1st International Conference on Artificial Intelligence in the Era of Digital Transformation
Event Place: Tbilisi,Georgia
www.Aicnf.ir
اولین کنفرانس بین المللی هوش مصنوعی در عصر تحول دیجیتال | گرجستان
1st International Conference on Artificial Intelligence in the Era of Digital Transformation
PUBLISH IN JOURNALS — INTERNATIONAL CERTIFICATION

Review of artificial intelligence-based cybersecurity

Marziyeh Felahat
Department of Mathematics,Faculty of Basic Sciences, Bozorgmehr University of Qaenat,Iran

Mohammad Kazem Beshkani
Master of Business Administration, E-Commerce, Hakim Nezami Quchan Institute of Higher

Maria Akbarpour Koumleh
Ph.D. student of Computer Engineering, University of Qatar

Abstract

Cybersecurity is one of the most important issues for organizations and companies in today's world. With the advancement of technology and the increase in the number of internet-connected devices and services, security risks have also increased. One of the solutions to combat security risks is the use of artificial intelligence. Security operations centers (SOCs) must be better equipped to manage the vast scale of data to monitor and analyze the complexity of threats. SOC analysts face a daunting task: sifting through thousands of alerts a day – most of which are false – while quickly identifying and mitigating real cybersecurity threats. Artificial intelligence excels at data analysis and quickly processes large data sets to identify patterns that indicate malicious behavior. When specifically trained on cybersecurity data, it can simplify cybersecurity operations by automating routine tasks such as triaging alerts, analyzing reports, and performing vulnerability scans, saving valuable time and resources for human analysts. AI's dominance in cyberattacks demonstrates the technology's unparalleled power to identify and counter complex threats. The use of AI in cybersecurity has become a vital tool in defending digital systems by combining machine learning algorithms, big data analysis, and predicting attacker behavior. Using advanced algorithms, AI can help detect cyberattacks automatically and in the shortest possible time. By analyzing huge amounts of data, AI can examine network traffic patterns and detect any attacks. Also, using neural networks, AI can automatically predict suspicious user behavior and notify him/her if necessary.

Keywords: Artificial intelligence, cybersecurity, security, machine learning, data.

1. Introduction

Today, the lack of adequate security on the web brings with it the risk of cyberattacks, theft of personal and financial information, and disruption of critical systems. By protecting data and infrastructure, cybersecurity helps industries stay safe from malicious threats and strengthens users' trust in digital services. This protection ensures not only the security of companies, but also the privacy of individuals. Nowadays **,** cybersecurity and artificial intelligence have become very closely related to each other.Because artificial intelligence is rapidly conquering various aspects of our lives, from industry and medicine to voice assistants and autonomous cars, but with the expansion of artificial intelligence applications, cybersecurity has become a major challenge in this field. Cyberattacks can damage artificial intelligence and cause extensive damage to infrastructure, data, and even humans. Artificial must move forward in tandem to protect the digital world.

Artificial intelligence allows devices and equipment to perform tasks that would normally require human intelligence, such as decision-making, human speech recognition, visual recognition of elements, and translation of languages . Artificial Intelligence uses classified data to understand the issue and determine how to react to different situations.It should be noted that the use of artificial intelligence in the field of cybersecurity is essential in order to increase the power of protecting online systems and data from all types of attacks. If used correctly, AI can lead to the automatic detection of threats, the sending of warnings and the detection of new malware, as well as the protection of important business data.

Artificial intelligence (AI) in organizational security involves the use of AI techniques such as deep learning, machine learning (ML), knowledge representation and reasoning, as well as natural language processing, and is used with the aim of defending more automatically and intelligently against all types of threats. In this way, organizations can identify and block thousands of cyber threats that they face on a daily basis.Improving and empowering cybersecurity now requires human intervention. However, some tasks, such as monitoring systems, can be automated with the help of artificial intelligence. Automating processes will increase the capabilities of organizations to protect their networks, so they will have ample opportunity to deal with new threats. Because the increase in cyber attacks occurs due to complexities.

It should be noted that cybersecurity automation using AI is completely safe because it is designed based on current use cases in different business environments. For example, human resources (HR) and information technology (IT) teams use AI to familiarize new employees with the organization, as well as provide them with the right resources and access levels to increase effectiveness.Cybersecurity automation is especially important given the shortage of relevant experts. It is then that organizations will be able to grow their security investments as well as carry out work processes without the slightest worry about finding other personnel as specialists.

