APPLICATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN SECURITY OF CYBER-PHYSICALSYSTEMS

Rashid Alakbarov and Mammad Hashimov

Institute of Information Technology, Ministry of Science and
Education Republic of Azerbaijan

ABSTRACT

Cybersecurity questions of cyber-physical systems (CPS) have become ever more vital in recent times. Advances in technology and digitization have posed new weaknesses in CPS and cyber attackers take advantage of it. Viruses, malware, and sophisticated forms of cyberattacks have become a dangerous reality for critical infrastructure CPS. 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 theoretical foundations, application fields, and AI conceptual models. It analyzes the benefits and shortcomings of applying AI technologies to the security of the abovementioned systems. Mechanisms for detecting cyber threats in cyber-physical systems with the help of AI and predicting and preventing security threats are proposed.

KEYWORDS

Artificial intelligence, Cyber security, Cyber physical systems, Machine learning, Deep learning.

1. INTRODUCTION

Artificial intelligence (AI) is a technology that duplicates and even surpasses the performance of the human mind in solving any program. AI consists of software algorithms to reproduceseveral human brain functions in a dynamic computing environment. Systems created on the basis of AI algorithms understand the environment, recognize objects, solve cyber security problems, learn from past experiences and make decisions. Recently, experts have broadly applied AI technologies to provide security of CPS. Here, AI provides system protection by providing security tools for rapid detection of threats and automatic execution of their solutions. In critical infrastructure systems, AI technologies are extensively applied to distinguish and avoid cyber-attacks, analyze and process big data, access control and authentication systems, predict and prevent security threats.

One of the key explanations for applying AI technologies in cyber security is its capacity to rapidly study and solve large volume of data. AI examine data which cannot be processed by the human being in a short period of time and automate the process of recognizing and responding to these attacks. AI uninterruptedly monitors the network to sense irregular actions and block hacker attacks and avoid data leakage. The application of AI in cyber security tools is an important and promising field. It helps improve the effectiveness and reliability of security systems by providing

DOI: 10.5121/ijcsit.2024.16404

earlier, more precise threat recognition and avoidance. The main idea of AI includes its capacity to sense and examine irregularities and unsafe actions in networks and control systems which can show the existence of a cyber-attack or security risk.AI is also applicable in decision-making and taking actions to avoid and react to these risks. To this end, this article highlights the use of AI technologies in solving cyber security challenges in CPS.

2. THEORETICAL FOUNDATIONS OF ARTIFICIAL INTELLIGENCE

AI is a way to make a machine intelligent and think like a human. The main goal of AI is to create the management of processes as the management of human consciousness. This is achieved by studying or analyzing the pattern of the human brain. Software for machines is developed based on these studies. Essentially, AI refers to a subfield of computer science to produce theories, approaches, practices and structures to reproduce and encompass human intelligence to machines [1]. The principle of operation of AI is analogous to the work of any other computer program, i.e., it receives data, analyzes them and draws conclusions. Researchers offer three types of AI. Poor AI works only to accomplish a narrow task. Strong AI is under development. It is capable to think and make decisions as a human being, analogous to the working principle of human intelligence. Super AI does not exist yet, there are only ideas that it will be in the near future. [2]:Methods and algorithms used in AI technologies:

2.1. Machine Learning

(ML) is a subfield of AI which develops algorithms and statistical models enabling computers to implement tasks with no obvious programming instructions. Here, algorithms learn from data, recognize patterns, provide estimates and optimize performance overtime. Algorithms of ML are applied in numerous applications, as well as in the recognition of image and speech, natural language processing (NLP), recommender systems, autonomous vehicles, medical diagnostics, and financial forecasting. The volume of data produced continues to grow, ML methods are getting very significant for gaining meaningful understandings and making data-driven decisions. 4 types of ML methods are distinguished [3-5]:

- An algorithm in supervised learning, learns from labeled data, and each input here is allied with an equivalent output. Its main goal is to learn a mapping from inputs to outputs which enablesit to produce predictions on new, unobserved data.

- The difference is that in unsupervised learning, no output information is provided. The learning process takes place using the relationships between the data. Moreover, unsupervised learning does not have training data.

- Semi-supervised learning contains the elements of both supervised and unsupervised learning. It trains algorithms on a database containing both labeled and unlabeled data.

- Reinforcement learning, an ML subfield, allows information about the environment to be learned more thoroughly according to human intelligence.

AI created in the above-mentioned ways is more efficient in creating, managing and storing more information. ML is applied to generate all sorts of AI tools (from applications for automatic text and speech recognition, to robots or unmanned vehicles, to built-in complex computer vision systems).

2.2. Deep Learning

(DL) includes a set of algorithms using numerous layers to increasingly extract more multilayered structures from raw data with no pre-processing. It makes emphasis onartificial neural networks with numerous levels between input and output layers. These deep neural networks can learn hierarchical representations of data and each layer extracts increasingly more abstract structures from the input data.

These algorithms automatically acquire to notice complex patterns and relationships in data with the help of training process on huge datasets. Key features of DL include the use of multiple layers, hierarchical feature learning, end-to-end learning, scalability to handle large datasets, and automatic feature extraction. DL has accomplished notable achievement in a variety of fields, as well as in computer vision, NLP, recognition of speech, healthcare, and autonomous systems [6].

