UDC: 004.89:004.5/.7.056.2
Professional paper

ENHANCING CYBERSECURITY AND DATA PROTECTION THROUGH INTELLIGENT ROBOTS

Avni RUSTEMI[1], Aliadis SELIMI[1], Eip RUFATI[1], Florin ASANI[1]

[1]*Department of Informatics, University of Tetova, North Macedonia*

Abstract

Recent technological developments are revolutionizing all areas of life, including artificial intelligence, which is being implemented in many fields, such as economics, medicine, cybersecurity, education, agriculture, etc. The more artificial intelligence is implemented, on the one hand, it facilitates and automates many tasks in various fields, but on the other hand, many issues and problems arise regarding the security, privacy, and reliability of intelligent robots. The implementation of AI in cybersecurity, in addition to helping developers protect themselves and be warned of various attacks that can threaten various systems, on the other hand, allows and empowers malicious people to create various malicious algorithms, to access various data, and misuse it. Artificial intelligence, thanks to its techniques such as machine learning, predictive analytics, and federated learning, is finding application in many systems, which are slowly replacing the human factor. AI can perform analysis, process data much faster than humans, and, above all, based on data analysis, create strategies for managing and preventing various attacks. Cybersecurity is an area that should be given great importance, because all data between different systems is carried and transmitted over the network to different databases. If this data were to be attacked and decrypted, then it would be a major disaster both in terms of society and in terms of privacy, ethics, and security. Therefore, mechanisms and strategies for cyber protection must be created, even despite the implementation of AI intelligent robots, because they can also be attacked by malicious people. The combination of IoT, blockchain technology, and AI, at the moment, represents a hope for cyber protection, although attempts are being made all the time to find mechanisms that will combat the synergy of these technologies, in particular through the power of quantum computers. Through the work, we will try to make an overview of these very important phenomena for society and present the main elements of how programmers can be protected and how ethical is the use of intelligent robots in cybersecurity.

Keywords: cybersecurity, artificial intelligence, blockchain technology, attacks, synergy.

I. Introduction

The development of contemporary technologies, including artificial intelligence, is marking a major technological development, with the whole world experiencing a new era of digitalization, where special emphasis is placed on security, privacy, automation and the use of intelligent robots. This technological revolution, including artificial intelligence, can be compared to the advent of the Internet for the first time, because in general the world is starting to change, and AI is starting to be integrated into all aspects of life, including the technologies we use, business, education, medicine, and all spheres of life. Despite technological developments and the positive promises that these technologies offer, there are still concerns regarding cybersecurity, privacy, and data security. Advanced AI techniques and algorithms in cybersecurity, among others, focus on the abilities of intelligent robots to detect, analyze and neutralize various threats with or without human intervention. Cybersecurity is a coordinated use of policies, tools, and technology to manage risks and protect digital systems from threats. This paper presents an important overview of AI in cybersecurity, the advantages, and ethical issues that arise in this regard. Artificial agents can be used to protect the system and their vulnerabilities, but they can also be used for various cyber attacks that target the architectural infrastructures of various systems [1]. There are many cases of various cyber attacks, where we can highlight WannaCry and NotPetya which are among the most famous and well-known

attacks that illustrated, among other things, the powerful capacity that malicious people and intelligent agents can have. These attacks affect a lot of private information, services, elements of architectural infrastructure, including hospital and banking servers, and even end-user devices, including mobile phones and personal computers. Therefore, to protect yourself from these cyberattacks, which, in addition to malicious people, are also being helped by various intelligent agents, the best possible way to counter them is to use intelligent agents, because only through agents can possible attacks on various systems be detected quickly and warned [2]. As malicious actors increasingly develop and empower various intelligent agents based on AI, cybersecurity has become a contemporary challenge where defenders must constantly renew critical system infrastructures and replace them with techniques and security measures in line with the latest technological developments. In this regard, blockchain technology represents a hope for cybersecurity, especially in terms of security, transparency, and data immutability. Also, the ethical concerns of integrating AI into data management systems are evident among users. It is evident that many AI systems have been trained and improved using user data, however, protection measures in terms of confidentiality, privacy have been lacking, causing users to lose trust in these technologies.

II. Literature review

Deep learning improves, among other things, the detection and reaction time, combining with human supervision to address ethical and functional limitations, where, among other things, in [3], the dual role of AI in cybersecurity is underlined. Also, in [4], the importance of analyzing the ethical issue regarding the use of AI in cybersecurity is underlined, warning that failure to comply with protective measures can lead to the compromise of data privacy. Machine learning and deep learning can detect threats in real time, analyze the vulnerability of the system to malicious people, and react in time to possible incidents, because the same techniques can analyze and make the best possible decisions based on the knowledge they receive from sensors and other real physical devices in terms of the management and decision-making process [5]. In [6], the importance of incorporating AI, blockchain technology, deep learning, and other AI techniques in order to improve IoT security is emphasized, underlining intelligent algorithms for detecting and preventing various threats in real time, in order to address scalability challenges.

