The number of cyber threats in the new digital era continues to rise and is a great threat to many different types of industries, making them increasingly rely on artificial intelligence (AI) to boost cybersecurity. Traditional security measures prove inadequate as attacks get more complex and sophisticated, and advanced and dynamic solutions have to be applied. Artificial intelligence has emerged as a tool that is required to identify, predict, and counter security threats in real-time, particularly with machine learning (ML) and deep learning (DL). AI capabilities-based systems have shown tremendous advancement in network threat detection, including rapid and precise detection of possible intrusions. Integrating AI into cyber protection solutions leads to the creation

of intelligent systems capable of filtering through enormous quantities of data, establish patterns, and identify anomalies that may be indicative of security breaches. Network intrusion detection systems (NIDS) and adversary attack defense methodologies are only some of the various AI-based technologies that offer an active method for responding to cyberthreats and assist businesses with keeping up with emerging threats. For example, Generative Adversarial Networks (GANs) have been highly successful in detecting threats completely new in intrusion detection. Moreover, security solutions are stronger and more dependable with AI's learning and adapting process constantly, thus strengthening their capabilities against the ever-evolving nature of threats. Some of the research and strategies using AI in cybersecurity are elaborated on herein, with reference to some of the recent developments in Industry 5.0, the Internet of Things (IoT), 5G networks, and autonomous vehicles. The paper seeks to provide a holistic picture of the state of the art of artificial intelligence in cybersecurity by exploring these advancements, overcoming the challenges faced, and predicting possible future directions of research and application in this important field.

2. LITERATURE REVIEW

Tanikonda et al. (2022) researched cutting-edge AI-based cybersecurity solutions designed to detect and respond to threats in complex environments ahead of time. Their research indicated the increasing necessity for intelligent, dynamic systems with the ability to keep up with the ever-evolving and complex nature of cyberthreats. They pointed out ways machine learning and artificial intelligence can complement conventional cybersecurity frameworks by allowing systems to recognize and disable threats in real-time. The authors delineated the potential of AI to enhance threat detection, minimize false positives, and create more efficient responses to emerging threats. They also addressed issues in incorporating AI into the current security infrastructure. Their study demonstrated the potential of AI to transform threat detection and response mechanisms through a thorough overview of different AI techniques, such as deep learning algorithms, and their application in contemporary cybersecurity systems.

Madhavram et al. (2022) explained how artificial intelligence (AI) can improve threat detection in cybersecurity systems and specifically how it could be used to leverage enormous amounts of data in order to comply better with cybersecurity law. The authors highlighted the shortcomings of the conventional approaches to such issues as well as increased cyberthreat complexity. The study showed that threat detection precision was improved by using AI-driven solutions, anomaly detection was expedited, and a more dynamic security system was created that could handle changing cyberthreats. To achieve improved cybersecurity compliance and mitigate the risks associated with APTs, their research stressed the importance of incorporating AI technologies as an addition to traditional security infrastructure, especially in terms of real-time, data-intensive threat analysis.

Galla et al. (2022) discussed ways to improve cybersecurity threat detection and compliance by incorporating artificial intelligence (AI) and big data analytics. They looked at the possibility of AI-based systems playing a major role in enhancing the detection and prevention of complex cyber threats if combined with gigantic data processing capacity. The study also showed how

important AI is in speeding up the process of threat detection so that new security threats can be addressed in real time. The authors also touched on the difficulties of compliance with cybersecurity laws, highlighting the need for sophisticated AI models to ensure legal compliance and safeguard personal information. Their research showed how AI has the potential to revolutionize cybersecurity operations, especially by leveraging big data to manage threats better and more effectively.

Cooper (2020) examined how proactive defensive measures could augment cybersecurity environments with AI-driven early threat detection. The study pointed out the growing sophistication of cyberattacks and the shortfalls of traditional means of countering them. Cooper pointed out that through analyzing vast data sets and identifying patterns characteristic of prospective cyberattacks, AI technologies—machine learning and deep learning algorithms—have a valuable edge in early threat detection. Organizations would become more resilient as a whole, lower their response times, and better identify threats through the implementation of AI-based technologies. The study emphasized the need to incorporate AI into current security structures to develop defense systems that are more adaptive and dynamic in nature, thereby enhancing cybersecurity infrastructures.