ML and DL methods are used to sense malevolent actions in information systems triggered by cyber-attacks [7].

2.3. Neural Network

is a computational model encouraged by the construction and function of biological neural networks such as the human brain. It consists of interrelated nodes or neurons systematized in layers. Each neuron receives input signals, processes them, and generates an output signal to be transmitted to other neurons in the network.

They can be applied to a variety of tasks, including regression, classification, clustering, pattern recognition, and feature approximation. They are particularly effective for tasks involving huge volume of data and complex patterns, for example recognition of image and speech, NLP, and reinforcement learning. In addition, different architectures and variations of neural networks, as well as convolutional neural networks, recurrent neural networks and deep neural networks, are developed to solve specific problems [8].

2.4. Fuzzy Logic

is a kind of logic used to regulate reasoning which is estimated rather than preciseone. It is based on the idea that true values can be represented as fuzzy sets rather than as binary (true or false) values. In other words, fuzzy logic makes uncertainty to be represented in decision making. In classical logic, propositions are either correct or wrong, however in fuzzy logic, propositions have degrees of truth between 0 and 1. Fuzzy logic is applied in control systems, pattern recognition, and decision-making. This kind of logic is predominantly appreciated when the limitations between categories are poorly defined or precise mathematical models are challenging to attain. Examples of fuzzy logic applications include automatic control systems fordevices, traffic light controllers, and expert systems for medical diagnostics [9].

2.5. Cognitive Computing Systems

Cognitive computing is a field of computer science and syndicates AI and ML to generate computing systems capable handle multifaceted tasks, implement data analysis and make decision as the human brain. Cognitive computing aims to recreate the process of human thinking in a computer model. The technology seeks to imitate the logic of the human mind and improve interactions between humans and machines. This happens, for example, through AI that recognizes human language and the meaning of images forsubsequent self-learning. Today, the implementation of a cognitive computing system is possibleonly on complex machines such as the

IBM Watson supercomputer [10].

2.6. Genetic Algorithms

are created to handle optimization and modeling problems by successively picking, merging, and shifting wanted parameters through mechanisms reminiscent of biological evolution. Genetic algorithms are a powerful optimization method extensively applied in different areas of AI [11].

2.7. Natural Language Processing Systems

is a technology that enables computers to understand, recognize, interpret and reproduce human language and speech. Today, the most fascinating example of NLP technology is the advanced NLP models such as openGPT [12].

2.8. Computer Vision Systems

exploits DL techniques to study image content such as images, raster and vector graphics, and video. CV is a field of AI and implements the analysis of images and videos. It contains a number of techniques to enable a computer to "realize" and get information from what it realizes. The systems contain a photo or video camera and distinct software to recognize and categorize objects. They examine images (photos, images, videos, barcodes), including faces and emotions. Experts use ML technologies to teach a computer to "recognize" [13].

2.9. Expert Systems

They are applied when it is needed to examine huge data about the business, and simple models cannot handle this task or they need a lot of time. An expert system is a computer system that can partially replace an expert in solving a problem situation. The AI approach used in expert systems differs from simple information retrieval in that the computer program is not limited to the capability of recognizing information according to certain criteria, but also has a way to integrate complex information. Moreover, these AI systems must have data entry complexity, as the initial data must be entered as precisely as possible. AI-based expert systems are widely used in the fields of weather forecasting, medical diagnosis, and sports event forecasting. Although expert models cannot replace humans, they can simplify the development of solutions [14].

3. CONCEPTUAL MODEL OF CYBER-PHYSICAL SYSTEM

AI, as a sub-field of computer science, is extensively applied in the administration of complex CPS, such as energy distribution networks, intelligent systems, oil and gas industry, water infrastructure, NLP, video and image recognition, etc. CPS includes a combination of physical processes integrated with sensors and actuators that interact during process monitoring and provide information to the control center for decision making [15].

This article presents a conceptual model of CPS, its elements and their interrelationship. CPS is built using modern technologies (Internet of Things, Big Data, Cloud Computing, etc.). Depending on the purpose of the system, additional technologies are widely used. The data in CPS is huge, therefore big data technology and effective methods are necessary to process and analyze this data and to make decisions. The term "cyber-physical systems" was proposed in 2006 by Helen Gill, employee of the US National Science Foundation. The US National Institute of Standards and Technology (NIST) defines CPS as a set of digital, analog, physical and human components to activate through an integrated physical environment and logic. CPS is a multifaceted distributed system managed through computer algorithms, thoroughly combined with the Internet and its users. The conceptual model of CPS involves three layers (Figure 1): physical, network and application layers [16-18]:

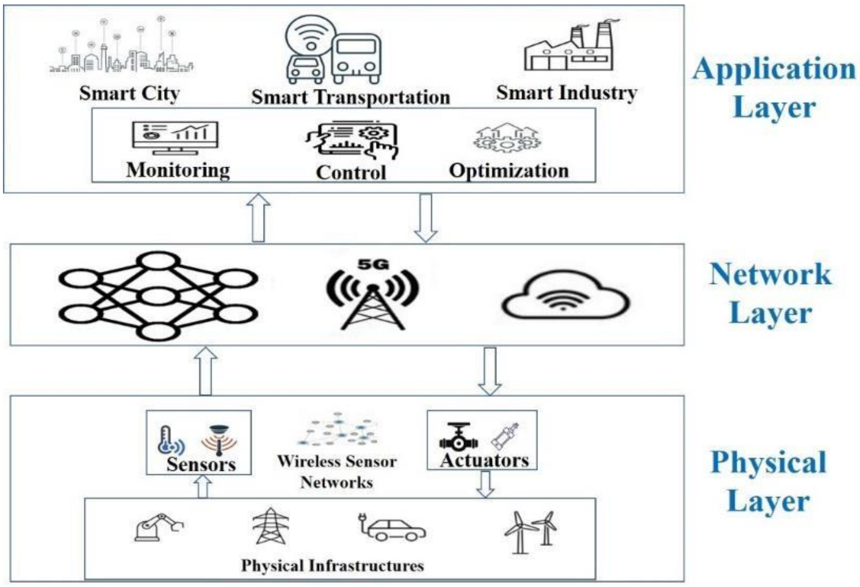

Figure 1. The conceptual model of CPS

3.1. Physical Level

The physical layer of a CPS characterizes the components to relate straight with the physical environment. This layer is the core of the CPS architecture and includes various devices that collect information from the environment or perform changes in the physical world. This layer involves sensors, actuators, tracking devices and computing elements. Physical level collects data from physical devices (sensors). Sensors distinguish and estimate physical phenomena such as temperature, pressure, humidity, light, movement, etc. They translate physical quantities into electrical signals or digital information to be processed by CPS. Real-time control devices gather data (temperature, pressure, etc.) from sensors and pre-process them in the vicinity and send them to cloud computing servers for further processing through the network. Actuators refer to the devices responsible for implementing changes in the physical environment based on commands from higher levels of CPS and computing systems. They convert digital or electrical signals into physical actions such as movement, heating, cooling or switching. Actuators may include motors, valves, pumps, heaters, relays, and switches.

The physical layer of CPS is exposed to numerous safety intimidations due to its straight relation with the physical world. Devices, including sensors and actuators, are often deployed in large and uncontrolled environments. On the other hand, the communication capabilities, storage and data processing power of these nodes are limited to some extent. Accordingly, traditional security mechanisms cannot be applied directly at the physical layer, making it vulnerable to hacking and other malicious attacks.

3.2. Network Layer

Performs communication and data sharing with several system components, as well as sensors, actuators, and computing devices. It acts as the pillar of the CPS architecture, allowing for communication and coordination between distributed entities. The network layer is responsible for communicating between physical sensors, smart devices, edge computing nodes or clouds, cloud services, and custom software components. Thislayer typically consists of various technologies to connect all the layers and sharing information in CPS. CPS use protocols of Wi-Fi, WiMAX, Zigbee, LoRa, GPRS and 3G/4G/LTE technologies in order to transmit data received from the physical level to cloud servers for storage and processing. The network layer infrastructure can vary depending on the scale and complexityof the CPS, from local area networks (LANs) to wide area networks (WANs) and the Internet.

The network layer of CPS is exposed to several cybersecurity challenges due to its crucial role in simplifying communication and data sharing with interconnected devices and systems.

3.3. Application Layer

This layer integrates data, algorithms, and user interfaces to ensure a diversity of applications designed to explicit use cases for end consumers, operators, and other service providers. This layer provides specific services to end users through various CPS applications. It outlines many applications in which sensors/actuators are applicable. Applications may be related to smart grid, smart factory, smart building, smart transportation, smart healthcare, etc. The application layer is responsible for making decisions and also activating commands to manage physical devices.

The software and applications used at the application layer control the physical systems, predict the state of the physical systems, and determine the system dynamics at the next time step. To analyze data and make informed decisions ML, statistical analysis, optimization and predictive modeling techniques are used. Overall, the application layer plays an important role in providing the functionality of CPS by providing data analytics, visualization tools, human-machine interfaces, and integration capabilities. CPS collect a lot of information from objects located at the physical layer. This data can be stored on a local server or in the cloud. They also process data using simulation models. Using the user's requests, reports and graphs are created to provide real-time monitoring. Data mining techniques such as data clustering, classification and regression can be used for forecasting and planning. Moreover, the results obtained in this layer are returned to the physical layer to control some devices and machines used in monitoring and control processes.

CPS application layer is vulnerable to various cybersecurity challenges due to its role in enabling data analytics, visualization, and human-machine interaction.

The Internet of Things (IoT), cloud computing systems and big data processing, which are mutual integration of technologies, are used in the design of CPS. IoT technology enables interaction between CPS devices. Each CPS in the IoT platform monitors and controls the physical environment of the real world. CPS generates a large amount of data. They are characterized by several features as volume, velocity and variety. Cloud technologies are used to process data measured in petabytes. Cloud technologies provide fast processing of data generated and collectedin real time. Real time data processing from multiple sensors and their managing through feedback involves huge computing and memory resources. Cloud technology is used to access these resources. Cloud computing systems provide storage of huge amount of data and their rapid processing using complex computing algorithms on cloud servers.

