9^{th} International Conference on

CONTROL AND OPTIMIZATION WITH INDUSTRIAL APPLICATIONS

Editors
Aliev Fikret (Azerbaijan)
Akdemir Ahmet Ocak (Türkiye)

Deputy Editors-in-Chief
Safarova Nargiz (Azerbaijan)
Dokuyucu Mustafa Ali (Türkiye)

ISBN 978 - 625 - 97879 - 3 - 0

MINISTRY OF DIGITAL DEVELOPMENT
AND TRANSPORT
OF THE REPUBLIC OF AZERBAIJAN

KATODER

PROCEEDINGS

of the

9^{th} International Conference on

CONTROL AND OPTIMIZATION WITH INDUSTRIAL APPLICATIONS

27-29 August, 2024
Istanbul, Türkiye

CONTENTS

The Role of Artificial Intelligence in Cyber Resilience of Cyber Physical Systems

Rashid Alakbarov
Institute of Information Technology
Baku, Azerbaijan
t.direktor_muavini@iit.science.az

Mammad Hashimov
Institute of Information Technology
Baku, Azerbaijan
mamedhashimov@gmail.com

***Abstract*—Lately, artificial intelligence (AI) technology has been extensively applied in the struggle against cyber threats in CPS. AI may improve system security by providing tools to quickly detect cyberthreats and automatically resolve them. Digitization of critical infrastructures (energy distribution networks, smart systems, oil and gas industry, water infrastructure, etc.) has increased their efficient management and at the same time, the number of cyber attackers on sensors, actuators, network and control equipment has also increased. Cyber security of critical objects can be ensured through AI. This article explores the role of AI in enhancing the cyber resilience of CPS. The article analyzes the advantages and disadvantages of using AI technologies in the security of Cyber-Physical systems. Mechanisms for detecting cyber threats in cyber-physical systems with the help of AI, predicting and preventing security threats have been proposed.**

***Index Terms*—artificial intelligence, cyber security, cyber physical systems.**

I. Introduction

Cyber-physical systems (CPS) connect digital and analogous devices, interfaces, networks, computer systems with the physical world. CPS is based on a computer system that processes information in the automotive, aviation, energy and other industries. These computer systems are used to perform specific tasks. CPS incorporates sensors, actuators and similar embedded systems that interact with the real world, as well as sophisticated software. CPS refers to the close interactions and relationships between cyber components such as sensor systems and physical components that form the origin of the Internet of Things [1], [2]. The main areas covered by CPS are shown below [2], [3]:

- In smart cities: Smart traffic management systems, Smart buildings and infrastructure, environmental monitoring and waste management, etc.
- In energy management: Supervisory Control And Data Acquisition (SCADA) systems, smart grid, production and distribution of electricity, and adaptation and optimization of its consumption;
- In the environment: monitoring of the environment in wide and diverse geographical areas (forests, rivers and mountains), early detection of natural disasters (forest fires);
- In intelligent transport management: operational management of complex traffic flow through real-time data sharing, accident prevention;
- In agriculture: precise farming, smart irrigation and more efficient distribution of nutrients (fertilization, nitrogen), improvement of crop production capabilities;
- In health care: real-time monitoring of patients' health and providing notification, telemedicine systems for remote delivery of medical services;

The interaction of the aforementioned areas with digital infrastructures exposes CPS to cyber threats and makes cyber resilience an important aspect of them. Increasingly sophisticated cyber threats, along with tranditional system vulnerabilities, posing significant challenges to CPS resilience [4].

