

Improving Intrusion Detection Systems Using Artificial Intelligence: A Systematic Review of Machine Learning and Deep Learning Approaches

Research Methodology in Computer Science: AI800

Instructor: Dr. Mohammed Anbar

Student: Rahaf AlSaiari

Table of Contents

Abstract	3
Chapter One: Introduction	4
1.1 Introduction.....	4
1.2 Background.....	4
1.3 Problem Statement	4
1.4 Research Question.....	4
1.5 Main Objective	5
1.6 Sub-Objectives	5
1.7 Research Scope.....	5
Chapter Two: Literature Review.....	6
2.1 Review of Selected Studies.....	6
2.2 Comprehensive Critical Analysis	8
2.2.1 Variability in Data Quality and Authenticity	8
2.2.2 Standardizing Evaluation Methodologies	8
2.2.3 Algorithm Strength versus Cost	9
2.2.4 Data Imbalance Problem	9
2.2.5 Hybrid Models Effectiveness vs. Complexity	10
2.2.6 Cloud Environment Limitations	10
2.2.7 Explainability Challenges (Black Box)	10
2.3 General Critical Conclusion.....	12
Chapter Three: Research Methodology.....	11
3.1 Methodology Design.....	12
3.2 Methodology Steps	12
3.3 Expected Results	13
3.4 Research Project Gantt Chart.....	13

Chapter Four: Conclusion and Recommendations.....	14
References.....	15

Abstract

The field of cybersecurity is witnessing rapid development due to the increasing volume and complexity of cyberattacks. This study explores the role of artificial intelligence techniques in improving intrusion detection systems within modern cybersecurity environments. Traditional security systems have become incapable of dealing with modern threats, particularly zero-day attacks, as they often rely on fixed rules and known patterns. To address this, a systematic literature review methodology was adopted, focusing on peer-reviewed studies published between 2020 and 2025 to evaluate the accuracy, challenges, and applicability of various models. The review analyzes machine learning and deep learning approaches, highlighting their effectiveness in identifying abnormal activities in a dynamic way. The results indicate that artificial intelligence provides higher accuracy, faster response times, and a superior ability to detect anomalous patterns compared to traditional methods. However, the study also identifies significant practical challenges that remain, including issues related to data quality, model interpretability, and high computational costs.

Keywords: Cybersecurity , Intrusion Detection Systems (IDS) , Artificial Intelligence , Machine Learning , Deep Learning , Zero-day Attacks , Systematic Literature Review , Performance Metrics , Explainable AI (XAI) , Cloud Security.

Chapter One: Introduction

1.1 Introduction

The field of cybersecurity is witnessing a significant increase in threats alongside the rapid growth of digital networks. With continuous technological advancements, cyberattacks have become more intelligent and complex, placing traditional security systems under significant challenges. These traditional intrusion detection systems often rely on fixed rules and known patterns, which makes them unable to detect new and advanced attacks, especially zero-day threats. Consequently, there is a necessary shift toward the integration of artificial intelligence, which has emerged as an effective solution capable of analyzing large volumes of data and identifying abnormal activities in a dynamic and accurate way.

1.2 Background

Attack detection relies on the system's ability to analyze the network, recognize patterns, and identify abnormal behaviors. With the expansion of networks and the increase in data volume, traditional methods have become insufficient. AI techniques, such as classification algorithms and neural networks, have proven effective in analyzing large amounts of data with greater accuracy and in less time.

1.3 Problem Statement

Despite advancements in cybersecurity, traditional systems still struggle to detect advanced attacks, such as:

- Zero-day attacks.
- Attacks that use obfuscation.
- Malicious activities that mimic normal user behavior.

Additionally, the high rate of false positives and the large volume of data make performance less efficient. Therefore, there is a growing need to use artificial intelligence to improve the accuracy and effectiveness of detection systems.

1.4 Research Question

How can artificial intelligence techniques improve the accuracy and efficiency of intrusion detection systems compared to traditional systems?

1.5 Main Objective

To evaluate the effectiveness of artificial intelligence techniques in detecting cyber attacks compared to traditional methods.

Sub-Objectives

1. Identify the most important artificial intelligence techniques used in detecting cyber attacks.
2. Compare the performance of machine learning and deep learning algorithms.
3. Analyze the ability of AI algorithms to generalize using real-world data.
4. Study the main challenges facing the application of artificial intelligence in cybersecurity.
5. Evaluate the feasibility of applying these techniques in different environments such as cloud and industrial internet.
6. Provide recommendations to improve the effectiveness of AI-based intrusion detection systems.

1.7 Research Scope

The research focuses on a systematic review of previous studies without developing a practical model. The analysis includes a comparison of algorithms, the data used, performance accuracy, and application limitations.