Among others, in [7], the importance of integrating blockchain, with cybersecurity and AI, in the Internet of Things in medicine is emphasized, when, among other things, it increases the protection of sensitive patient data through decentralized encryption and decentralized identity, offering higher security. The combination of these technologies, among other things, offers secure exchange of private patient data and efficient interaction and services of medical personnel. Kuzlu et al. [8] study the role of AI development in cybersecurity of IoT devices, analyzing, among other things, advanced AI techniques and algorithms such as neural networks and support vector machines, as well as the most frequent threats used by cyber attackers, to identify their weaknesses and strengths. Jonas et al. [9] explain, among other things, that integrating AI into cybersecurity frameworks and architectures particularly improves early detection of potential threats and overall system security. Based on their surveys, they concluded that AI positively impacts security, and most researchers believe in the effectiveness of AI in preventing and early detection of threats. This contributes to faster and more accurate decision-making, especially in cybersecurity-related actions.

Tao et al. [10] emphasize that AI, and in particular machine learning techniques such as support vector machines, have had a positive impact on the detection of real intrusions and the prevention of false alarms for cyberattacks, also thanks to the combination with contemporary techniques of blockchain, IoT, and cyber forensics. However, challenges in this direction

remain numerous, especially in terms of privacy, prediction, and the creation of long-term strategies for the prevention of attacks and the long-term protection of personal data, which are the targets of malicious persons.
Finally, AI techniques, in addition to being used for protection against cyberattacks, can also be used by cyberattacks to deceive various systems or to decrypt data in various data management systems, which is why recently the implementation of technologies such as BT and quantum computing has been seen as a possibility as a hope for more secure protection against current possible threats. Through Figure 1, we have presented the most important elements that should be taken into account when using AI to protect against various cyberattacks.