II. Different Types of Attacks, Threats and Vulnerabilities in Cyber-Physical Systems

Below are some of the different types of attacks, threats, and vulnerabilities that compromise CPS [5]–[7]:

- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. DoS attacks aim to disrupt CPS availability at the expense of multiple system resources, whereas DDoS attacks use multiple compromised systems to intensify this effect. These attacks can cause significant interruptions to critical infrastructure, such as shutting down production lines or disordering power grids.
- Mal ware attacks. Mal ware, including viruses, worms, trojans, and ransom ware, can intrude CPS to steal data, disrupt operations, or control system functions. Mal ware can cause data corruption, loss of control over physical processes, and significant financial and reputational damage.
- Man-in-the-Middle (MitM) Attacks. In MitM attacks, attackers intercept and manipulate CPS components or connections between CPS and external networks. These attacks can result in data theft, unauthorized control of system operations, and injection of false information, compromising the integrity and reliability of the CPS.
- Advanced Persistent Threats (APTs). APTs are long-term and targeted attacks where cyber criminals intrude a system and collect data over a long period of time and compromise the integrity of the system. APTs can cause significant data exfiltration, disruption of critical services, and long-term damage to system integrity and reliability.

- Insider Threats. Insider threats include malicious actions by individuals with access to CPS within the organization. These threats can lead to data breaches, sabotage of system operations, and unauthorized access to vulnerable information.
- Zero Day Exploits. Zero-day exploits target unknown vulnerabilities in software or hardware and leave the system vulnerable until a patch is developed and deployed. Because these threats exploit un patched vulnerabilities, they can lead to significant damage and potentially cause widespread disruption and data corruption.
- Phishing and Social Engineering. Phishing and social engineering attacks trick individuals into revealing confidential information or taking actions that compromise CPS security. These attacks can lead to unauthorized access, data corruption, and the introduction of malware into the CPS.
- Software vulnerabilities. Bugs, flaws, or vulnerabilities in software code can be used by attackers to gain unauthorized access, disrupt operations, or steal data. Software vulnerabilities can compromise the integrity, availability, and confidentiality of CPS.
- Hardware Vulnerabilities. Deficiencies or weaknesses in the physical components of the CPS can be exploited to disrupt operations or gain control over system functions. Hardware vulnerabilities can lead to physical damage, disruption of operations, and unauthorized control of CPS.
- Communication Protocol Vulnerabilities. Secure communication protocols can be used to capture, modify, or insert data into CPS communication streams. These vulnerabilities can compromise data integrity, allow unauthorized access, and disrupt system operations.

Given the various types of attacks, threats and vulnerabilities mentioned above, cyber security is a critical concern in current digital age, with cyber-attacks posing significant risks to individuals, organizations and nations. Although traditional security methods are important, new countermeasures are needed to keep up with the dynamism of cyber threats. As cyber threats grow in complexity and frequency, traditional security measures often fail to provide adequate protection. AI offers advanced capabilities to detect and prevent cyber-attacks through sophisticated algorithms and real-time analysis. AI provides a promising solution by automating threat detection and response, increasing the accuracy and efficiency of cyber security systems. AI has emerged as a transformative force in enhancing the resilience of CPS. AI's ability to process large amounts of data, recognize patterns, and make autonomous decisions ensure new opportunities to protect these systems from cyber threats.

III. Applying Artificial Intelligence to Detect and Prevent Cyber Attacks

Signature-based detection systems are mainly used to ensure the cyber security of traditional CPS. These systems work by comparing an incoming package (of software) against a database of identified intimidations or malevolent code signatures. If any part of the code of the viewed program matches a known virus code (signature) in the database of antivirus programs, the antivirus program deletes the infected program, sends the program to "quarantine", or tries to restore the program by removing the virus itself from the program. This approach is actual against acknowledged intimidations, but insufficient against new and unidentified ones. Cyber criminals may effortlessly avoid signature-based detection systems by changing code in applications or creating new mal ware that is not available in the database. Analysis of cyber security issues for signature-based detection systems is mainly performed by engineers (security analysts). Security analysts manually used to review patterns or indicators of security breaches. This was time-consuming and also relied on the security analyst's expertise in identifying threats. Although signature-based detection systems are operative in specified circumstances, they are often inflexible and unable to recognize evolving threats. In order to solve the above mentioned problems, AI technologies have been used in recent times. Systems designed by people to facilitate the exchange of information, goods, and services have become an integral part of modern life, effectively forming a crucial infrastructure. These infrastructures encompass a range of networks, including transportation, communication, energy, and digital systems, which have evolved over centuries to meet the evolving needs of society. AI is a powerful intelligence tool that can effectively detect and prevent threats to the security of cyber-physical systems. Some of them are shown below [8]–[11]:

- Threat detection. AI has the ability to detect and automatically remediate cyber attacks on the network. If AI detects a threat in the system, it can take automatic actions such as blocking access to infected resources (hardware). AI can instantly access vast amounts of data and analyze specific data patterns to detect signs of an attack. It helps provide system defense mechanisms by automatically detecting threats in network traffic data.
- Anomaly detection: Anomaly detection embraces identifying deviations from established patterns of behavior. AI algorithms can analyze network traffic, user behavior and system logs to detect anomalies that could indicate a cyber-attack. For example, an AI system can detect unusual access attempts from unfamiliar locations or at unusual times and record them as potential security incidents.
- Attack prediction: AI is used to predict and prevent future attacks based on available data. It helps develop defense strategies against potential attacks based on analysis of past attack patterns and data. AI equipped with learning algorithms, can study data to identify new types of attacks and develop defense strategies against these attacks.
- Automation of routine processes. AI automates routine cyber threat detection processes. Systems can automatically update their defenses based on new threat information, allowing them to quickly respond to new

types of attacks. AI helps perform deep analysis and other defensive measures to defend against an attack, automatically applying security policies after detecting dangerous data.

- Incident Response: AI can automate the incident response process, reducing the time needed to mitigate the threat. AI-driven systems can generate alerts, prioritize them based on severity, and enable pre-defined response protocols.
- Behavioral Analysis: Behavioral analysis involves monitoring and analyzing the behavior of users and systems to detect suspicious activities. AI algorithms can determine baselines of normal behavior and detect deviations that could indicate a security breach. For example, an AI system can detect when a user is accessing sensitive information that they would not normally interact with and enable an alert for further investigation.
- Alert prioritization: Cyber security teams are often faced with a high volume of alerts, making it difficult to prioritize and respond to the most critical threats. AI algorithms can analyze alerts based on factors such as threat severity, potential impact on the organization, and historical data. This helps security teams focus on the most urgent and high-risk incidents.
- Mal ware detection. Machine learning algorithms are exploited by AI to identify both known and unknown mal ware threats and react to them. These algorithms examine huge volumes of data to distinguish patterns and irregularities that are hard for humans to identify. Analysis of mal ware behavior may determine new and unknown mal ware variations that cannot be detected through old-style antivirus software.
- Transaction monitoring: Financial institutions and e-commerce platforms use AI to detect fraudulent transactions. AI algorithms can monitor financial transactions in real-time to detect signs of fraud. By analyzing transaction patterns, such as the frequency and costs of transactions, AI systems can identify unusual activities that may indicate fraudulent behavior. For example, an AI system may detect that a user's spending behavior significantly deviates from their typical patterns and record the transaction for further investigation.
- Identity Verification: AI-powered identity verification involves the use of biometric data such as facial recognition and fingerprint scanning to verify the identity of users. This helps prevent identity theft and ensures that only authorized individuals can access sensitive information and conduct transactions.
- Vulnerability Assessment: AI algorithms can scan systems and applications for known vulnerabilities by comparing them to a database of known vulnerabilities, such as the Common Vulnerabilities and Exposures (CVE) database. AI can also identify potential vulnerabilities based on observed patterns in code or configuration.
- Detection of phishing attacks. Old-style approaches to phishing detection often rely on rule-based filtering or blacklisting to detect and obstruct identified phishing emails. Since these approaches are only actual against recognized attacks and not against newly created ones, they have limitations. Using machine learning algorithms AI-powered phishing detection solutions analyze the emails' content and structure in order to detect possible phishing attacks. These algorithms can learn from huge volumes of data to identify patterns and irregularities showing a phishing attack.
- Predictive Analytics: AI-powered predictive analytics can identify potential vulnerabilities before they are exploited by analyzing trends and patterns in cyber security data. For example, AI algorithms can predict what types of vulnerabilities will be targeted by attackers based on historical data and emerging threat intelligence.
- Implementation of AI in access control and authentication systems. Access control and authentication systems play an important role in ensuring the security of in- formation systems and data. They determine who has access to certain system resources and functions and verify that the user is the one who claims to be.