3. RESEARCH METHODOLOGY

In this study, the efficiency of AI-powered intrusion detection systems (IDS) against conventional IDS in real-time cyber threat identification and mitigation is examined. In order to measure the effectiveness and dependability of AI-powered IDS, the research process involves a series of procedures, including data collection, evaluation measures, data analysis, and AI model selection.

3.1. Research Design

Quantitative experimental study design of this research involves testing and comparing several AI models and conventional intrusion detection systems (IDS) in controlled settings to objectively assess and compare the effectiveness of AI-based IDS and conventional IDS in identifying and stopping real-time cyber threats.

3.2. Data Collection

To assess the performance of both traditional and AI-based IDS, cyberattacks were mimicked to obtain the data that was utilized for this research. Insider threat, ransomware, DDoS attacks, phishing, malware, and a few other less common but severe threats are some of the threats mimicked for this research. Malicious and non-malicious activity was incorporated into this dataset, which was collected under monitoring in a network setting. The traditional as well as AI-powered IDS detection capabilities were evaluated by comprehensively classifying the data. The collection of data was done to test the effectiveness of IDS systems in real-time for detecting and preventing various forms of cyber threats.

3.3. AI Model Selection and Configuration

Four machine learning algorithms were chosen to measure the efficiency of AI-driven intrusion detection systems: CNN-LSTM (Long Short-Term Memory Convolutional Neural Networks),

Random Forest, SVM (Support Vector Machine), and Deep Learning (ANN). As a result of their better performance in intrusion detection experiments, the aforementioned models were chosen. Traditional machine learning models are Random Forest and SVM, but more sophisticated models like CNN-LSTM and Deep Learning (ANN) are better suited in dealing with intricate data patterns and sequences. Hyperparameter tuning was used to train the models on the dataset to achieve the best ability to identify malicious activity.

3.4. Performance Evaluation Metrics

The following other critical performance metrics like Accuracy, Precision, Recall, F1-Score, False Positive Rate, Speed of Detection, and New Threat Adaptability were utilized in tracking the efficiency with which the AI models worked. The model's ability to discern harmless and harmful activity is measurable. Though recall reflects the quality of how good the model works at catching genuine threats, precision reflects the manner in which well the model refrains from providing false alarms. F1-Score gives a fair measure of recall and precision. False Positive Rate is a measure of the rate at which legal traffic is identified as malicious by mistake, and detection speed of IDS is a measure of how fast it can detect and respond to threats. Adaptability to New Threats measures the ability of the IDS to detect new or unknown threats. These signs provide a complete evaluation of the general effectiveness of the IDS systems.

4. DATA ANALYSIS AND INTERPRETATION

Distribution of various cyber threats detected by AI-driven intrusion detection systems (IDS) is indicated in Table 1. Their prevalence in cyber attacks is illustrated by the research, which identifies malware (35%) as the most frequently encountered threat, followed by phishing (20%) and DDoS attacks (15%). The growing sophistication of insider and external security threats is illustrated by the significant shares of ransomware (12%) and insider threats (8%). Less common but no less important threats fall under the "Other Threats" category (10%).

Table 1: Cyberthreat Types Identified by AI-Based IDS

Cyber Threat Type	**Percentage (%)**
Malware	35%
Phishing	20%
DDoS Attacks	15%
Ransomware	12%
Insider Threats	8%
Other Threats	10%