There are two main ways that AI boosts cybersecurity. First, AI can help automate many of the tasks that a human analyst often performs manually. These include automatically identifying unknown workstations, servers, code repositories, and other hardware and software on the network. It can also determine how to allocate the best security defenses. These are data tasks, and AI has the potential to process terabytes of data much more efficiently And more effectively than a human can check.Second, AI can help identify patterns in large amounts of data that

human analysts are unable to detect. For example, AI can identify key language patterns of hackers who send emerging threats on the dark web and alert analysts.In particular, AI-powered analytics can help recognize the terms and code words that hackers develop to reference their new tools, techniques, and procedures. One example is the use of the name Mirai , which means botnet. Hackers have created the term to hide the botnet topic from law enforcement and cyberthreat intelligence professionals.

Figure 1: Cybersecurity and helping humans

AI has already seen early successes in cybersecurity. Companies such as FireEye, Microsoft, and Google are increasingly developing innovative artificial intelligence, such as approaches to detecting malware, preventing phishing campaigns, and monitoring the spread of misinformation. One notable success is Microsoft's Cyber Signals program, which uses artificial intelligence to analyze 24 trillion security signals, with the help of 40 nationally and 140 hacker groups, to generate cyber threat intelligence for senior executives.Federal financial agencies such as the Department of Defense and the National Science Foundation recognize the potential of AI for cybersecurity and have invested tens of millions of dollars to develop advanced AI tools to extract insights from data generated from the dark web and open-source software platforms such as GitHub, a global software development code repository where hackers can also share code.

2. Artificial Intelligence

Artificial intelligence or AI is a branch of computer science that deals with the creation of machines that work intelligently, and this branch of computer science is broadly divided into two broad categories:

- **Strong Artificial Intelligence**: Strong AI refers to machines that can think and act completely like humans. This type of artificial intelligence is still in its early stages of development and has not been fully realized.
- **Weak AI**: Weak AI refers to machines that can exhibit intelligent functions in certain fields. This type of AI is widely used in a variety of fields, such as industry, healthcare, transportation, and government.

Types of Artificial Intelligence

AI can be classified based on different types of machine learning algorithms. Some common types of AI include:

- Supervised Machine Learning:

Supervised machine learning refers to machines that learn using sample data. This data includes expected inputs and outputs.

- Unsupervised Machine Learning:

Unsupervised learning refers to machines that learn without sample data. In this type of learning, machines are trained based on patterns and relationships in the data. The Academy has designed another comprehensive course titled Unsupervised Machine Learning for those interested in getting acquainted with different techniques and algorithms of unsupervised learning, which can complete your knowledge in this field.

- Reinforcement Learning:

Reinforcement learning refers to machines that learn by experience. In this learning, machines learn by performing actions and receiving rewards or punishments.

Artificial intelligence and cybersecurity have a deep and two-way relationship. On the one hand, AI can help improve security systems and counter cyber threats by analyzing large amounts of data and identifying suspicious patterns. Machine learning algorithms can quickly predict and respond to attacks. On the other hand, AI itself may also be the target of cyberattacks. Attackers can use exploit weaknesses in AI models and deceive these systems with attacks such as data manipulation or intrusion attacks. Therefore, close interaction between AI and cybersecurity experts is essential to protect these sensitive technologies and improve their security.

3. Cybersecurity

Cybersecurity refers to a set of actions and processes designed to protect systems, networks, and data from cyberattacks. Cyberattacks can include:

- Intrusion: Intrusion into a system or network to gain unauthorized access to data or resources.
- Damage: Damage to the system or network, such as deleting or altering data or interrupting service.
- Espionage: Collecting confidential information from the system or network.

Types of Cyber Attacks

Cyberattacks can be classified based on the different types of points of vulnerability. Some common types of cyberattacks include:

- Software-based attacks: Software-based attacks use malicious software, such as viruses, malware, and spyware, to attack systems or networks.

- Hardware-based attacks: Hardware-based attacks use malicious hardware, such as malware from internet-connected (IoT) devices, to attack systems or networks.
- Network-based attacks: Network-based attacks use network vulnerabilities to attack systems or networks.

Artificial intelligence and cybersecurity are two important areas that have been developing rapidly in recent years. AI can help improve cybersecurity, but it can also be the target of cyberattacks. To reduce the risk of cyberattacks in AI, there is a need for collaboration between AI and cybersecurity experts.