4. RELATED WORKS

The paper [19] proposes a detection system to detect cyber security attacks in IoT with the use of (DL) methods. It compares the DL model with traditional ML approaches. [20] ouitlines the importance of cyber security infrastructure and discusses how to measure, avoid and diminish cyber-attacks executed against industrial cyber-physical systems (ICPS). It shows ML-generated attacks based on multiple criteria to demonstrate the applicability of solution offered. To this end,it examines and assesses ICPS security in two real use cases. In [21], the importance of artificial immune systems in IoT environments is studied by evaluating and determining the performance of an empirical study to secure IoT environments. [22] develops an intrusion detection system (IDS) for IEEE 1815.1 power system using CPSs. To determine the presence of anomalies a bidirectional recurrent neural network is applied, and a verification process is performed in several aspects. [23] presents a cyber-attack detection methodology by applying a DL model. The results of the study show that this model is more efficient than other ML models in the market ina real cyber security scenario for IoT equipment used in Industry 4.0. To identify irregularities in industrial control systems (ICSs), [24] applies artificial neural networks using window-based feature extraction techniques from time series data sets. It uses a group of two neural network learning algorithms (the Error-Back Propagation and Levenberg-Marquardt). The IDS-NNM algorithm is proven to be able to capture all network intrusion attempts without generating any false alarms. [25] applies several ML methods for the detection of intrusions in aerospace ICSs. The study uses the Cooja IoT simulator to generate highly accurate attack data on IoT 6LoWPAN networks. Experimental results show that ML models for intrusion detection achieve better results with more than 99% accuracy, efficiency and detection. Furthermore, it needs low power consumption and memory, which shows that these models are applicable in constrained environments such as IoT sensors. [26] proposes a new structure to identify and differentiate DoS and fidelity cyber-attacks in ICSs using 1-dimensional Convolutional Neural Networks (CNN). This new structure is superior to the currently used methods. [27] presents a scheme to protect remote patient monitoring systems from DoS attacks. An attack detection model is created using decision trees. The model can help find different kinds of attacks, concentrating mainly on flood attacks, and can be appropriate for devices with restricted memory and processing resources, such as sensors and healthcare devices. As the further work, they suggest the possibility of developinga mechanism to identify other types of attacks and even prevent a wide range of attacks. [28] discusses intelligent security measures using ML-based techniques against several characteristic attacks at different layers of CPSs. In addition, the paper identifies open research challenges related to the development of intelligent security measures for CPSs. Finally, an overview of the security project for smart CPSs is presented with important analyses. A semi-automatic method for online security assessment using ML techniques is presented in [29]. Many ML algorithms are trained offline using a resampling cross-validation method. Later, the best model among the ML algorithms is carefully chosen based on performance and used online. The authors argue that the use of ML techniques provides reliable and robust solutions for the planning and operation of future industrial systems with an acceptable level of security. In [30], the authors propose a partial model attack based on an AML (Adversarial Machine Learning). This attack is implemented through a modification of a small part of the sensor information. t ML-based analysis in IoT systems is exposed to AML attacks, when attackers deploy a little part of equipment information. For example, when an adversary seizes only 8 out of 20 IoT devices, the attack accomplishment rate is 83%. Consequently, the ML engine of an IoT system is estimated to be very weak to attacks even with a small number of IoT devices, and the result of these attacks seriously disrupts the operations of the IoT system.

5. 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. Cybercriminals may effortlessly avoid signature-based detection systems by changing code in applications or creating new malware 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 abovementioned problems, AI technologies have been used in recent times. The complexity of CPSs network creates risks, particularly in terms of cyber security [31].

To increase the cyber security rate, intelligent methods, i.e., AI systems, are used for cyber defense. AI can automatically afford significant cybersecurity understandings with no human interaction. It is one of the key latent tools for cyber security and data security protection in cyberspace [32]. AI technologies are widely used to ensure the security of cyber-physical systems (smart networks, autonomous vehicles, healthcare systems, water management systems, SCADA systems, etc.) created on the basis of technologies such as the IoT, cloud computing systems and big data processing.

The use of AI in the security tools of CPS includes numerous advantages. First, AI is capable to handle and examine huge volume of data faster and more efficiently than humans. It ensures real-time threat detection and response. Second, AI can learn from experience and advance its skills over time. Since new threats appear, ML algorithms can learn from new data to expand their capacity to perceive and react to threats. Thus, changing threats can be identified through AI solutions, and they offer more successful cyber security protection against both known and unknown threats. Organizations can better defend their important data by using ML algorithms to distinguish threats and react to them in real-time. This technology also provides new ways to combat cyber threats. AI systems examine huge volumes of data through ML and DL algorithms in order to identify threats and track anomalies showing a cyber-attack. Below is the use of AI technologies in cyber security [33-35]:

- **Threat detection.** Patterns of behavior are analyzed by AI and deviations from the norm that could indicate a potential threat are identified. This can include anything from unusual network traffic patterns to unusual user actions.

- **Automation of routine processes.** AI automates routine cyber threat detection processes. Systems can automatically update their defenses based on new threat information, allowing themto quickly respond to new types of attacks.

- **Predicting attacks.** AI predicts and prevents future cyberattacks using information about past threats and attacks. AI algorithms are crucial for the discovery and avoidance of cyber-attacks, because it can examine huge amounts of data and detect irregularities and non-specific patterns that indicate the presence of cyber threats. It can also detect irregularities and forecast possible threats, assisting organizations take action to defend own systems and information.