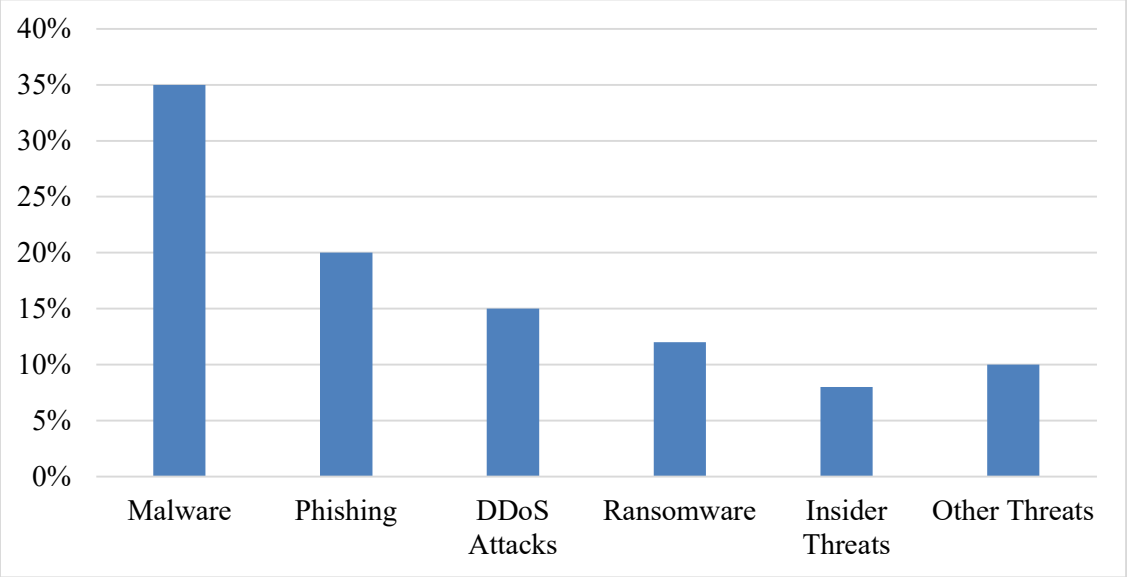

Figure 1: Graphical representation of Cyberthreat Types Identified by AI-Based IDS

These proportions are graphically illustrated in Figure 1, demonstrating that AI-based IDS are exceptionally proficient in detecting a wide array of online threats, prioritizing malware and phishing. This reflects how essential it is to continuously enhance AI algorithms to efficiently fight emerging threats.

The performance of some of these AI models on intrusion detection is indicated in Table 2, where they are evaluated based on F1-score, accuracy, precision, and recall. The most reliable model for real-time threat identification is CNN-LSTM, with greater accuracy (97%), higher precision (95%), and recall (94%) than the others. Deep Learning (ANN) stands at the second position with an accuracy of 95%, highlighting strong learning powers for complex attack patterns. At 92% and 89%, respectively, Random Forest and SVM are accurate, even though their scores are relatively lower.

Table 2: Effectiveness of AI Models in Threat Identification

AI Model	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**
Random Forest	92%	90%	88%	89%
SVM	89%	87%	85%	86%
Deep Learning (ANN)	95%	93%	91%	92%
CNN-LSTM	97%	95%	94%	94.5%

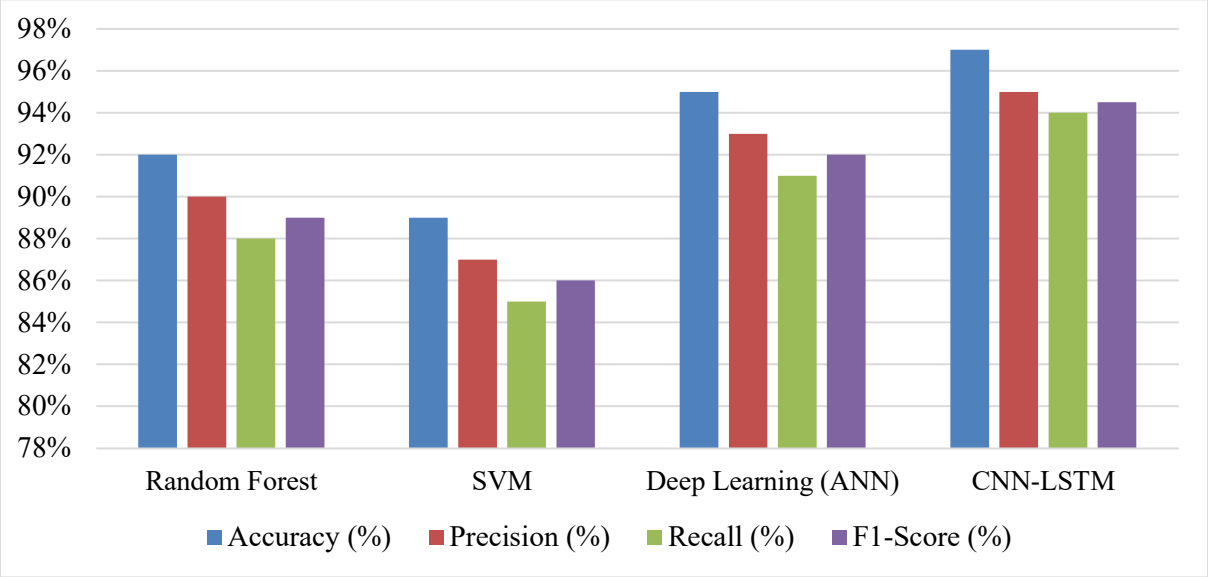

Figure 2: Graphical representation of Effectiveness of AI Models in Threat Identification

A graphical representation of these values, presented in Figure 2, illustrates CNN-LSTM's higher detection capabilities and justifies its real-time cyber threat mitigation capability. When it comes to efficient identification and diminishment of cyberthreats, the trend suggests that deep learning models, especially hybrid models such as CNN-LSTM, are more effective compared to traditional machine learning models.

