Laboratory Activity -2 ***22nd Jan 2026***

Note: ***An open session will be held on Microsoft Teams. Please ensure that you submit your work through it, as lab activities that are not submitted will not be marked.***

Contents

The Relationship Between Artificial Intelligence and Cybersecurity

Introduction

Artificial Intelligence (AI) enhances cybersecurity by enabling faster and more accurate detection of complex cyber threats that traditional systems often miss. Using techniques like machine learning, AI can analyze large datasets and adapt to evolving attack patterns.

However, AI also creates new risks, as attackers can exploit the same technologies to launch more advanced attacks. Therefore, balancing AI's defensive advantages with its challenges is essential for effective cybersecurity.

Definition of AI and Its Core Concepts

Artificial Intelligence (AI) is the branch of computer science that focuses on creating systems capable of performing tasks that typically require human intelligence. These tasks include reasoning, learning, problem-solving, perception, and language understanding.

Figure 1:AI

Key AI Techniques Relevant to Cybersecurity

Machine Learning (ML)

ML is a subset of AI that allows systems to learn from data and improve performance without being explicitly programmed.

Cybersecurity Use Cases:

- Detecting malware and phishing attacks
- Identifying anomalous network behavior
- Predictive threat analysis

Deep Learning (DL)

DL is a subset of ML that uses multi-layered neural networks (deep neural networks) to model complex patterns in data.

Cybersecurity Use Cases:

- Advanced intrusion detection
- Image/video analysis for surveillance

- Natural language processing for threat intelligence

Definition and Goals of Cybersecurity

Cybersecurity is the practice of protecting computers, networks, programs, and data from unauthorized access, damage, or theft. It ensures that digital systems operate safely and securely against threats.

Goals (CIA Triad)

- Confidentiality – Ensuring data is accessible only to authorized users.
- Integrity – Maintaining the accuracy and reliability of data.
- Availability – Ensuring systems and data are accessible when needed.

Figure 2:Cybersecurity

Common Cyber Threats

Malware

Malicious software designed to damage, disrupt, or gain unauthorized access to systems. Examples include viruses, worms, trojans, and spyware.

Phishing

Fraudulent attempts to obtain sensitive information (like passwords or credit card numbers) by pretending to be a trustworthy entity, usually via email or fake websites.

Ransomware

Malware that encrypts a victim's files or systems and demands a ransom for their release.

Traditional Cybersecurity Approaches and Limitations

Role of AI in Cybersecurity

AI for Threat Detection

Anomaly Detection using ML

Machine learning algorithms analyze historical data to determine normal behavior in systems and networks. Any deviation, such as unusual login attempts or abnormal data transfers, is flagged as a potential threat. This allows for early detection of attacks that traditional rule-based systems might miss.

Intrusion Detection Systems (IDS)

AI-enhanced IDS can automatically identify suspicious activities like malware infiltration or unauthorized access. Unlike traditional IDS, AI can learn from past attacks and adapt to detect new types of threats effectively.

AI for Threat Prevention

Predictive Analysis of Attacks

AI models forecast potential attack vectors by analyzing patterns in cyber threats. This enables organizations to anticipate attacks and strengthen defenses proactively.

Automate Vulnerability Assessment

AI tools scan systems and applications to identify weaknesses or misconfigurations that attackers could exploit. This reduces the time needed for manual security audits and ensures continuous protection.

Conclusion

In conclusion, AI plays a crucial role in modern cybersecurity by improving threat detection, response, and prevention. While it offers significant advantages, it also introduces new risks, as attackers can exploit AI for sophisticated attacks. Effectively leveraging AI in cybersecurity requires careful management of these risks to build resilient and adaptive security systems.