- **Threat analysis.** AI analyzes threats and identify new types of cyberattacks as well. It can analyze data about previously known threats and generate models that can identify similarities and patterns in new data. It ensures the discovery and prevention of new kinds of cyberattacks which were formerly unidentified. AI can also be used to predict security attacks through historical data and trends analysis. ML algorithms can learn from data of previous events and exploit that data to forecast upcoming threats. For example, AI can determine a certain type of attack that is more common and suggest measures to prevent it. It enables organizations to be ready for new threats and take actions to avoid them before they become a reality.

- **Malware detection.** ML algorithms are exploited by AI to identify both known and unknown malware 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 malware behavior may determine new and unknown malware variations that cannot be detected through old-style antivirus software. Malware can be identified by AI-based malware detection solutions with static and dynamic analysis techniques. Static analysis includes analyzing file properties such as size, structure, and code to recognize patterns and irregularities. Dynamic analysis includes analysis of behavior of a file to detect patterns and irregularities while running.

- **Detection of phishing attacks.** Phishing is a common type of cyber-attack which aims at individuals and organizations. 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 ML algorithms AI-powered phishing detection solutions analyze the emails' content and structure in order to detect possible phishing attacks. These algorithms can learn from large data to recognize patterns and anomalies showing a phishing attack. During the interaction of emails to identify potential phishing attacks user behavior is also analyzed. For instance, if a user clicks on a mistrustful link or type private data to reply to a phishing email, abovementioned solutions can capture that action and notify security teams.

- **Detecting anomalies by security log analysis**. Using ML algorithms AI performs real-time security log data analysis. This kind of analysis enables companies to detect possible insider threats. User behavior analysis across multiple systems and applications can detect a typical actions indicating insider intimidations, namely, illegal access or uncommon data spread. Then, organizations may take measures to avoid data breaches and other security events before they occur. AI-powered security log analysis offers organizations a powerful tool to sensepossible threats and take mitigation measures.

- **Taking automatic response measures against threats**. AI can also be used to mechanically react to stop cyberattacks. For example, if AI detects an anomaly or threat, it can take automatic actions to prevent an attack, such as blocking access to infected resources or disconnecting suspicious devices from the network.

- **Network security monitoring**. AI algorithms implement the capabilities of CPS to monitor the network infrastructure, identify unusual traffic patterns, and sense unauthorized devices in the network. AI expands the network safety by detecting network anomalies. It performs network traffic analysis to identify abnormal patterns. Through historical traffic data analysis, AI algorithms can acquire what is typical for a given network and identify anomalous or suspicious traffic. This may include uncommon port usage, rare protocol, or traffic from distrustful IP addresses. AI also expands network safety through the network device monitoring. AI algorithms can be trained to identify unlicensed devices on the network and notify security teams about the possible intimidations.

- **Security issues on endpoint devices (laptops and smartphones).** Cybercriminals often target the laptops and smartphones, that is endpoint devices. Using signature-based detection, traditional antivirus software can only distinguish recognized malware variations. But AI identifies unknown malware variations through their behavior analysis. AI-powered endpoint security solutions analyze computers' behavior and identify possible threats using ML algorithms. These solutions can also obstruct unauthorized access efforts and avoid attackers from accessing sensitive data by providing real-time protection. AI algorithms perform real-time endpoint behavior analysis and notify security teams about possible threats. Consequently, security teams have the opportunity to react to threats in advance and avoid the damage.

- **Implementation of AI in access control and authentication systems**. Access control and authentication systems are crucial for ensuring the security of information systems and data. They determine who has access to certain system resources and functions and verify that theuser is the one who claims to be.

Biometric identification, multi-factor authentication can be used to increase the efficiency and reliability of AI access control and authentication systems:

- Biometric identification: AI can be applied to analyze and process biometric data such as fingerprints, voice, face and retina. AI systems can be trained to identify the unique characteristics of each user and use them for authentication. This upsurges security as it is difficultto falsify or steal biometric data.
- Multi-factor authentication. AI can be applied to improve multi-factor authentication. It analyzes various authentication factors such as password, biometrics, devices and location of the user and decide to grant access based on a combination of these factors. This upsurges security by making it challenging for an attacker to spoof or bypass multiple authentication factors.

6. 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. Numerous significant advantages of using AI in the field of cyber security are revealed below [36-38]:

6.1. Advantages of Using Artificial Intelligence in Cyber Security

Speeding up the threat detection process. AI can analyze large amount of data in real time, ensuring faster and more productive threat detection than traditional methods.

Development of protection strategies. Due to its capability to learn from past cyberattack data, AI can predict future threats and help develop defense strategies.

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.

Complex Anomaly Detection. Can detect unusual and complex anomalies that may be unnoticed by AI operators, which allows for the identification of hidden threats and avoidance of cyber-attacks.

Hidden threat detection. AI can sense hidden patterns and irregularities in big data which specify security threats, which allows for fast response to possible threats and their prevention.

Cost reduction. Organizations can save costs in many fields of their cybersecurity procedures by forcing AI-powered automation and increasing the accuracy of threat detection. AI reduces costs by automating tasks. AI's capability to advance the accuracy of threat detection also helps lessen costs.

Real-time threat detection and response. In a rapidly changing cyber threat environment, the opportunity to detect and response to attacks in real-time is serious for diminishing the probable damage triggered by malicious actions. By rapidly processing data from a variety of sources, AI can identify mistrustful patterns, irregularities, or signs of compromise that could indicate ongoing or approaching cyberattacks. Real-time analysis allows security teams to immediately realize possible threats and take agile actions to mitigate risks. By quickly noticing and counteracting threats, organizations lessen the time attackers spend on their networks, decreasing the probability of data leaks, system compromises, or unauthorized access.