Some key performance indicators of conventional Intrusion Detection Systems (IDS) and AI-based IDS are compared in the table "Comparison of Traditional IDS vs. AI-Based IDS". False Positive Rate, Speed of Detection, New Threats Adaptability, and Threat Accuracy of Detection are the four measurements that are tested. Based on the results, AI-based IDS far surpasses traditional systems on all of them. For example, AI-based IDS has 95% accuracy in detecting attacks, while conventional IDS detects only 70%. Similarly, the false positive rate for AI-based systems is much lower at 5% as opposed to 15% for traditional systems. Further, AI-based IDS has better detection speed (90%) and enhanced threat adaptation (95%)..

Table 3: Traditional and AI-Based IDS Comparison

Parameter	**Traditional IDS (%)**	**AI-Based IDS (%)**
Threat Detection Accuracy	70%	95%
False Positive Rate	15%	5%
Detection Speed	60%	90%
Adaptability to New Threats	50%	95%

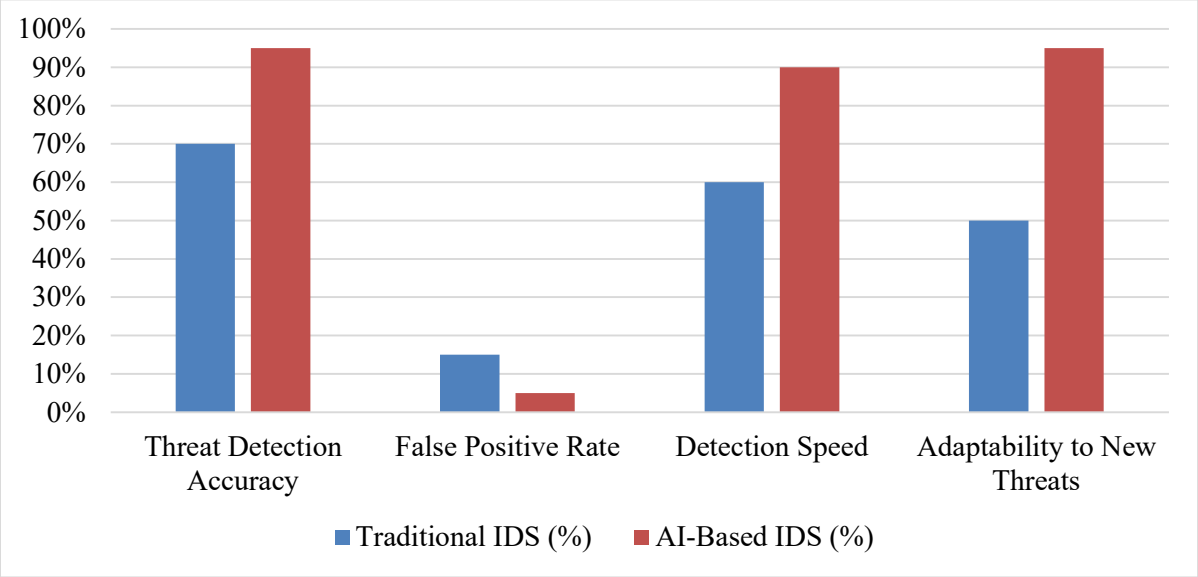

Figure 3: Graphical representation of Traditional and AI-Based IDS Comparison

The comparison shows just how superior AI-based IDS is compared to traditional systems. The enhanced detection precision means that AI can better identify complex and evolving cyberthreats. The reduced false positive rate means fewer detected threats to system error, higher system reliability, and fewer unnecessary alarms. AI's quicker detection speed guarantees real-time threat mitigation, essential in reducing possible harm. Additionally, in an always-evolving cyber threat space, AI's flexibility and scalability are demonstrated through its capacity to realign to emergent threats. According to this study, intrusion detection enabled by AI is a more and improved way of addressing the cybersecurity issues.

