International Journal of Advanced Engineering Research and Science (IJAERS)
Peer-Reviewed Journal
ISSN: 2349-6495(P) | 2456-1908(O)
Vol-10, Issue-5; May, 2023
Journal Home Page Available: https://ijaers.com/
Article DOI: https://dx.doi.org/10.22161/ijaers.105.8

Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention

Mohammed Rizvi

Exelon Corporation, Chicago, IL USA

Received: 11 Apr 2023,

Receive in revised form: 08 May 2023,

Accepted: 18 May 2023,

Available online: 26 May 2023

©2023 The Author(s). Published by AI Publication. This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/).

Keywords*— *Cybersecurity, Artificial Intelligence (AI), threat detection and prevention, incident response system.

Abstract *— Due to its ability to evaluate security threats in real-time and take appropriate action, artificial intelligence has emerged as a key component of cyber security. AI now has a bigger impact on spotting and stopping attacks that keep businesses on the cutting edge. Threat detection and prevention are the main focus of AI's role in cybersecurity. Artificial intelligence can detect trends and anomalies in network traffic and user behavior that may indicate a potential cyberattack through the use of machine learning algorithms and advanced data analysis. This allows security personnel to respond to potential attacks quickly and proactively. Through predictive modeling, AI can be used to prevent attacks. AI also can recognize potential threats before they occur and take action to avoid them by assessing past attacks and detecting similarities. Creating automated incident response systems is another important function of artificial intelligence in cybersecurity. These systems can evaluate data, identify potential risks, and then work to contain or mitigate the attack, minimizing damage and disruption. Businesses must employ artificial intelligence in cybersecurity to protect their networks and sensitive data from ever changing online threats. Because of its ability to analyze vast volumes of data in real time and automate incident response, AI is swiftly becoming into a key tool for efficient cybersecurity in today's digital environment. In this paper, we will discuss the role of AI in cybersecurity including its uses in threat detection and prevention.*

I. INTRODUCTION

Artificial Intelligence is become a serious technology in the fight against cybercrime. Artificial Intelligence-based cybersecurity solutions can detect and prevent threats in real time, automate response actions, and can help organizations stay ahead of cyber threats (Srivastava et al., 2021). Cybercrime has been growing rapidly and traditional security measures are no longer sufficient to protect against advanced cyber threats (Shamiulla, 2019a). AI is a vital technology for cybersecurity because it can analyze and identify threats, predict future attacks, and automate response actions. AI-based cybersecurity solutions can use machine learning and deep learning algorithms to analyze large volumes of data and information to identify patterns and anomalies which indicate potential cyber threats (Bhatele et al., 2019a). These solutions are particularly useful for detecting new and emerging threats that traditional signature-based approaches may not use. AI is also capable of quickly analyzing enormous volumes of data, spotting trends, and learning from previous actions to anticipate and avert assaults in the future. Problem detection driven by AI can identify possible dangers instantly and cut down on the time it takes to notice and address the problem. Automation of threat detection and response is the main advantage of AI in cybersecurity (Harel et al., 2017a). AI-based solutions can automatically respond to threats and reduced the burden on human security analysts. This automation can also improve response times and AI can respond to threats in real time all the time. This automation can also help organizations to reduce the cost of cybersecurity by minimizing the need for human analysts (Xiaohua et al., 2021). AI can also help organizations to improve their security posture by identifying vulnerabilities in their respective systems and networks. By analyzing the network traffic AI can identify potential weak points and suggest techniques to mitigate these threats (Sadiku et al., 2020a). This approach to cybersecurity can help organizations prevent attacks before they occurred. Organizations looking for protection of their networks and sensitive data from growing cyber threats and are now relying on the use of artificial intelligence in cybersecurity. Organizations can proactively respond and mitigate the risk of data loss and disruption by using AI to detect and prevent attacks in real-time (Okutan & Eyüpoglu, 2021).