In the financial industry, for example, banks use artificial intelligence to detect suspicious transactions and prevent fraud. For example, JPMorgan uses machine learning algorithms to analyze customer behavior and detect unusual activities. These systems are able to quickly detect threats and neutralize them before cyberattacks occur. However, this technology It is also not immune to the risk of attacks, as attackers may attempt to disrupt AI systems by manipulating data or tricking algorithms.

4. The Role and Application of AI in Cybersecurity

The use of AI in cybersecurity allows organizations and companies to use big data and information to detect, analyze, and respond to cyber threats faster and more accurately, for example:

Discover new attacks

This technology has the ability to detect complex patterns in the data, even if the threats have not been seen before. In other words, artificial intelligence can detect zero-day attacks. This is especially important because hackers are constantly developing new ways to infiltrate systems.

Optimizing safety processes

AI plays a significant role in optimizing security processes. Through automation, tasks such as analyzing logs and security events, security experts can focus on more complex threats, while routine and routine tasks are handled by AI.

The use of AI in cybersecurity allows for the creation of a dynamic and adaptable wall of defense. AI-based systems are able to continuously learn from threats and adapt their defense strategies to counter new attacks. This flexibility ensures that the organization will be able to cope with the constant evolution of threats.

Cybersecurity is one of the most important issues that are related to cyberspace. In fact, most of the people's work is done on the Internet, and its high level of security helps to improve the quality of cyberspace users' experience in various fields. On the other hand, the development of artificial intelligence and the development of its presence in various aspects of life, including online activities, has been accompanied by changes.

In fact, artificial intelligence protects the passwords of user accounts and authenticates users with high precision. In this way, information security is placed at the highest level. Users are alerted to cyber threats such as phishing, and various harms in cyberspace such as cyber bullying or

cyber theft are reduced. The use of artificial intelligence in identifying and preventing cyber threats and preventing attackers from entering the network has become one of the basic solutions in cybersecurity. Among the applications of artificial intelligence in cybersecurity, the following can be mentioned:

1. Unknown Threat Detection: AI is able to detect anomalous patterns in the network and respond to them quickly.
2. High speed in data processing: The huge amount of data generated in networks cannot be managed by humans, but AI does it at a high speed.
3. Reducing human errors: The use of automated systems minimizes errors caused by human factors.
4. Predicting future attacks: Advanced algorithms can analyze attack patterns and suggest preventive measures.

Different Applications of AI in Cybersecurity

- Password protection and authentication

With the help of artificial intelligence, organizations can better protect their users' passwords and accounts. Most websites require users to enter important information in order to make a purchase or fill out a form. Naturally, an extra layer of security is required for these types of websites.

AI tools such as CAPTCHA, facial recognition, and fingerprint scanners allow organizations to automatically detect if any login requests are legitimate. These categories of solutions help prevent cybercrime tactics such as brute-force and credential stuffing attacks, each of which can compromise the entire enterprise network.

- Phishing Threat Detection

Phishing is one of the biggest cyber threats that all businesses face. When AI is combined with email security solutions, it enables organizations to detect suspicious items and unusual messages. In this case, it is possible to analyze the content of the email to quickly determine whether the message is spam or not. For example, AI can quickly and easily detect phishing signs such as email spoofing, forged senders, and misspelled domain names.

ML algorithms help AI make learning happen and the data is examined more carefully to identify new threats. Another benefit that machine learning has for AI is a better understanding of how users communicate, their typical behavior, as well as text patterns. This is necessary to prevent more advanced threats such as spear phishing, in which cyber attackers try to impersonate high-ranking people in the organization, such as the CEO. However, AI is able to detect suspicious activity to prevent spear phishing attacks.

- Vulnerability Management

As cyber attackers use more sophisticated methods and techniques, new vulnerabilities are also reported. As a result, organizations are trying to manage a large amount of new vulnerabilities, and their legacy systems cannot prevent these high-risk attacks in real time.

- Network Security

Network security involves time-consuming processes of creating policies and understanding topography. When policies are in place, organizations can put in place processes to identify valid connections and those that are malicious. These policies help organizations implement a zero-trust approach for greater security.

However, creating and maintaining policies across multiple networks requires sufficient time and continuous efforts. Often, organizations do not correctly name their applications and work processes. In other words, the security team may have to spend more time determining which work processes belong to a particular application. It monitors for a long time, so it recommends appropriate policies and work processes.

- Behavioral Analysis

With the help of behavioral analysis, organizations will be able to identify known threats. Traditional security methods relied on signatures and indicators of compromise (IOCs) to detect threats.

