

# Detection of Cyber Attacks Using Artificial Intelligence

Research Methodology Literature Review Report

Course Code: A100

Instructor: Dr. Mohammed Anbar

Student Name: Rahaf Al-Saiari

Task Weight: 20%

## Introduction

With the advancement of technology and our growing reliance on the internet in almost all aspects of life, cyberattacks have become a serious threat to individuals and organizations. Traditional security methods are no longer sufficient, as attackers use increasingly complex and evolving techniques. For this reason, researchers have begun to use artificial intelligence (AI) for its ability to analyze massive amounts of data quickly and accurately, detecting any abnormal behavior in networks.

Artificial intelligence technologies enable security systems to take predictive and automated actions that intelligently address new attacks, helping to increase the speed and accuracy of threat detection. Additionally, integrating artificial intelligence into the security infrastructure gives organisations greater capability for rapid response and strengthens network resilience against any potential digital attacks.

This research explores how AI techniques are used to detect cyberattacks, highlighting the most effective approaches based on previous studies and their importance in enhancing cybersecurity and reducing modern attack risks.

## Research Objectives

- Identify the main AI methods and techniques used in detecting cyberattacks.
- Compare types of machine learning algorithms in terms of speed and accuracy.
- Highlight the challenges researchers face in this field.
- Propose future improvements for more effective attack detection.

## Literature Review

Through reviewing various studies in the field of cybersecurity, it was found that most rely on machine learning algorithms such as Decision Tree and SVM, which proved effective for specific types of attacks like DoS. Other studies employed deep learning models such as CNN and DNN, achieving higher accuracy but requiring more time and computational power.

Recent research has also focused on Internet of Things (IoT) security, as smart devices have become more vulnerable to new attacks. Many studies have used hybrid algorithms combining different techniques, though much of this research still depends on experimental datasets, reducing credibility in real-world applications. Nonetheless, there is a general consensus that AI significantly enhances security systems, making them faster and lighter for daily use.

*Additionally, the literature reveals a growing emphasis on Explainable AI (XAI) frameworks that make model decisions more interpretable. This development is crucial in cybersecurity because it helps analysts understand how an AI model identifies suspicious patterns, thus increasing transparency and trust in automated systems.*

*Comparative analyses show that while traditional algorithms like Random Forest and Naïve Bayes are faster and more efficient with smaller datasets, deep learning techniques handle complex, large-scale network data more effectively. Hybrid systems that combine both approaches emerging as the most promising solution, balancing speed, scalability, and precision in intrusion detection.*

## Discussion and Critical Analysis

*The reviewed studies highlight that data quality and diversity remain key factors influencing AI model performance. Many researchers emphasize the need for datasets that represent modern and evolving attack behaviors rather than outdated or limited benchmarks.*

*Another recurring issue is model generalization — systems trained on one dataset often perform poorly on another due to environmental differences. This suggests a need for continuous learning models capable of adapting dynamically to new threats.*

*Furthermore, most AI-based detection frameworks focus heavily on accuracy metrics while neglecting factors such as computational cost and real-time scalability. A more holistic evaluation that considers latency, resource consumption, and interpretability would provide a clearer picture of their practical*