Creating automated incident response systems is an important function of artificial intelligence in cybersecurity. These systems can evaluate the data, identify potential risks and then work to contain or mitigate the attack, minimizing the damage and disruption. This is essential in the event of widespread attacks. Human support might not be able to respond in a timely enough manner. The use of AI in cybersecurity has both advantages and disadvantages (Zhang, Hamadi, et al., 2022). The most important application of AI in cybersecurity is threat intelligence. AI can analyze huge amounts of data from various sources that identify patterns and trends that indicate potential cyber threats (Sahoo & Yadav, 2022). By analyzing these data AI can help organizations stay ahead of cybercriminals by predicting and preventing future attacks. This threat intelligence can help organizations to improve their incident response capabilities by providing real-time information on emerging threats. AI can also improve cybersecurity by improving their authentication process and improve their access control systems (Abbas et al., 2019). By using AI-based biometric authentication systems the organizations can ensure that only authorized users can have access to their systems and networks. These systems can also detect and prevent unauthorized access attempts by analyzing user activities and can identify patterns that indicate potential threats. AI can also enhance end-points of security by detecting and responding to threats at the device level (Zhang, Ning, et al., 2022). By using AI-based powered end-point security solutions organizations can detect and prevent threats from infecting their devices even if they are not connected to these networks. These solutions can also help organizations to respond very quickly to threats by automatically isolating infected devices from the network. However, AI-based cybersecurity solutions also have some challenges, without these AI cannot be used in cybersecurity. The biggest challenge is the lack of transparency in AI algorithms (de Azambuja et al., 2023). It can be difficult to comprehend how an AI system makes judgements, which makes it tough to have faith in these systems. Another issue is the potential for false positives from AI systems, which could result in pointless alarms and more work for security analysts. Organizations should use new technologies such as AI to stay ahead of the curve as cyber risks evolve (Harel et al., 2017b). They can do this by keeping their networks and data secure and allowing them to focus on their key organization goals without having to worry about cyber security concerns.

II. ARTIFICIAL INTELLIGENCE TECHNIQUES IN CYBER SECURITY

AI techniques have revolutionized the field of cybersecurity. These are the techniques that enable cybersecurity professionals to analyze large amounts of data, detect anomalies and patterns and identify potential threats before they become actual attacks (Thuraisingham, 2020). Following are some common AI techniques that are being used in cyber security.

- **Machine Learning**

It is a type of AI that enable the systems to learn from data without being explicitly programmed. Machine Learning algorithms are trained on large datasets of both benign and malicious traffic to detect patterns and identify potential threats (Merat & Almuhtadi, 2015). ML is used for tasks like malware detection, network intrusion detection, and anomaly detection.

- **Natural Language Processing**

It is a type of AI that enables computers to understand and interpret human language. NLP is used in cybersecurity to analyze unstructured data sources like social media feeds and online forums for potential threats.

- **Deep Learning**

It is a subset of ML that utilizes deep neural networks to learn complex patterns from data. It is used in cybersecurity for tasks like malware detection, phishing detection, and fraud detection.

- **Reinforcement Learning**

It is a subset of ML that emphasizes judgement. Reinforcement learning can be used in cybersecurity to train systems to decide how to respond to attacks based on the situation and the perceived level of threat.

- **Computer Vision**

It is an AI technique that enables computers to interpret and analyze visual data. It is used in cybersecurity for tasks like facial recognition and video surveillance.

- **Expert Systems**

These are the AI systems that mimic the decision-making capabilities of a human expert in a particular domain. In cybersecurity, these systems are used for tasks like intrusion detection and response and vulnerability assessment.

III. THREAT DETECTION USING ARTIFICIAL INTELLIGENCE

Whether it is physical security, cybersecurity, or homeland security. Threat detection is an essential component of keeping people and organizations safe. Detecting and eliminating threats in real-time has become easier, thanks to advances in artificial intelligence technology (Shamiulla, 2019b). Security systems can detect risks and threats faster, more accurately, and more efficiently thanks to AI-based threat detection systems. AI-based threat detection systems learn from massive volumes of data and find patterns that can hint at potential dangers using algorithms and machine learning techniques (G. A., 2022). Network traffic, video surveillance footage, and social media feeds are just a few of the data types that may be used for training AI algorithms to identify and notify security personnel of potential security breaches or threats (Soni, n.d.).