Organizations can use behavioral analytics to enhance their threat-hunting processes, which are AI models used to develop application profiles on the network and process large amounts of data. The data received can then be analyzed based on those profiles to prevent malicious activity from occurring.

5. The Role of AI in Preventing Cyberattacks

Artificial intelligence (AI) is known as a powerful tool in the field of cybersecurity, which has significantly increased the prevention of cyber threats. Using advanced algorithms and machine learning, this technology is capable of analyzing and processing massive amounts of security data in real-time, which helps in identifying and responding to threats faster and more accurately. With the help of AI, organizations can easily identify complex patterns and unusual symptoms and prevent new cyberattacks, including zero-day attacks. The technology also provides the ability to optimize security processes by automating repetitive tasks such as analyzing logs and managing alerts.

However, although AI plays a significant role in increasing cybersecurity, its use also comes with risks. Cybercriminals can use this technology to optimize attacks, create automated malware, and social engineering . Therefore, it is essential to pay special attention to security and ethical tips in addition to exploiting the benefits of AI to avoid potential problems and threats.For cybersecurity in general, AI is used to analyze, correlate event data, and cyber threats across multiple sources, translating them into clear, actionable insights that security professionals use to investigate, respond, and report further. If a cyberattack meets certain criteria defined by the security team, AI can Automate response and isolate damaged assets. Generative AI takes this work a step further by generating text, images, and other content in the original natural language based on patterns in existing data. A cyber attack occurs when hackers, cyber thieves, and cybercriminals in general attempt to gain illegal access to information stored on the system and network of Internet users through cyberspace. The impact of artificial intelligence on cybersecurity remains controversial because artificial intelligence is growing rapidly in many ways and its future cannot be accurately predicted.

However, it is better to note that like buying an original antivirus that plays a positive role in taking care of the security of Internet users, artificial intelligence considers the specifications of various types of attacks to improve cybersecurity.

In addition, with the help of the authentication system, it can route cyberattacks at a faster speed. In this way, it will more easily use clues to identify cybercriminals. As a result, it will prevent various cyberattacks by strengthening the defense power of the systems.

In this context, AI helps to strengthen threat-based intelligence and provides security professionals with:

- Exploring the characteristics of cyberattacks
- Strengthening Defensive Power
- Analyze data such as fingerprints and voice patterns in order to authenticate users
- Investigating Clues to Identify Specific Cyber Attackers

6. The Importance of Cybersecurity

According to the definition of this term, it should be said that today, the number of users who use devices and applications, or modern companies that produce large amounts of data, have highly sensitive or confidential data, the amount of which has increased significantly. Therefore, here comes the importance of cybersecurity, as data theft in systems continues to grow. In fact, the increase in volume and complexity in the methods used by cyber attackers through attack techniques has created many problems that cannot be prevented except with cybersecurity techniques.

7. Cybersecurity Components

In this regard, the field of cybersecurity can be divided into different components based on the type of security they create on the devices, and integrating all of them into one company is very important to achieve the success of the cybersecurity program. So, the components of cybersecurity are as follows:

- App Security
- Information or data security
- Network Security
- Disaster Recovery & Business Continuity Planning
- Operational Security
- Cloud Security
- Critical Infrastructure Security
- Physical Security
- End-user training
- Work in the field of cybersecurity

8. Cybersecurity Benefits

It can be said that cybersecurity has many advantages due to the reasons that we will mention below, which of course include the following options:

- Businesses are protected from cyberattacks and data breaches. In addition, data and networks are protected.
- Unauthorized user access is prevented.
- People are protected to use devices and end users.

- It has regulatory compliance.
- It ensures the continuity of business.
- Trust improves an organization's reputation.

9. Cybersecurity Enhancement Solution with AI

Artificial intelligence (AI), as a powerful tool in cybersecurity, helps organizations protect their assets and sensitive information by providing innovative solutions. Some effective solutions to enhance cybersecurity using artificial intelligence are:

- Upgrading machine learning-based systems with up-to-date and diverse data.
- Combining AI with other security solutions such as cryptography and multi-factor authentication.
- Training human resources to manage advanced AI systems.

In general, it can be said that artificial intelligence has not only been able to detect and stop a large share of cyberattacks, but it has also become a key tool in the fight against digital threats, so that the future of cybersecurity is unimaginable without the use of artificial intelligence, and the development of this technology will continue to play an important role in protecting information and data.