IV. Advantages and Disadvantages of Using Artificial Intelligence in Cyber Security

Applying AI in cyber security of CPSs has several advantages. AI ensures real-time threat detection and response. Second, AI can learn from experience and improve its skills or abilities over time. A number of important advantages of using AI in the field of cyber security are shown below [12], [13]:

- High level of security. AI technologies allow to implement security measures faster and more effectively by analyzing data in real-time. This helps to make the systems more secure.
- Real-time Analysis: AI systems can analyze large amounts of data in real-time and identify threats as they happen. This immediacy enables faster response to potential breaches.
- Data processing efficiency. AI has the ability to process and analyze larger amounts of data than humans, allowing it to identify complex or hidden threats.
- Anomaly Detection: AI can determine baselines of normal behavior and detect anomalies that may indicate cyber threats. Machine learning algorithms can identify patterns that would be difficult for humans to recognize.
- Speeding up the threat detection process. AI is capable of analyzing huge volumes of data in real time, providing faster and more productive threat detection than traditional methods. AI can respond faster to security incidents and prevent attacks from spreading.
- Adaptability: AI systems can adapt to the evolving cyber security landscape by learning from new data and emerging threats to be up-to-date and effective.
- Development of protection strategies. Due to its capability to learn from past cyber attack data, AI can predict future threats and help develop defense strategies. AI,

equipped with learning algorithms, can learn from past threats and perform higher levels of data analysis to detect new or evolving threats.
- Machine learning: Machine learning algorithms learn from historical data and adapt to new threats. The more data they process, the more improves their ability to distinguish between malicious and malicious activity.
- Automation of the analysis process. AI can automate the process of analyzing big data, which can reduce the time and resources spent on information processing. This is especially important in an environment where the volume of data is constantly increasing. AI reduces the workload of implementing security measures and protecting systems by automatically managing large amounts of data.
- Speed and Efficiency: Automated systems can immediately react to threats, isolate affected systems, block malicious IP addresses, and initiate other defensive measures immediately. This reduces the attackers' opportunity and minimizes potential damage.

Despite the advantages of AI technologies, the issues related to the use of these methods for malicious purposes have caused argument. Applying AI in cyber security tools also has its limitations and challenges. First, the security AI itself can be attacked and manipulated by malicious hackers. Second, AI can fail and misinterpret data, which can lead to wrong things being done or real threats being missed. Despite the significant advantages, several problems related to the use of AI in cyber security. While there are many benefits of applying AI in cyber security, there are also possible risks to consider. Below are some of them [14], [15]:

- Misuse of AI by attackers. Just as security professionals can use AI to combat cyber threats, attackers can also take advantage of AI technology to generate new types of attacks. This may include everything from creating more convincing phishing attacks to automating the process of seeking vulnerabilities in network systems.
- Data Quality and Quantity: AI systems rely on large volumes of high-quality data for training and operation. Inadequate or biased information can undermine their effectiveness.
- Incomplete Information: Incomplete information can lead to inaccurate detection of threats and wrong conclusions. Providing comprehensive data sets is crucial for full AI performance.
- Privacy issues. The use of AI to analyze large volumes of data may increase privacy concerns, particularly those related to personal data.
- Dependence on AI. While AI automates many aspects of cyber security, human control remains essential. Relying solely on AI without human intervention can lead to non-avoided threats and inadequate responses.
- With the increased use of AI in cyber security, there is a risk of over-dependence on technology, which can lead to people losing control over it.
- Lack of qualified specialists. Implementing and maintaining AI systems requires specialized knowledge and expertise, which can be a barrier for some organizations. Learning and working with AI requires high qualifications and specialized knowledge, which is currently in short supply in the labor market.
- Possibility of wrong decisions. AI can sometimes make wrong decisions, that is, it may consider normal user actions as security threats. This may cause the security system to be overloaded. AI can create new risks related to data security and protection. Algorithms are likely to make bad decisions, increasing the potential access by hackers to data and creating new threats to the protection of that data.
- Computing resources. AI requires powerful systems with large computing resources and memory resources to process and analyze huge volume of data. This can be problematic for organizations with limited funds.
- Integration with Existing Systems: Integrating AI with existing cyber security infrastructure can be complicated and requires a significant investment in time and resources.