The use of deep learning techniques allows the algorithms to learn from vast data sets and discover even tiny patterns. That may suggest possible risks are one of the most important aspects of AI-based threat detection. Deep learning simulates the learning process of the human brain using neural networks which allow the algorithms to become more accurate over time by recognizing and learning from new data points (Rehman, 2022). Security teams can respond fast and stop possible risks from developing into significant security events thanks to AI-based threat detection which is very effective at spotting threats in real time. These systems can simultaneously analyze data from several sources which enables them to identify and track threats across various systems and networks (Jenis Nilkanth Welukar & Gagan Prashant Bajoria, 2021).

Depending on the type of data and algorithms utilized, threat detection systems based on AI can detect a variety of dangers. These technologies for example can recognize malware, phishing scams, and other online risks (Kuzlu et al., 2021). AI can detect suspicious activity or behavior in video surveillance footage such as unauthorized access or theft in the context of physical security. AI can examine data from social media feeds in homeland security to identify potential terrorist threats. AI for threat detection has several advantages. Because AI-based systems are so effective and precise and security teams can identify threats immediately and take action. These systems are perfect for analyzing data from several sources at once because they can swiftly analyze massive amounts of data. The accuracy of AI systems can also be improved over time by learning from new data and adapting to it that lowering the possibility of false positives (Sadiku et al., 2020b).

IV. ARTIFICIAL INTELLIGENCE BASED APPROACHES IN CYBER SECURITY

Thanks to advances in computing technology our society is rapidly changing (Mehra & Badotra, 2021). People's everyday routines and employment are significantly impacted by this. Some of these technologies have made it possible to develop computers that have cognitive abilities similar to those of humans, including the ability to learn, make decisions, and solve problems. AI can analyze enormous amounts of data, for instance, and can make judgements in real time while using intelligence. Numerous fields of research and technology benefit from the usage of AI techniques (Achi et al., 2021). It's no secret that the Internet is filled with a lot of personal data which leads to a lot of cybersecurity problems. First, the amount of data makes manual analysis all but impossible. Secondly, there may be dangers based on AI or rising threats. Additionally, the expense of preventing threats rises due to the high cost of hiring specialists (Ansari et al., 2022). The development and application of algorithms to identify those dangers likewise involve a lot of time, money, and effort. Utilizing AI-based techniques is one remedy for those problems. AI is capable of quickly, correctly, and efficiently analyzing massive amounts of data (*Cyber_Security_Based_on_Artificial_Intelligence_for_Cyber-Physical_Systems*, n.d.). An AI-based system can predict future assaults that will be similar to those that have already occurred by using threat history, even if the patterns of those attacks vary. AI can handle vast data, find new and significant changes in attacks, and continuously improve its security system's response to threats. The application of AI to cybersecurity has changed the traditional security approach from reactive to proactive and assisting in the real-time identification and mitigation of threats (Rawat et al., 2022). Here are some of the AI-based approaches in cybersecurity:

- **Threat Detection and Analysis**

AI-based threat detection systems can automatically analyze vast amounts of data and identify potential security threats. Machine learning algorithms can detect patterns and anomalies in network traffic and identify malicious code in files and analyze user behavior to detect suspicious activities (Bishtawi & Alzubi, 2022).

- **Fraud Detection**

AI-based fraud detection systems can analyze massive amounts of data to detect fraudulent transactions or activities. These systems can identify unusual patterns, behaviors, and trends in financial transactions and help to detect fraud in real-time (Benzaïd & Taleb, 2020).

- **User and Entity Behavior Analytics**

UEBA is an AI-based approach that uses machine learning algorithms to identify suspicious activities and behaviors in user accounts and devices. It can detect malicious insiders or compromised accounts which are challenging to detect with traditional security methods.

- **Incident Response**

AI-based incident response systems can automate the response to cyber threats that reduced the time required to respond to an attack. These systems can analyze data from various sources and provide actionable insights to the security team to take appropriate action quickly (Bhatele et al., 2019b).

- **Chatbots and Virtual Assistants**

AI-powered chatbots and virtual assistants can help to automate routine security tasks, such as password resets and account management. They can also provide instant assistance to users helping them to resolve security-related issues quickly.