Improved scalability. Traditional cybersecurity approaches regularly face challenges when it comes to managing huge data and maintaining efficient operations in multifaceted environments. AI is scalable, and enables the organizations to efficiently analyze huge data and react efficiently to cyber threats. The expansion of AI enables it to process the growing volumesof data in current digital ecosystems, as well as cloud environments, IoT devices, and interconnected networks. With AI, organizations can leverage the characteristic scalability to process and analyze data in real-time to ensure rapid detection and elimination of cyberthreats.

6.2. The Challenges Posed yb AI in Cyber Security

Despite the advantages of AI technologies, the issues related to the use of these methods for malicious purposes have caused argument [39]. 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 [33]. While there are many benefits of applying AI in cybersecurity, there are also possible risks to consider. Below are some of them [30, 40, 41]

- **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 ofseeking vulnerabilities in network systems.
- **Privacy issues**. The use of AI to analyze huge data may upsurge privacy concerns, predominantly those related to personal data.
- **Ethical issues.** Ethical issues can also arise when AI is used to pursue and explore user behavior. For example, defining what level of monitoring is acceptable and identifying the boundaries between defense against cyber threats and unacceptable invasion of privacy is difficult.
- **Dependence on AI**. With the amplified use of AI in cybersecurity, there is an over-dependencerisk on technology, which can lead to losing control over it.
- **Lack of qualified specialists**. 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.
- **Difficulty of interpreting results**. AI can produce complex and confusing results that are difficult for humans to interpret. This can complicate making decisions and responding to securitythreats.
- **Dependence on data quality**. AI requires high quality and reliable data for its work. If the datais unfinished or imprecise, the analysis results may be improper or imperfect.
- **Possibility of cheating**. AI-based detection and prevention systems can be tricked or bypassedby attackers.
- **Computing resources**. AI requires powerful systems with large computing resources and memory resources to process and analyze huge volume of data. This can be challenging for organizations with restricted capitals.
- **Bias.** Bias in cybersecurity can lead to wrong decisions, missed threats, or unfair actions. Bias in AI algorithms comes from the data used to train them. If the training data is biased, the AI algorithm will learn and continue these biases in its predictions and assumptions. For instance, if an AI algorithm is trained on a dataset of mostly male senders, it may unintentionally recognize the emails from female senders as spam more frequently, suggesting a biased relationship betweengender and spam content.
- **Destructive use**. Attackers can use AI technologies to increase the complexity and effectivenessof their cyberattacks, which poses serious challenges to defense measures.
- **Use of phishing attacks through AI**. Phishing attacks comprise using deception techniques totrick people into disseminating personal information or executing malevolent activities. Attackers can use AT to generate highly substantial and modified phishing emails. These phishing emails generated by AI bypass traditional email filters and ensure that attacks are successful.
- **Automated attack tools**. AI automates several steps of the cyberattack lifecycle, making it easier for attackers to expand their operations and target more victims.

7. VULNERABILITIES IF AI-POWERED SYSTEMS IN CYBER SECURITY SOLUTIONS

Like any other software or system, AI-powered security solutions may encompass vulnerabilities which can be used by attackers for malicious actions. These weaknesses could allow attackers to avoid or deploy AI algorithms, which would undermine the effectiveness of cybersecurity measures. To remove and lessen risks related to security vulnerabilities in AI systems, organizations should consider the following actions [42, 43]:

- **Regular security assessments:** Regular security assessments and dissemination testing of AI systems should be performed to identify and eliminate potential weaknesses. These assessments should simulate real-life attacks and try to misuse weaknesses in the AI system’s infrastructure, algorithms, or data processing.
- **Secure development practices:** Secure development practices in the early stages of AI system development should be achieved. This includes adhering to secure coding standards, performing comprehensive security assessments, and applying secure development frameworks and tools.
- **Secure deployment and configuration:** Safe positioning and configuration practices for AI systems should be realized. These may include proper configuration of access controls, secure storage of sensitive data used by the AI system, and implementation of safe communication protocols. Moreover, organizations must frequently update and reinforce their AI systems to copewith any recognized security vulnerabilities.

- **Continuous monitoring and incident response:** AI system should be constantly monitored for any unusual or suspicious activity pointing to a security breach. Robust logging and monitoring mechanisms should be implemented to monitor system behavior, sense anomalies, and quickly respond to any security incidents. An incident response plan should be developed to guide the organization in the event of a security breach or exploit.
- **Vendor assessment and security considerations:** When implementing third-party AI systems, a thorough security assessment should be executed to approve that the seller follows safe development practices and has strong security controls in place. When selecting AI solutions, it is recommended to consider security as a critical consideration and to contact vendors to solve any security concerns.

8. CONCLUSION

This article examined the use of AI in cyber security tools of CPS. It analyzed the use of a conceptual model of CPS and AI in identification and avoidance of cyber-attacks, analysis and processing of big data, access control and authentication, and in prediction and prevention of security threats. 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 article also identified the vulnerabilities existing in cyber security solutions that employ AI. It emphasized that the application of AI in the cyber security tools of CPS significantly increases the efficiency and reliability of information protection.