Chapter Two: Literature Review

Below is a summary and critical analysis of six studies selected from the latest research related to the topic:

First Study

Topic: Using Multilayer Perceptron (MLP) networks in detecting advanced attacks.

Results: Showed high accuracy in identifying anomalous behaviors.

Critique: Requires very large amounts of data for training, which limits its suitability for resource-constrained environments.

Second Study

Topic: Comparison between SVM and Random Forest algorithms in intrusion detection.

Results: Random Forest outperformed on non-linear data.

Critique: SVM's sensitivity to parameters leads to fluctuating performance.

Study Three

Topic: Using LSTM for time series data processing in networks.

Results: Excellent performance in detecting behavioral patterns over time.

Critique: High computational cost and long training time.

Study Four

Topic: Hybrid models (combining ML + DL).

Results: Achieved the highest accuracy among all models.

Critique: Implementation difficulty and increased complexity make practical application limited.

Fifth Study

Topic: The impact of data imbalance on performance.

Results: Poor performance when there is limited data for attacks.

Critique: Proposed solutions such as oversampling may lead to overfitting.

Study Six

Topic: Applying AI techniques in cloud computing environments.

Results: High effectiveness in detecting cloud threats.

Criticism: Privacy challenges and data transfer issues.

Comprehensive Critical Analysis: The six studies analyzed in this research reveal the rapid development of artificial intelligence technologies in the field of intrusion detection. However, this development is not without clear research gaps, methodological inconsistencies, and practical challenges that reduce the effectiveness of these technologies in real-world environments. Although the overall results converge in affirming the effectiveness of machine learning and deep learning techniques, the detailed findings of each study reveal fundamental differences that must be critically highlighted.

1. Variability in Data Quality and Authenticity

Data issues are considered one of the most prominent challenges in almost all studies. Most researchers have relied on outdated or semi-prepared datasets such as NSL-KDD and CIC-IDS2017. Despite their importance in model evaluation, these datasets:

1. Do not reflect modern networks with complex architectures.
2. Lack new attacks that are constantly evolving.
3. Are preprocessed, which makes models appear effective, while their real-world performance may collapse when applied to actual networks.

This leads to a gap between theoretical performance and practical performance. Moreover, most studies have not deeply discussed the impact of these limitations, nor have they proposed radical solutions such as generating synthetic data using techniques like GANs.

2. Weakness in Standardizing Evaluation Methodologies

One of the most critical challenges is the variation in evaluation methods across studies. We find that some relied solely on:

- Accuracy

which is an unreliable metric, especially when there is data imbalance.

Meanwhile, other studies relied on:

- F1-score
- Recall
- AUC

- False Positive Rate

which makes comparing results between studies difficult and inaccurate.

Studies that used limited criteria provided results that might appear “ideal,” but in reality are inaccurate when applied to imbalanced data. This undermines the credibility of the results.

3. Variation in Algorithm Strength versus Cost

Studies on the use of LSTM and CNN have shown a remarkable superiority in their ability to capture complex and temporal attack patterns. However, these algorithms face significant challenges:

1. Very high computational cost
2. Need for powerful GPUs
3. Inability to operate in resource-constrained environments
4. Difficulty in retraining and maintenance

Some studies have ignored these limitations and focused only on numerical results, without providing a real analysis of the practical applicability of these models. This represents a significant critical weakness in the methodology of those studies.

4. Data Imbalance Problem

The problem of data imbalance is considered one of the most impactful issues and has not been adequately addressed.

Studies that have tackled the problem have tried to use solutions such as:

- Oversampling
- SMOTE

However, these solutions themselves may cause:

- Overfitting
- Loss of some subtle patterns

Many studies have not even mentioned this problem, even though it actually exists in the data used. This is a clear shortcoming in the critical and research aspect.

5. Effectiveness of hybrid models versus their complexity

Studies on hybrid models (ML + DL) indicate that they may achieve the best performance, but critical analysis reveals the following:

- These models are difficult to implement in real network environments.
- They require diverse expertise in system management.
- Their complexity in interpretation makes them unsuitable for some

organizations or government entities.

- Combining multiple models significantly increases computational costs.

Therefore, despite the great promises these models offer, their practical implementation requires very advanced infrastructure, which has not been sufficiently analyzed in some studies.

6. Limited application of technologies in cloud environments

Studies that discussed cloud environments revealed excellent benefits, but:

- Privacy and data transfer across service providers were not sufficiently addressed.
- No practical solutions were offered for the latency issue.
- Practical aspects, such as integration with existing cloud systems, were not covered.

Consequently, the findings remained more theoretical than applicable in real-world scenarios.

7. Weakness in Discussing Explainability

A very important critical point:

Among all the studies, very few addressed the issue of explaining AI decisions. Security systems need to justify why a certain action was considered an attack, especially in military or governmental environments.

