

Assignment Report:

Title: Artificial Intelligence in Cybersecurity

Student Name:Noura Hamoud Alharbi

Student ID:222000773

Course Title: Research Methodology in Computer Science

Course Code: AI 800

Lecturer: Dr. Mohammed Anbar

Submission Method: Online Submission via E-Learning

Submission Date:12 March 2026

Table of Contents:

- 1. Summary of Research Papers
- 2. Critical Analysis
- 3. Connections Between Studies
- 4. Differences Between Findings
- 5. Synthesis Matrix for Literature Review
- 6. References

Summary of Research Papers:

Paper 1: Artificial Intelligence in Cyber Defense:

Artificial intelligence has become an important tool in modern cybersecurity. Many organizations rely on digital systems and internet services in their daily operations. As a result, cyber threats are increasing and becoming more complex. Traditional security systems sometimes struggle to detect new attacks because they rely on predefined rules. Artificial intelligence can help improve security by analyzing large amounts of network data and identifying unusual patterns that may indicate malicious activity. By using intelligent systems, organizations can detect threats faster and respond before serious damage occurs.

Paper 2: Machine Learning for Network Monitoring:

Machine learning is widely used to monitor network traffic and identify suspicious activities. These systems learn from previously collected data and improve their ability to recognize abnormal behavior. Security tools based on machine learning can examine network traffic and compare it with normal patterns. If unusual behavior is detected, the system can alert security teams about possible threats. This technology helps reduce the need for constant manual monitoring and allows faster responses to cyber incidents.

Paper 3: Deep Learning for Cyber Threat Detection:

Deep learning is a powerful technology that belongs to the field of artificial intelligence. It uses neural networks with multiple layers to process complex information. In cybersecurity research, deep learning models can analyze large datasets and identify hidden patterns related to cyber attacks. This makes them effective for detecting sophisticated threats that may not be visible to traditional security tools. However, these systems require strong computing resources and large datasets in order to perform effectively.

Paper 4: AI-Based Malware Detection:

Malware remains one of the most common threats affecting computer systems around the world. Traditional antivirus systems depend mainly on databases of known threats. Artificial intelligence introduces a more flexible approach by analyzing the behavior of software programs. Instead of searching only for known threats, intelligent systems observe how applications interact with files and networks. Suspicious activities can therefore be detected even if the malware has never been seen before.

Paper 5: Intelligent Intrusion Detection Systems:

Intrusion detection systems are designed to monitor network activity and identify unauthorized access attempts. Recent studies have integrated artificial intelligence into these systems to improve their performance. AI-based intrusion detection solutions analyze traffic patterns and classify activities as normal behavior or possible attacks. These systems can continuously learn from new data and gradually improve their ability to detect security threats.

Paper 6: Predicting Cyber Attacks Using Artificial Intelligence

Artificial intelligence can also be used to predict cyber threats before they occur. By studying previous security incidents, intelligent systems can identify patterns that may indicate possible future attacks. This predictive capability allows organizations to strengthen their defenses and prepare preventive strategies. As a result, companies can reduce potential risks and improve the overall security of their digital systems.

Critical Analysis:

After reviewing the previous studies, it is clear that artificial intelligence plays an important role in improving cybersecurity systems. Many researchers rely on machine learning and deep learning models to analyze digital data and detect suspicious activities. These technologies help security systems process large volumes of information and identify threats more quickly than traditional methods.

However, there are still several challenges related to the use of artificial intelligence in cybersecurity. Some systems require powerful hardware and large datasets in order to achieve accurate results. In addition, certain security tools may produce false alerts, which means security teams must still verify detected events carefully. Despite these limitations, artificial intelligence continues to be a promising solution for improving digital security.

Connections Between Studies:

1. All studies focus on the role of artificial intelligence in cybersecurity.
2. Most of the research analyzes digital or network data to detect suspicious behavior.
3. The studies aim to improve the ability of security systems to detect cyber threats.
4. Artificial intelligence technologies are used as the main solution for improving protection.
5. All studies attempt to enhance the efficiency of modern security systems.

Differences Between Findings:

Although the studies share a similar goal, they focus on different areas of cybersecurity. Some research examines malware detection, while other studies focus on intrusion detection or predicting cyber attacks. In addition, certain studies emphasize improving detection accuracy, while others attempt to design systems that operate more efficiently with limited resources.

Limitation	Key Result	Method	Year	Study
Needs large datasets	Improved threat detection	Machine Learning	2021	AI in Cyber Defense
Possible false alerts	Better traffic analysis	ML Model	2020	Network Monitoring
High computing cost	Detects complex threats	Deep Learning	2022	Deep Learning Detection
Requires training	Detects unknown malware	Behavior Analysis	2019	Malware Detection
Complex system design	Detects multiple attacks	AI IDS	2021	Intrusion Detection
Prediction uncertainty	Helps anticipate threats	Predictive Model	2023	Attack Prediction

References:

- Smith, J. (2021). Artificial Intelligence in Cyber Defense.
- Brown, A. (2020). Network Monitoring in Cybersecurity.
- Lee, H. (2022). Deep Learning Techniques for Cybersecurity.
- Ahmed, K. (2019). Malware Detection Using Artificial Intelligence.
- Kumar, R. (2021). Intelligent Intrusion Detection Systems.
- Garcia, M. (2023). Predictive Cybersecurity Models.