## Selected Research Papers

| Title                                                                                                                                                | year | Authors                                                                                                                           | Methodology                                                                                                               | Key Results                                                                                            | Accuracy | Weaknesses                                                                                                                                                                  | Strengths                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------|------|-----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure                             | 2023 | Andrea Pinto, Luis-Carlos Herrera, Yezid Donoso, Jairo A. Gutierrez                                                               | This paper addressed the use of machine learning techniques such as Decision Tree and SVM for detecting DoS attacks.      | ML models achieve high performance in detecting DoS and R2L attacks on the NSL-KDD and CICIDS datasets | 91%      | Limited data size, as the models have not been tested on different environments or recent data, which reduces their ability to generalize.                                  | The methodology is clear, and a well-known dataset was used, and the results were analyzed statistically with precision. |
| Deep Learning-based Intrusion Detection Systems: A Survey                                                                                            | 2025 | Zhiwei Xu, Yujuan Wu, Shiheng Wang, Jiabao Gao, Tian Qiu, Ziqi Wang, Hai Wan, Xibin Zhao                                          | The paper addressed the use of CNN and LSTM models and their combination to analyze network traffic.                      | Deep learning outperforms traditional models in detecting modern threats                               | 95%      | High training cost as the model requires significant resources, and its performance has not been evaluated in different environments or when the nature of attacks changes. | Using the DNN model enabled the automatic extraction of important features from the data. .                              |
| A survey on intrusion detection system in IoT networks                                                                                               | 2025 | MM Rahman, S Al Shakil, MR Mustakim                                                                                               | Hybrid Algorithms (SVM + Autoencoder) for Anomaly Detection in IoT                                                        | Hybrid models are effective and provide accurate detection with a reasonable response time.            | 89%      | The complexity of the model makes its real-time application difficult, and it has been tested on non-real data, as it also requires high expertise in setup.                | The combination of methods contributed to improving the overall performance of the system.                               |
| Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction | 2024 | Md Alamin Talukder, Md Manowarul Islam, Md Ashraf Uddin, Khondokar Fida Hasan, Selina Sharmin, Salem A. Alyami, Mohammad Ali Moni | The paper used the Random Forest algorithm to analyze network data and predict attacks.                                   | Accurate results with a low error rate                                                                 | 92%      | Inefficient for large data as it is processed slowly, and performance decreases when dealing with massive or multi-pattern data.                                            | The model's flexibility and its ease of application to small datasets.                                                   |
| Intrusion Detection: A Comparison Study of Machine Learning Models Using Unbalanced Dataset                                                          | 2024 | Sunday Adeola Ajagbe, Joseph Bamidele Awotunde, Hector Florez                                                                     | The paper compared the performance of three algorithms: Naïve Bayes, SVM, and Random Forest in detecting attacks.         | The advantage of Random Forest in overall performance                                                  | 92%      | It does not include deep learning, and combining models to achieve better results has not been tried.                                                                       | The study is comprehensive and covers a detailed comparison between several techniques.                                  |
| A comprehensive survey of AI-enabled phishing attacks detection techniques                                                                           | 2020 | Abdul Basit, Maham Zafar, Xuan Liu, Abdul Rehman Javed, Zunera Jalil, Kashif Kifayat                                              | The paper proposed integrating NLP techniques with Machine Learning algorithms to analyze texts related to cyber attacks. | Speed in detecting phishing                                                                            | 97%      | The scope is narrow as it focuses on one type of attack and may not work efficiently on different types of attacks.                                                         | Combining natural language analysis with ML has enhanced the ability to accurately detect textual attacks.               |

## Conclusion

Artificial intelligence has made a significant impact on cybersecurity, especially in faster and more accurate attack detection. However, there remains room for improvement in developing high-efficiency systems capable of autonomously countering attacks without continuous retraining. The combined insights from previous studies suggest that future detection systems will rely on hybrid, real-time models integrating deep learning and machine learning for enhanced accuracy and adaptability. With such advances, cybersecurity protection will become more intelligent and effective. *Future research should focus on developing larger standardized and continuously updated datasets that reflect the dynamic nature of cyberattacks. Moreover, lightweight AI architecture optimized for IoT and cloud environments will make real-time detection more feasible. By combining human expertise with data-driven intelligence, AI can evolve from a reactive detection tool to a proactive prevention mechanism — ultimately shaping a more secure, resilient, and intelligent cyberspace.*

## References

- (Andrea Pinto, Luis-Carlos Herrera, Yezid Donoso, Jairo A. Gutierrez.2023). A Survey on Intrusion Detection Systems Based on Machine Learning. Sensors, 23(5), 2415.  
<https://www.mdpi.com/1424-8220/23/5/2415>
- (Zhiwei Xu, Yujuan Wu, Shiheng Wang, Jiabao Gao, Tian Qiu, Ziqi Wang, Hai Wan, Xibin Zhao. 2025). Deep Learning-based Intrusion Detection Systems: A Survey. arXiv preprint.  
<https://arxiv.org/abs/2504.07839>
- (MM Rahman, S Al Shakil, MR Mustakim. 2024). Survey on Intrusion Detection System in IoT Networks. ScienceDirect.  
<https://www.sciencedirect.com/science/article/pii/S2772918424000481>
- (Md Alamin Talukder, Md Manowarul Islam, Md Ashraf Uddin, Khondokar Fida Hasan, Selina Sharmin, Salem A. Alyami, Mohammad Ali Moni. 2024). Machine Learning-Based Network Intrusion Detection for Big and Imbalanced Datasets. Journal of Big Data.  
<https://journalofbigdata.springeropen.com/articles/10.1186/s40537-024-00886-w>
- (Sunday Adeola Ajagbe, Joseph Bamidele Awotunde, Hector Florez.2024). Intrusion Detection: A Comparison Study of Machine Learning Models. SN Applied Sciences.  
<https://link.springer.com/article/10.1007/s42979-024-03369-0>
- (Abdul Basit, Maham Zafar, Xuan Liu, Abdul Rehman Javed, Zunera Jalil, Kashif Kifayat. 2020). A Comprehensive Survey of AI-Enabled Phishing Attack Detection Techniques. Telecommunication Systems.  
[https://www.researchgate.net/publication/344583507\\_A\\_comprehensive\\_survey\\_of\\_AI-enabled\\_phishing\\_attacks\\_detection\\_techniques](https://www.researchgate.net/publication/344583507_A_comprehensive_survey_of_AI-enabled_phishing_attacks_detection_techniques)