ACKNOWLEDGEMENTS

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

REFERENCES

[1] J. LI, (2018) “Cyber security meets artificial intelligence: a survey”, Frontiers of Information Technology & Electronic Engineering, Vol. 19, Issue 12, pp. 1462-1474.

[2] H. Khan, (2021) “Types of AI | Different Types of Artificial Intelligence Systems”, fossguru.com/types-of-ai-different-types-of-artificial-intelligence-systems.

[3] T. Wuest, D. Weimer, C. Irgens, and K. D Thoben, (2016) “Machine learning in manufacturing: advantages, challenges, and applications”, Production & Manufacturing Research, Vol. 4, No. 1, pp. 23–45.

[4] S. R. Mubarakova, S. T. Amanzholova, and R. K. Uskenbayeva, (2022) “Using Machine Learning Methods in Cybersecurity. Eurasian Journal of Mathematical and Computer Applications, Vol. 10, Issue. 1, pp. 69–78.

[5] T. T. Nguyen, and V. J. Reddi, (2021) “Deep Reinforcement Learning for Cyber Security”, IEEE Transactions on Neural Networks and Learning Systems, pp. 1–17.

[6] H. Ji, O. Alfarraj, and A. Tolba, (2020) “Artificial Intelligence-Empowered Edge of Vehicles: Architecture, Enabling Technologies, and Applications”, IEEE Access, Vol.8, pp. 61020–61034.

[7] J. Wang, Y. Ma, L. Zhang, R. X. Gao, and D. Wu, (2018) “Deep learning for smart manufacturing: Methods and applications”, Journal of Manufacturing Systems, Vol. 48, pp. 144–156.

[8] M. Madhiarasan, and M. Louzazni, (2022) “Analysis of Artificial Neural Network: Architecture, Types, and Forecasting Applications”, Journal of Electrical and Computer Engineering, Vol. 2022, pp.1-23.

[9] L. A. Zadeh, (1965) “Fuzzy sets,” Information and Control, Vol. 8, pp. 338–353.

[10] Y. Wang, (2009) “On Cognitive Computing”, Int. J. of Software Science and Computational Intelligence, Vol. 1, issue. 3.

[11] L. Haldurai, T. Madhubala, and R. Rajalakshmi, (2016) “A Study on Genetic Algorithm and its Applications”, International Journal of Computer Sciences and Engineering, Vol. 4, Issue. 10, pp. 139-143.

[12] N. Jagdishbhai, and K. Y. Thakkar, (2023) “Exploring the capabilities and limitations of GPT and ChatGPT in natural language processing”, Journal of Management Research and Analysis, Vol. 10, Issue. 1, pp. 18-20.

[13] V. Wiley and T. Lucas, (2018) “Computer Vision and Image Processing: A Paper Review”, International Journal of Artificial Intelegence Research, Vol. 2, No. 1, pp. 28-36.

[14] M. Pandit, (2013) “Expert System-A Review Article”, International Journal of Engineering Sciences & Research Technology, Vol. 2, Issue. 6, pp. 1583-1585.

[15] Y. Ashibani, and Q.H. Mahmoud, (2017) “Cyber physical systems security: Analysis, challenges andsolutions”, Computers and Security, pp. 81–97.

[16] A.R. Al-Ali, R. Gupta, and A. A. Nabulsi, (2018) “Cyber physical systems role in manufacturing technologies”, 6th Internatıonal Conference on Nano and Materıals Scıence.

[17] F. Januário, A. Cardoso, and P. Gil, (2019) “A Distributed Multi-Agent Framework for Resilience Enhancement in Cyber-Physical Systems,” IEEE Access, Vol. 7, pp. 31342 – 31357.

[18] S. Kim, and K. J. Park, (2021) “A Survey on Machine-Learning Based Security Design for Cyber-Physical Systems”, Applied Sciences. Vol. 11.

[19] A. A. Diro, and N. Chilamkurti, (2018) “Distributed attack detection scheme using deep learning approach for Internet of Things”, Future Generation Computer Systems, Vol. 82, pp. 761–768.

[20] A. Khaled, S. Ouchani, Z. Tari, and K. Drira, (2021) “Assessing the severity of smart attacks in industrial cyber-physical systems”, ACM Transactions on Cyber-Physical Systems, Vol. 5, No. 1, pp.1-28.

[21] S. Aldhaheri, D. Alghazzawi, L. Cheng, A. Barnawi, and B.A. Alzahrani, (2020) “Artificial Immune Systems approaches to secure the internet of things: A systematic review of the literature and recommendations for future research” Journal of Network and Computer Applications.

[22] S. Kwon. H. Yoo, and T. Shon, (2020) “IEEE 1815.1-Based Power System Security with BidirectionalRNN-Based Network Anomalous Attack Detection for Cyber-Physical System”, IEEE Access, Vol. 8,pp. 77572 – 77586.

[23] R. V. Mendonça, J. C. Silva, R. L. Rosa, M. Saadi, D. Z. Rodriguez, and A. Farouk, (2022) “A lightweight intelligent intrusion detection system for industrial internet of things using deep learning algorithms”. Expert Systems, Vol. 39, Issue. 5.