10. Basic Components of Artificial Intelligence

Intrusion detection

One of the most important aspects of using AI in cybersecurity is intrusion detection. AI-powered intrusion detection systems are capable of detecting unusual patterns and suspicious activity in networks and information systems. These systems are becoming increasingly more accurate and reliable by continuously learning from existing data and updating their knowledge base

Threat Analysis

After detecting suspicious activity, the AI becomes familiar with the analysis of data collected from various sources, including network traffic, system logs, and security alerts, the type of threat, and its risk level assessment.

This analysis helps security teams have a better understanding of the tactics and techniques used by attackers and can design a more effective defensive strategy.

Responding to threats

The final step in using AI in network security is to respond to threats. After identifying and analyzing the threat, it is necessary to take the necessary measures to deal with the threats. AI-powered systems can automatically make faster decisions to prevent threats from advancing or minimize the damage caused by them.

This process includes actions such as disconnecting suspicious network connections, updating firewall rules to block malicious traffic, and isolating infected systems.

11. Benefits of Using AI in Cybersecurity

Cybersecurity organizations are increasingly relying on AI in conjunction with more traditional tools such as antivirus protection, data loss prevention, fraud detection, identity and access management, intrusion detection, risk management, and other core security areas. Because of the nature of AI, which can analyze huge sets of data and find patterns, AI is uniquely To a person for tasks such as:

- Identifying real attacks is done more accurately than humans, and prioritizing responses is based on their real-world risks
- Identify and flag the type of suspicious emails and messages that are often used in phishing campaigns.
- Simulate social engineering attacks, which help security teams identify potential vulnerabilities before cybercriminals take advantage of them.
- Quickly analyze a huge amount of incident-related data, so that security teams can act quickly to contain the threat.

Additionally, AI has the potential to be a game-changing tool in penetration testing – deliberately examining software and network defenses to identify weaknesses. By developing AI tools to target their technology, organizations are better able to identify their weaknesses before hackers exploit them.Having this information gives cybersecurity organizations a significant advantage in preventing future attacks. Stopping a breach before it happens not only helps protect the data of individuals and companies, but it also reduces IT costs for businesses.

The benefits of AI-powered automation in the cybersecurity sphere include:

- Cost-effectiveness**:**

  Combining cybersecurity and AI leads to faster data collection. As a result, countering threats will be done more dynamically and effectively. It also eliminates the need for security professionals to do manual and time-consuming tasks. Therefore, they can focus more on strategic activities and increase the value of their business.

- Human errors**:**

  One of the common weaknesses in the old methods of providing security was the need for human intervention, which sometimes led to huge financial losses. But now, artificial intelligence has eliminated the human factor from most security processes. Certainly, this approach is much more effective and efficient because human resources can be used in the areas where they are needed most.

- Better decision-making**:**

  Cybersecurity automation helps organizations identify potential weaknesses in their security strategies. In this way, they will be able to choose more appropriate methods to improve the security of their IT environments.

Of course, organizations should be aware that cybercriminals are adjusting their new methods according to AI patterns. They use AI to design and create advanced attacks and deploy new and updated forms of malware.

The implementation of artificial intelligence in the field of cybersecurity brings many benefits to organizations, some of which are mentioned below:

- **Continuous Learning**

AI is constantly being updated and learning with new data, so AI's capabilities are evolving and improving. Techniques such as deep learning and ML allow AI to identify patterns, but also establish a baseline based on regular activities and identify any suspicious activity that deviates from that baseline. Artificial Intelligence's ability to Continuous learning has a significant impact on the difficulty of hackers' work.

- **Uncover Unknown Threats**

As cyberattackers invent new and sophisticated attack vectors, organizations are becoming more vulnerable to unknown threats. AI has the ability to provide solutions to vulnerabilities that have not yet been identified or patched by software providers.

- **The Role of AI in Large Volumes of Data**

AI-powered systems can handle vast amounts of data that security professionals are unable to do. In this way, organizations can automatically detect new threats amid the vast amount of data and network traffic that may not be detected by legacy systems.

- **Improving Vulnerability Management with the Help of AI**

Artificial intelligence gives organizations the ability to better manage vulnerabilities in addition to discovering new threats. In fact, it provides them with "more effective assessment", "improved problem-solving power", and "better decision-making ability".

- **Improving the overall security posture**

Managing a wide range of threats, including denial-of-service (DoS), phishing, and ransomware, is difficult and time-consuming. But AI-powered management empowers organizations to detect and manage different types of attacks in real time.