- **Threat Intelligence**

AI-based threat intelligence systems can analyze massive amounts of data from various sources to identify emerging threats and vulnerabilities (Li, 2018). They can provide real-time threat intelligence that helps organizations proactively protect against cyber threats.

V. DISCUSSION

In the past few years, artificial intelligence has become a significant tool employed in the field of cybersecurity (Rekha et al., 2020). Organizations have started using AI-based systems for the detection and prevention of cyberattacks as a result of the volume and complexity of cyber threats increasing daily.

a) Threat Detection using AI

The primary role of AI in cybersecurity is threat detection. Systems for detecting threats in the past have focused on signature-based strategies, which can only identify known threats. However, these solutions are no longer as effective due to the growing sophistication of cyber threats. However, AI-based systems can identify both known and unidentified dangers by utilizing sophisticated algorithms and machine learning models. Machine Learning is one of the most commonly used AI techniques in threat detection (Ghillani, 2022). ML models can analyze large amounts of data and identify patterns that are indicative of a threat. The models are trained on datasets of both benign and malicious traffic which allows them to learn to identify potential threats accurately. For example, ML models can detect anomalous network behavior which may indicate a potential cyberattack. Deep Learning is another AI technique used in threat detection. Deep Learning models use deep neural networks to analyze and classify data. These models are able to recognize intricate patterns and categorize them as either good or bad. Deep Learning models, for instance, can recognize and categorize malware, phishing scams, and other cyber threats. Threat detection uses Natural Language Processing (NLP), another AI tool. NLP models can analyze unstructured data sources like social media feeds and online forums to identify potential threats. The models can extract information from text data and use it to improve threat detection accuracy (Alhayani et al., 2021).

b) Threat Prevention using AI

Furthermore, to the threat detection, AI can be used for threat prevention. AI-based systems can identify potential threats and take proactive measures to prevent them from causing harm. Here are a few examples of how AI is being utilized to counter threats:

- Intrusion Prevention

Artificial intelligence-based intrusion prevention systems can detect and stop intrusions before they enter the network.

- Malware Prevention

AI-based antimalware systems can detect and prevent the installation of malicious software.

- Phishing Prevention

AI-based ant phishing systems can detect and prevent phishing attacks by analyzing emails and identifying suspicious content.

- Vulnerability Assessment

AI-based vulnerability assessment systems can identify potential vulnerabilities in the network and take proactive measures to mitigate them.

- Access Control

AI-based access control systems can identify potential threats and deny access to unauthorized users.

VI. CONCLUSION

Artificial intelligence's place in cybersecurity is quickly developing and becoming more and more important to businesses. Traditional methods of threat detection and prevention are no longer adequate given the complexity and sophistication of cyber threats, which are constantly evolving. AI-based systems provide complex and cutting-edge methods to counter cyber-attacks. To identify and stop cyber risks, AI-based systems employ methods including machine learning, deep learning, natural language processing, predictive analytics, and behavioral analytics. These systems have the ability to analyze enormous volumes of data, find patterns, and make predictions that are not achievable using conventional techniques. Additionally, AI-based systems are a useful tool for businesses that want to remain ahead of cyber threats since they can identify and stop both known and new dangers. These systems are an all-in-one cybersecurity solution since they can be used for access control, vulnerability assessment, intrusion prevention, malware prevention, and phishing prevention. The application of AI in cybersecurity will develop along with the technology. For their systems to remain safe from cyber assaults, organizations will need to adapt and adopt these cutting-edge solutions. AI will soon play a crucial role in cybersecurity, and companies that invest in these technologies will be better able to protect themselves from online threats.

AVAILABILITY OF DATA AND MATERIALS

As the author of this paper I have used various open access research papers available online for this review. All the citations are included in the paper.

FUNDING

As the author of this paper I received no funding for this work.

ACKNOWLEDGEMENTS

I would like to express my appreciation for the time and effort that the reviewers and editorial team will invest in evaluating my submission.

Should my paper be accepted for publication, I look forward to the opportunity to engage with the editorial team and make any revisions required to ensure the highest quality of scholarship.

Thank you for considering my submission, and I look forward to hearing from you soon.