V. Conclusions

This article examined the use of AI in cyber security tools of CPS. Proposals were made for the use of AI technologies in the identification and avoidance of cyber attacks. The advantages and disadvantages and problems of using AI in cyber security systems were highlighted. The purpose of this review article is to identify future research directions and to use machine learning, deep learning methods, neural networks, etc. to improve the efficiency, reliability and cyber resilience of cyber-physical systems. Future research work is to develop new methods and algorithms through AI tools.

Acknowledgment

This work supported by the Science Foundation of the State Oil Company of Azerbaijan Republic (SOCAR) (Contract No. 3LR-AMEA)

References

[1] T. Sanislav, and L. Miclea, "Cyber-physical systems - concept, challenges and research areas," Control Engineering and Applied Informatics, vol. 14, 2012, pp. 28–33.
[2] R. G. Alakbarov, and M. A. Hashimov, "Fog computing technology application in cyber-physical systems and analysis of cybersecurity problems," Problems of Information Society, vol. 13, pp. 23–29, 2022.
[3] C. Hong, "Applications of cyber-physical system: A literature review," Journal of Industrial Integration and Management, vol. 2, 2017, pp. 1–28.
[4] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, "Cyber-physical systems and their security issues," Computers in Industry, vol. 100, 2018. pp. 212–223.
[5] A. K. Tyagi, and N. Sreenath, "Cyber physical systems: Analyses, challenges and possible solutions," Internet of Things and Cyber-Physical Systems, vol. 1, 2021, pp. 22–33.
[6] M. Sagar, and C. Vanmathi, "Attacks on cyber physical system: Comprehensive review and challenges," I.J. Wireless and Microwave Technologies, vol. 5, 2022, pp. 53–73.
[7] J. A. Yaacouba, O. Salmanb, H. N. Nouraa, N. Kaanichec, A. Chehabb, and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," Microprocessors and Microsystems, vol. 77, 2020, pp. 103–201.

[8] N. B. Dokur, “Artificial Intelligence (AI) Applications in Cyber Security,”
[9] M. F. Rafy, “Artificial Intelligence in Cyber Security.”
[10] A. J. G. Azambuja, C.Plesker, K. Sch?tzer, R. Anderl, B. Schleich, and V. R. Almeida, “Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0-A Survey”, Electronics, vol. 12, 2023, pp. 1–18.
[11] N. Capuano, G. Fenza, V. Loia, and C. Stanzione, “Explainable artificial intelligence in cybersecurity: A Survey,” IEEE Access, vol. 10, 2022, pp. 93575–93600.
[12] R. Calderon, “The benefits of artificial intelligence in cybersecurity,” Economic Crime Forensics Capstones, vol. 36, 2019, pp. 1–22.
[13] L. Lazic, “Benefit From AI in Cybersecurity”, The 11th International Conference on Business Information Security (BISEC-2019), 18th October 2019, Belgrade, Serbia.
[14] J. Wilkins, “Is artificial intelligence a help or hindrance,” Network Security, vol. 2018, 2018, pp. 18–19.
[15] M. F. Ansari, B. Dash, P. Sharma, and N. Yathiraju, “The impact and limitations of artificial intelligence in cybersecurity: A literature review,” International Journal of Advanced Research in Computer and Communication Engineering, vol. 11, 2022, pp. 81–90.