- **Make better decisions with Artificial Intelligence**

Threat detection is arguably one of the most essential elements of network security. And AI-based cybersecurity can lead to quick and real-time detection.

12. Cybersecurity and AI Challenges

The question remains whether AI can definitely improve cybersecurity sufficiently, perhaps because of the challenges that this factor has in relation to each other. For example:

- It is possible that AI is not tracking the right information. As a result, the leads that reach cybersecurity experts are wrong and cause experts to stray from the right path.
- Sometimes the information obtained is misunderstood and the answers to some of the experts' questions will not be provided correctly.
- The changes that are made in artificial intelligence to prepare for cybersecurity protection sometimes make it challenging to receive and transmit information related to cybersecurity.
- Sometimes, the AI's response to threats is not correct and decisive. As a result, contrary to what is expected, the number of cyberattacks will increase.
- Hackers and cyber thieves use artificial intelligence to create a complex process for their phishing and online theft.
- With the help of artificial intelligence, cybercriminals create threats to users that threaten the security of their information and system.

13. Conclusion

In conclusion, AI has quickly become one of the key tools in modern life, with its amazing abilities to analyze data and learn from experiences. Not only does this technology offer new ways to improve the quality of life and increase productivity, but it also allows us to deal with the complexities of the digital world in a more effective and intelligent way. However, it is still in need. We are constantly paying attention and monitoring to ensure that AI advancements are deployed in a responsible and safe manner. A future where AI becomes an integral part of our lives will continue to present many challenges and opportunities.Looking to the future, there is significant room for AI to grow. Particularly in cybersecurity, the predictions that intelligence systems make based on the patterns they identify help analysts respond to emerging threats. AI is an attractive tool that can help contain the tide of cyberattacks and, with careful training, become an essential tool for the next generation of cybersecurity professionals .However, the current pace of AI innovation suggests that fully automated cyberbattles between attackers' AI and defenders' AI are likely still years away.

References

1. Abbas et al., 2019 N.N. Abbas, T. Ahmed, S.H.U. Shah, M. Omar, H.W. Park Investigating the applications of artificial intelligence in cyber security Scientometrics, 121 (2) (2019), pp. 1189-1211.
2. Bhardwaj, M.D. Alshehri, K. Kaushik, H.J. Alyamani, M. Kumar Secure framework against cyber-attacks on cyber-physical robotic systems J. Electron. Imaging, 31 (6) (2022).
3. P. Chithaluru, A.T. Fadi, M. Kumar, T. Stephan Computational intelligence inspired adaptive opportunistic clustering approach for industrial IoT networks IEEE Internet Things J (2023).
4. M. Barrett Technical Report National Institute of Standards and Technology, Gaithersburg, MD, USA (2018).
5. I. Wiafe, F.N. Koranteng, E.N. Obeng, N. Assyne, A. Wiafe, S.R. Gulliver Artificial intelligence for cybersecurity: a systematic mapping of literature IEEE Access, 8 (2020).
6. Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang, K.K.R. Choo Artificial intelligence in cyber security: research advances, challenges, and opportunities Artif. Intell. Rev., 55 (2022).

7. J. Martínez Torres, C. Iglesias Comesaña, P.J. García-Nieto Machine learning techniques applied to cybersecurity Int. J. Mach. Learn. Cybern., 10 (10) (2019).
8. T.C. Truong, I. Zelinka, J. Plucar, M. Čandík, V. Šulc Artificial intelligence and cybersecurity: past, presence, and future Artificial intelligence and evolutionary computations in engineering systems (2020).
9. Agrawal et al., 2023 V. Agrawal, M. Hazratifard, H. Elmiligi, F. Gebali Electrocardiogram (ECG)-Based user Authentication using deep learning algorithms Diagnostics, 13 (3) (2023).
10. F. Ahamed, F. Farid, B. Suleiman, Z. Jan, L.A. Wahsheh, S. Shahrestani
11. An intelligent Multimodal Biometric Authentication model for Personalised healthcare services Future Internet, 14 (8) (2022).
12. K. AL-Dosari, N. Fetais, M. Kucukvar Artificial intelligence and cyber defense system for Banking Industry: A qualitative study of AI applications and challenges. Cybernetics and systems (2022).
13. A.M. AL-Hawamleh Predictions of cybersecurity experts on future cyber-attacks and related cybersecurity measures International Journal of Advanced Computer Science and Applications, 14 (2) (2023).