[24] O. Linda, T. Vollmer, and M. Manic, (2009) “Neural Network Based Intrusion Detection System for Critical Infrastructures”, International Joint Conference on Neural Networks. Atlanta, GA, USA.

[25] Y. Maleh, (2019) “Machine Learning Techniques for IoT Intrusions Detection in Aerospace Cyber-Physical Systems,” Machine Learning and Data Mining in Aerospace Technology, pp. 205–232.

[26] C. M. Paredes, D. Martínez-Castro, V. Ibarra-Junquera, and A. González-Potes, (2021) “Detection and Isolation of DoS and Integrity Cyber Attacks in Cyber-Physical Systems with a Neural Network-Based Architecture”, Electronics, Vol. 10, Issue. 18, 2238.

[27] V. Liagkou, V. Kavvadas, S. K. Chronopoulos, D. Tafiadis, V. Christofilakis, and K. P. Peppas, (2019) “Attack Detection for Healthcare Monitoring Systems Using Mechanical Learning in Virtual Private Networks over Optical Transport Layer Architecture”, Computation, Vol. 7, Issue. 2.

[28] M. Shafique, F. Khalid, and S. Rehman, “Intelligent Security Measures for Smart Cyber-Physical Systems”, 21st Euromicro Conference on Digital System Design (DSD), 29-31 August 2018, pp. 280-287.

[29] N. V. Tomin, V. G. Kurbatsky, D. N. Sidorov, and A. V. Zhukov, (2016) “Machine Learning Techniques for Power System Security Assessment”, IFAC-PapersOnLine, Vol. 49, Issue 27, pp. 445-450.

[30] Z. Luo, S. Zhao, Z. Lu, Y. E. Sagduyu, and J. Xu, “Adversarial Machine Learning based Partial-model Attack in IoT”, Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning, 25 June 2020. pp. 13-18.

[31] D. T. Matt, V. Modrák, and H. Zsifkovits, (2020) “Industry 4.0 for SMEs Challenges, Opportunities and Requirements”, p. 436.

[32] World Economic Forum. Cyber Information Sharing: Building Collective Security. Geneva, Switzerland, (2020). pp. 1-26.

[33] A. J. Gonçalves de Azambuja, C. Plesker, K. Schützer, R. Anderl, B. Schleich, and V. R. Almeida, (2023) "Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey", Electronics, Vol. 12, Issue 8, pp. 1-18.

[34] N. Capuano, G. Fenza, V. Loia, and C. Stanzione, (2022) "Explainable Artificial Intelligence in CyberSecurity: A Survey" IEEE Access, Vol. 10, pp. 93575 – 93600.

[35] Z. Zhang, H. Al Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, (2022) "Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research", IEEE Access, Vol. 10, pp. 93104 – 93139.

[36] R. Calderon, (2019) "The Benefits of Artificial Intelligence in Cybersecurity", Economic Crime Forensics Capstones. 36, pp. 1-22.

[37] M. F. Rafy, "Artificial Intelligence in Cyber Security", 2024. doi: 10.13140/RG.2.2.19552.66561.

[38] L. Lazic. "Benefit From AI in Cybersecurity", The 11th International Conference on Business Information Security (BISEC-2019), 18th October 2019, Belgrade, Serbia.

[39] A. Angelopoulos, E. T. Michailidis, N. Nomikos, P. Trakadas, A. Hatziefremidis, S. Voliotis, and T. Zahariadis, (2020) "Tackling Faults in the Industry 4.0 Era-A Survey of Machine-Learning Solutions and Key Aspects", Sensors, Vol. 20, Issue. 1.

[40] J. Wilkins, (2018) "Is artificial intelligence a help or hindrance", Network Security, Vol. 2018, Issue. 5, pp. 18-19.

[41] M. F. Ansari, B. Dash, P. Sharma, and N. Yathiraju, (2022) "The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 11, Issue. 9, pp. 81-90.

[42] S. Wilson, "Cybersecurity and Artificial Intelligence: Threats and Opportunities", Contrast Security, 56 p.

[43] AI and cybersecurity: How to navigate the risks and opportunities. https://www.weforum.org/agenda/2024/02/ai-cybersecurity-how-to-navigate-the-risks-and- opportunities/

AUTHORS

Rashid Alakbarov graduated from Automation and Computer Engineering faculty of Azerbaijan Polytechnic University named after C. Ildirim. He received his PhD degree in 2006 from Supreme Attestation Commission under the President of the Republic of Azerbaijan. His primary research interests incloude various areas in cloud computing, data processing, computer networks, virtual computing, particularly in the area of distributed computing. He is head of department at the Institute of Information Technology as of 2002. Since 2010, he has been leading the development of "AzScienceNet" infrastructure. In 2021, he was appointed a executive director of the institute by the decision of the Presidium of Azerbaijan National Academy of Sciences. He is the author of 95 scientific papers, inclouding 5 inventions.

Mammad A. Hashimov received his Master's degree in automation and control from Azerbaijan Technical University in Baku, Azerbaijan. He received his PhD degree in 2016 from Supreme Attestation Commission under the President of the Republic of Azerbaijan. He is scientific researcher of Institute of Information Technology of Azerbaijan National Academy of Sciences. His primary research interests include various areas in internet of things, cloud computing, data processing, computer networks, virtual computing, particularly in the area of cloud technology applications. He is the author of 30 journal scientific papers and 20 proceedings