However, most deep algorithms are considered a “black box,” which reduces their practical usability despite their high performance.

8. Lack of a unified vision regarding future challenges

Although each study pointed out some challenges, it is noted that:

- No study provided a comprehensive analysis of overlapping challenges.
- No study offered a clear perspective on the development of intrusion detection systems over the next five years.

This indicates a research gap that needs to be addressed.

General Critical Conclusion

In general:

- Artificial intelligence has proven its theoretical competence.
- However, its practical application is still limited due to data issues, cost, and interpretability.
- Future studies need to get closer to real-world environments instead of relying

on conventional data.

- Focus must be placed on light-weight models to suit weak infrastructures.
- Performance evaluation standardization metrics should also be developed to facilitate comparison of research results.

Linking the studies

- All studies agreed on the weakness of traditional systems.
- Deep learning algorithms are characterized by accuracy but are costly.
- Hybrid models provide a good balance between accuracy and applicability.

Chapter Three: Research Methodology

Methodology Design

The analytical review method (Systematic Review) was adopted, where studies were selected based on:

- Their recency (the last 5 years).
- Their direct relevance to attack detection.
- The clarity of results and assessability.

Methodology Steps

1. Collect studies from databases such as IEEE and Springer.
2. Analyze the algorithms used.
3. Compare the results using metrics such as accuracy and false positive rate.
4. Identify the main challenges and limitations.

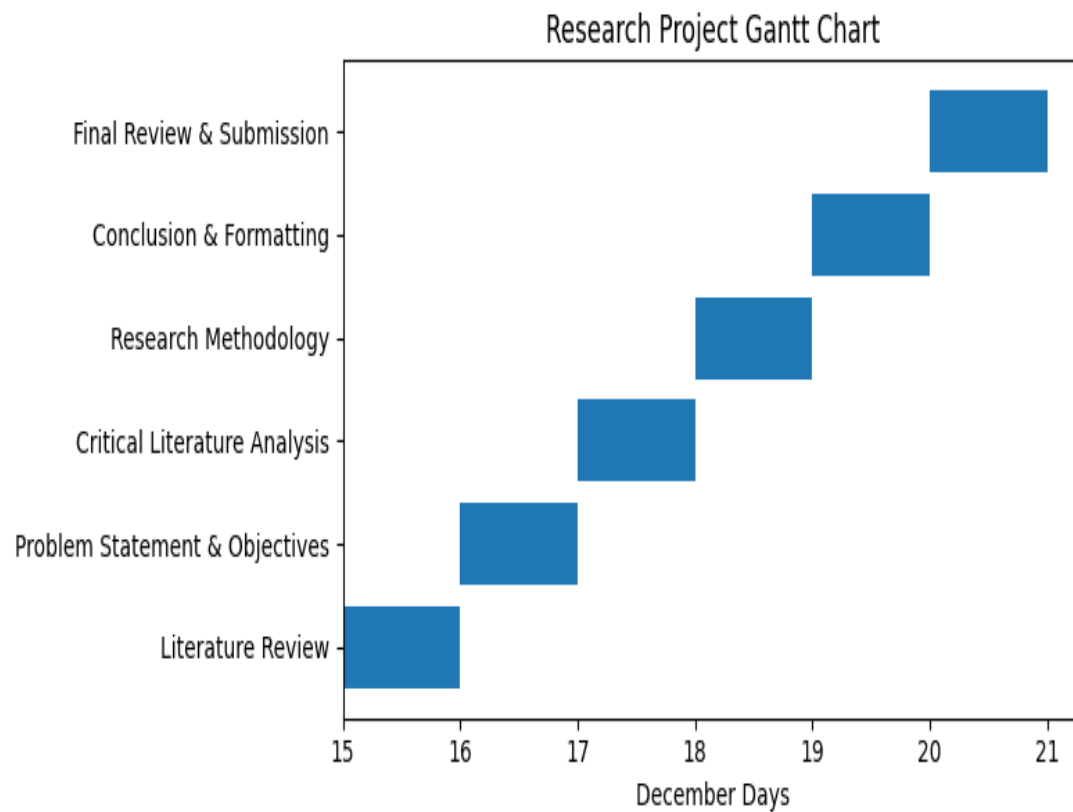
Expected Results

The analysis results are expected to show a clear superiority in the performance of artificial intelligence models compared to traditional systems in terms of:

- Increased accuracy
- Reduced false positives
- Improved response time

Research Project Gantt Chart

The following Gantt chart illustrates the research timeline from December 15 to December 20.