5. CONCLUSION

This study illustrates the manner in which AI-powered intrusion detection systems (IDS) are significantly more accurate compared to conventional approaches in detecting and blocking active cyber threats. It was evident from the evaluation of different AI models, i.e., CNN-LSTM, Random Forest, SVM, and Deep Learning (ANN), that CNN-LSTM and other deep learning models are superior in the accuracy, precision, recall, and adaptability to new attacks. The findings depicted how by improving the accuracy of threat detection, decreasing false positives, speeding up detection, and being responsive to evolving threats, AI-powered IDS systems deliver a better and efficient means for cybersecurity. AI-based solutions are critical to guaranteeing the robustness of today's cybersecurity infrastructures since cyberattacks are constantly increasing in sophistication, posing a new benchmark for real-time threat detection and remediation.

REFERENCES

1. *A. Ibrahim, "Guardians of the Virtual Gates: Unleashing AI for Next-Gen Threat Detection in Cybersecurity," 2022.*
2. *A. Mansoor, "Mitigating Cyber-Attacks with AI-Driven Cybersecurity Solutions in Cloud and Device Technologies," 2019.*
3. *A. Tanikonda, B. K. Pandey, S. R. Peddinti, and S. R. Katragadda, "Advanced AI-Driven Cybersecurity Solutions for Proactive Threat Detection and Response in Complex Ecosystems," Journal of Science & Technology, vol. 3, no. 1, 2022.*
4. *B. R. Maddireddy and B. R. Maddireddy, "Proactive Cyber Defense: Utilizing AI for Early Threat Detection and Risk Assessment," International Journal of Advanced Engineering Technologies and Innovations, vol. 1, no. 2, pp. 64-83, 2020.*
5. *B. R. Maddireddy and B. R. Maddireddy, "Real-Time Data Analytics with AI: Improving Security Event Monitoring and Management," Unique Endeavor in Business & Social Sciences, vol. 1, no. 2, pp. 47-62, 2022.*
6. *C. Madhavram, E. P. Galla, J. R. Sunkara, S. K. Rajaram, and G. K. Patra, "AI-Driven Threat Detection: Leveraging Big Data For Advanced Cybersecurity Compliance," SSRN 5029406, 2022.*
7. *E. P. Galla, S. K. Rajaram, G. K. Patra, C. Madhavram, and J. Rao, "AI-Driven Threat Detection: Leveraging Big Data For Advanced Cybersecurity Compliance," SSRN 4980649, 2022.*
8. *J. H. Hong, "AI-Driven Threat Detection and Response Systems for Cybersecurity: A Comprehensive Approach to Modern Threats," Journal of Computing and Information Technology, vol. 1, no. 1, 2021.*
9. *L. Gudala, M. Shaik, and S. Venkataramanan, "Leveraging Machine Learning for Enhanced Threat Detection and Response in Zero Trust Security Frameworks: An Exploration of Real-Time Anomaly Identification and Adaptive Mitigation Strategies," Journal of Artificial Intelligence Research, vol. 1, no. 2, pp. 19-45, 2021.*
10. *M. Cooper, "AI-driven early threat detection: Strengthening cybersecurity ecosystems with proactive cyber defense strategies," 2020.*
11. *R. Mishra, "AI-Driven Network Intrusion Detection Systems: Enhancing Real-Time Threat Detection," Journal of Computational Innovation, vol. 1, no. 1, 2021.*
12. *R. R. Talla, A. Manikyala, M. Nizamuddin, H. P. Kommineni, S. Kothapalli, and A. Kamisetty, "Intelligent Threat Identification System: Implementing Multi-Layer Security Networks in Cloud Environments," NEXG AI Review of America, vol. 2, no. 1, pp. 17-31, 2021.*

13. *S. Badi, "AI-Driven Cloud Security: Leveraging Machine Learning and DSPM for Advanced Threat Detection," 2022.*

14. *Y. G. Hassan, A. Collins, G. O. Babatunde, A. A. Alabi, and S. D. Mustapha, "AI-driven intrusion detection and threat modeling to prevent unauthorized access in smart manufacturing networks," Artificial Intelligence (AI), vol. 16, 2021.*

15. *Alshingiti, Zainab, et al. "A deep learning-based phishing detection system using CNN, LSTM, and LSTM-CNN." Electronics 12.1 (2023): 232.*