REFERENCES

[1] Abbas, N. N., Ahmed, T., Shah, S. H. U., Omar, M., & Park, H. W. (2019). Investigating the applications of artificial intelligence in cyber security. *Scientometrics*, *121*(2), 1189–1211. https://doi.org/10.1007/s11192-019-03222-9

[2] Achi, A., Kuwunidi Job, G., Shittu, F., Baba Atiku, S., Unimke Aaron, A., & Zahraddeen Yakubu, I. (2021). SEE PROFILE Survey On The Applications Of Artificial Intelligence In Cyber Security. *Survey On The Applications Of Artificial Intelligence In Cyber Security Article in International Journal of Scientific & Technology Research*. www.ijstr.org

[3] Alhayani, B., Jasim Mohammed, H., Zeghaiton Chaloob, I., & Saleh Ahmed, J. (2021). WITHDRAWN: Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2021.02.531

[4] Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. *IJARCCE*, *11*(9). https://doi.org/10.17148/ijarcce.2022.11912

[5] Benzaïd, C., & Taleb, T. (2020). AI for beyond 5G Networks: A Cyber-Security Defense or Offense Enabler? *IEEE Network*, *34*(6), 140–147. https://doi.org/10.1109/MNET.011.2000088

[6] Bhatele, K. R., Shrivastava, H., & Kumari, N. (2019a). *The Role of Artificial Intelligence in Cyber Security* (pp. 170–192). https://doi.org/10.4018/978-1-5225-8241-0.ch009

[7] Bhatele, K. R., Shrivastava, H., & Kumari, N. (2019b). *The Role of Artificial Intelligence in Cyber Security* (pp. 170–192). https://doi.org/10.4018/978-1-5225-8241-0.ch009

[8] Bishtawi, T., & Alzubi, R. (2022). Cyber Security of Mobile Applications Using Artificial Intelligence. *1st International Engineering Conference on Electrical, Energy, and Artificial Intelligence, EICEEAI 2022*. https://doi.org/10.1109/EICEEAI56378.2022.10050484

[9] *Cyber_Security_Based_on_Artificial_Intelligence_for_Cyber-Physical_Systems*. (n.d.).

[10] de Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. *Electronics*, *12*(8), 1920. https://doi.org/10.3390/electronics12081920

[11] G. A., S. (2022). The Review of Artificial Intelligence in Cyber Security. *International Journal for Research in Applied Science and Engineering Technology*, *10*(1), 1461–1468. https://doi.org/10.22214/ijraset.2022.40072

[12] Ghillani, D. (2022). Deep Learning and Artificial Intelligence Framework to Improve the Cyber Security. *American Journal of Artificial Intelligence*, *x*, *No. x*, x–x. https://doi.org/10.22541/au.166379475.54266021/v1

[13] Harel, Y., Gal, I. Ben, & Elovici, Y. (2017a). Cyber security and the role of intelligent systems in addressing its challenges. *ACM Transactions on Intelligent Systems and Technology*, *8*(4). https://doi.org/10.1145/3057729

[14] Harel, Y., Gal, I. Ben, & Elovici, Y. (2017b). Cyber security and the role of intelligent systems in addressing its challenges. *ACM Transactions on Intelligent Systems and Technology*, *8*(4). https://doi.org/10.1145/3057729

[15] Jenis Nilkanth Welukar, & Gagan Prashant Bajoria. (2021). Artificial Intelligence in Cyber Security - A Review.

International Journal of Scientific Research in Science and Technology, 488–491. https://doi.org/10.32628/ijsrst218675

[16] Kuzlu, M., Fair, C., & Guler, O. (2021). Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. *Discover Internet of Things*, *1*(1). https://doi.org/10.1007/s43926-020-00001-4

[17] Li, J. hua. (2018). Cyber security meets artificial intelligence: a survey. In *Frontiers of Information Technology and Electronic Engineering* (Vol. 19, Issue 12, pp. 1462–1474). Zhejiang University. https://doi.org/10.1631/FITEE.1800573

[18] Mehra, A., & Badotra, S. (2021). Artificial Intelligence Enabled Cyber Security. *Proceedings of IEEE International Conference on Signal Processing,Computing and Control*, *2021-October*, 572–575. https://doi.org/10.1109/ISPCC53510.2021.9609376