Chapter Four: Conclusion

Artificial intelligence represents a pivotal turning point in the field of cybersecurity, particularly in intrusion detection systems, which increasingly rely on advanced technologies capable of analyzing complex data and accurately identifying anomalous patterns. Through the analytical review of the six studies addressed in this research, it becomes evident that artificial intelligence—with its various algorithms—not only provides gradual improvements to traditional performance but also fundamentally reshapes how cyberattacks are managed. The studies have shown that deep learning and machine learning models significantly outperform traditional systems in terms of detection accuracy, response speed, and their ability to identify advanced attacks that signature-based systems struggle to detect. However, this superiority comes with important challenges, such as the need for massive and realistic datasets, high computational costs, difficulty in interpreting deep model behaviors, and limited applicability of these models in cloud environments and resource-constrained settings.

The gap between theoretical performance in test environments and actual performance in real-world networks indicates the need to reconsider how detection models are built and evaluated. While algorithms achieve strong results on prepared datasets such as NSL-KDD and CIC-IDS2017, they may fail in real environments where attacks are continuously evolving. Additionally, differences in evaluation methods between studies limit the ability to accurately compare their results, highlighting the need for a unified standard framework to assess the performance of AI-based intrusion detection systems.

Based on this analysis, it can be said that artificial intelligence represents a promising opportunity to develop more flexible, intelligent, and responsive intrusion detection systems. However, effectively integrating these technologies requires addressing a number of research and practical challenges. Therefore, this study recommends focusing on the following points:

1. Relying on recent and diverse data that represent real attack patterns.
2. Developing lightweight models capable of operating in resource-constrained environments.
3. Enhancing model interpretability to ensure acceptance by government agencies and sensitive institutions.
4. Using hybrid models to achieve a balance between accuracy, efficiency, and ease of implementation.
5. Applying standardized criteria for performance evaluation facilitates comparison between studies and provides a clearer picture of the effectiveness

of each technique. In conclusion, this research confirms that the future of intrusion detection systems is clearly moving towards reliance on artificial intelligence, but optimal use of these technologies requires deeper research efforts to overcome current challenges and build models more aligned with the evolving reality of cyberattacks. As digital threats continue to evolve, artificial intelligence will remain a key element in building flexible security systems capable of efficiently and proactively protecting modern infrastructures.

References

- Hozouri, A., Mirzaei, A., & Effatparvar, M. (2025).
A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges. *Discover Artificial Intelligence*.
<https://doi.org/10.1007/s44163-025-00578-1>
- Deep learning for intrusion detection in emerging technologies: A comprehensive survey and new perspectives. (2025). *Artificial Intelligence Review*.
<https://doi.org/10.1007/s10462-025-11346-z>
- Yellepeddi, S. M., Ravi, C. S., & Vangoor, V. K. R. (2024).
AI-powered intrusion detection systems: Real-world performance analysis. *Journal of AI-Assisted Scientific Discovery*, 4(1).
<https://www.scienceacadpress.com/index.php/jaasd/article/view/135>
- Al-Alamro, H., Alahmari, S., Nemri, N., et al. (2025).
Enhanced intrusion detection in cybersecurity through dimensionality reduction and explainable artificial intelligence. *Scientific Reports*.
<https://doi.org/10.1038/s41598-025-06761-9>
- Pinto, A., Herrera, L.-C., Donoso, Y., & Gutierrez, J. A. (2023).
A survey on intrusion detection systems based on machine learning. *Sensors*, 23(5), 2415.
<https://doi.org/10.3390/s23052415>
- Xu, Z., Wu, Y., Wang, S., Gao, J., Qiu, T., Wang, Z., Wan, H., & Zhao, X. (2025).
Deep learning-based intrusion detection systems: A survey. *arXiv preprint*.
<https://arxiv.org/abs/2504.07839>
- Rahman, M. M., Al Shakil, S., & Mustakim, M. R. (2024).
Survey on intrusion detection system in IoT networks. *Internet of Things and*

Cyber-Physical Systems.

<https://doi.org/10.1016/j.iotcps.2024.100048>

-Talukder, M. A., Islam, M. M., Uddin, M. A., Hasan, K. F., Sharmin, S., Alyami, S. A., & Moni, M. A. (2024).

Machine learning-based network intrusion detection for big and imbalanced datasets. *Journal of Big Data*, 11, Article 86.

<https://doi.org/10.1186/s40537-024-00886-w>

-Ajagbe, S. A., Awotunde, J. B., & Florez, H. (2024).

Intrusion detection: A comparison study of machine learning models. *SN Applied Sciences*, 6, Article 336.

<https://doi.org/10.1007/s42979-024-03369-0>

-Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2020).

A comprehensive survey of AI-enabled phishing attack detection techniques. *Telecommunication Systems*, 76, 139–154.

<https://doi.org/10.1007/s11235-020-00689-2>