[19] Merat, S., & Almuhtadi, W. (2015). Artificial intelligence application for improving cyber-security acquirement. *Canadian Conference on Electrical and Computer Engineering*, *2015-June*(June), 1445–1450. https://doi.org/10.1109/CCECE.2015.7129493

[20] Okutan, A., & Eyüpoglu, C. (2021). A Review on Artificial Intelligence and Cyber Security. *Proceedings - 6th International Conference on Computer Science and Engineering, UBMK 2021*, 304–309. https://doi.org/10.1109/UBMK52708.2021.9558949

[21] Rawat, B. S., Gangodkar, D., Talukdar, V., Saxena, K., Kaur, C., & Singh, S. P. (2022). The Empirical Analysis of Artificial Intelligence Approaches for Enhancing the Cyber Security for Better Quality. *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*, 247–250. https://doi.org/10.1109/IC3I56241.2022.10072877

[22] Rehman, S. F. U. (2022). Practical Implementation of Artificial Intelligence in Cybersecurity – A Study. *IJARCCE*, *11*(11). https://doi.org/10.17148/ijarcce.2022.111103

[23] Rekha, G., Malik, S., Tyagi, A. K., & Nair, M. M. (2020). Intrusion detection in cyber security: Role of machine learning and data mining in cyber security. *Advances in Science, Technology and Engineering Systems*, *5*(3), 72–81. https://doi.org/10.25046/aj050310

[24] Sadiku, M. N. O., Fagbohungbe, O. I., & Musa, S. M. (2020a). Artificial Intelligence in Cyber Security. *International Journal of Engineering Research and Advanced Technology*, *06*(05), 01–07. https://doi.org/10.31695/IJERAT.2020.3612

[25] Sadiku, M. N. O., Fagbohungbe, O. I., & Musa, S. M. (2020b). Artificial Intelligence in Cyber Security. *International Journal of Engineering Research and Advanced Technology*, *06*(05), 01–07. https://doi.org/10.31695/IJERAT.2020.3612

[26] Sahoo, B. M., & Yadav, S. A. (Eds.). (2022). *Information Security Practices for the Internet of Things, 5G, and Next-Generation Wireless Networks*. IGI Global. https://doi.org/10.4018/978-1-6684-3921-0

[27] Shamiulla, A. M. (2019a). Role of artificial intelligence in cyber security. *International Journal of Innovative Technology and Exploring Engineering*, *9*(1), 4628–4630. https://doi.org/10.35940/ijitee.A6115.119119

[28] Shamiulla, A. M. (2019b). Role of artificial intelligence in cyber security. *International Journal of Innovative Technology and Exploring Engineering*, *9*(1), 4628–4630. https://doi.org/10.35940/ijitee.A6115.119119

[29] Soni, V. D. (n.d.). *ROLE OF ARTIFICIAL INTELLIGENCE IN COMBATING CYBER THREATS IN BANKING*. www.iejrd.com

[30] Srivastava, S., Benny, B., Priyanka, M., Ma'am, G., Batra, N., & Am, M. '. (2021). *EasyChair Preprint Artificial Intelligence (A.I.) and It's Application in Cyber Security ARTIFICIAL INTELLIGENCE (A.I.) AND IT'S APPLICATION IN CYBER SECURITY*.

[31] Thuraisingham, B. (2020). The role of artificial intelligence and cyber security for social media. *Proceedings - 2020 IEEE 34th International Parallel and Distributed Processing Symposium Workshops, IPDPSW 2020*, 1116–1118. https://doi.org/10.1109/IPDPSW50202.2020.00184

[32] Xiaohua, F., Marc, C., Elias, E., & Khalid, H. (2021). Artificial Intelligence and Blockchain for Future Cyber Security Application. *2021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, 802–805. https://doi.org/10.1109/DASC-PICom-CBDCom-CyberSciTech52372.2021.00133

[33] Zhang, Z., Hamadi, H. Al, Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. *IEEE Access*, *10*, 93104–93139. https://doi.org/10.1109/ACCESS.2022.3204051

[34] Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, *55*(2), 1029–1053. https://doi.org/10.1007/s10462-021-09976-0