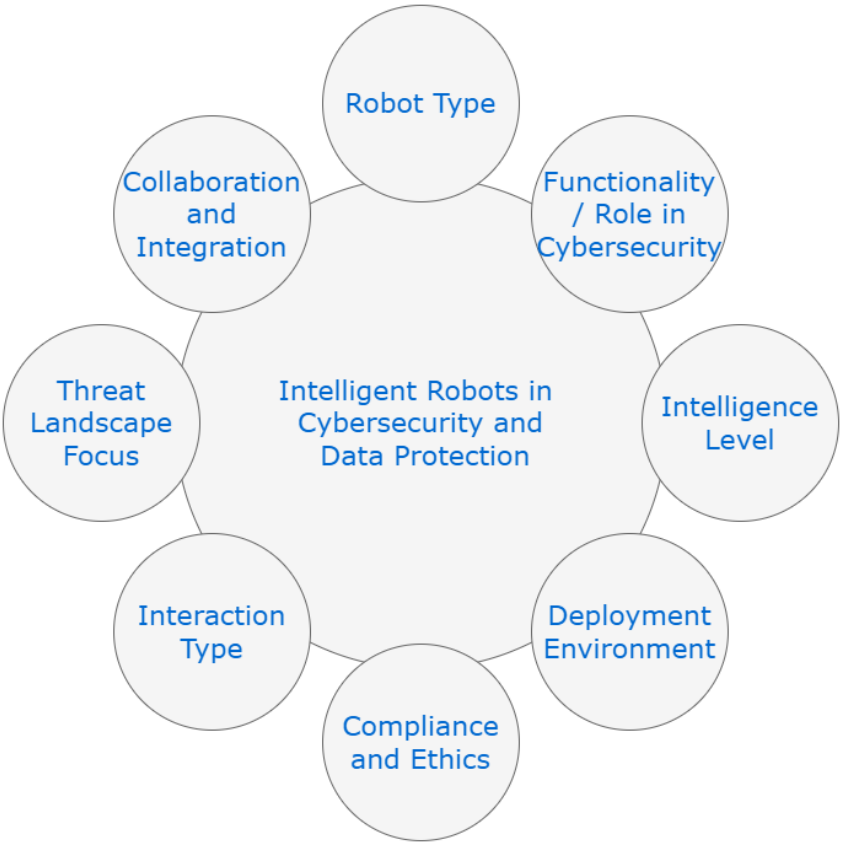

Figure 1. AI influencing factors in cybersecurity

III. Artificial intelligence in cybersecurity: from anomaly detection to predictive analytics

AI has transformed the field of cybersecurity by introducing advanced intelligent systems that can automate the processes of predicting, detecting, and responding to cyber threats promptly. Traditional cybersecurity approaches have relied primarily on predefined rules and manual interventions, which often fail to keep pace with the increasingly sophisticated nature of cyber threats. AI represents one of the most advanced technological developments of the modern era. It has distilled the capacity of machines, enabling them to perform sophisticated calculations and tasks with high precision. The development of artificial intelligence is considered one of the greatest achievements of humanity, surpassing most current capacities. The main attempts and objective are to create devices that can function autonomously and efficiently, without any limitations and independent of third parties [11].
The inclusion of blockchain technology within AI-driven cybersecurity frameworks represents a hope towards increasing the integrity, privacy, scalability, and stability of systems that manage

data. The decentralized nature of the blockchain architecture, among other things, encourages data consistency and data distribution mechanisms, thus mitigating the risks associated with single points of failure and unauthorized data manipulation. Transparency and traceability, as characteristics of blockchain technology, create a richer and more reliable environment for security operations, especially in contexts that require verification and auditing of transactions [12]. Blockchain technology enables the development of reliable systems without requiring trust between network participants, and is based primarily on the non-repudiation of information and the distributed ledger in which all actions related to participants in the blockchain network are stored [13].

Cybersecurity is not a recent development. For decades, many techniques and methods, such as statistical modeling, pattern matching, have been used to identify anomalies in the network. AI, due to its capabilities to analyze large volumes of data, determine attack patterns, and support rational decision-making of agents, has begun to be recommended for use in the network, for detecting and preventing cyberattacks [14]. AI encompasses a combination of computational procedures that power techniques that include a wide range from supervised and unsupervised understanding algorithms, to probabilistic logic and heuristic optimization. Protection from cyber attacks can be superficially described in 4 main phases: Prevention, Detection, Response, and Recovery. Each phase plays an important role, which we have briefly outlined in Figure 2.

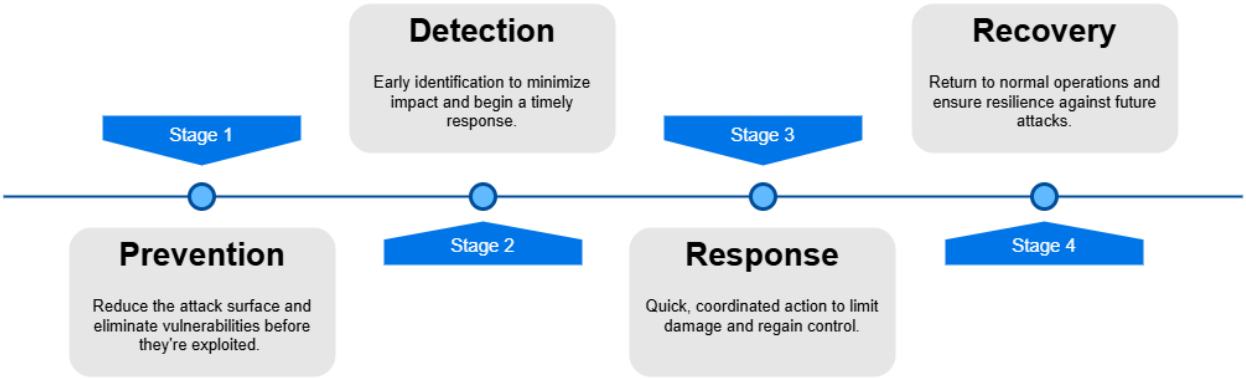

Figure 2. Protection from cyber attacks

Machine learning facilitates decision-making and prediction by drawing abstractions and conclusions based on the analytics of data collected from IoT sensors. ML has shown effectiveness in making more rational decisions while simultaneously detecting and preventing various cyberattacks. Through sophisticated algorithms that analyze the behavior of malicious people and their attempts at various cyberattacks, ML collects information, analyzes it, and makes important decisions in an automatic way to prevent various cyberattacks [15]. Identifying anomalies through ML relies on the fact that sophisticated algorithms can adapt to dynamic changes by learning through movement and changing their parameters depending on the evolving data [16]. Deep learning, also a subset of machine learning, is one of the powerful techniques in cybersecurity due to its ability to process large amounts of data and make decisions without manual intervention.

Deep learning techniques such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs) have been effectively applied to detect system intrusions, analyze and process large amounts of data, and make more rational decisions [17]. Due to their flexibility, deep learning and machine learning frameworks offer high accuracy in classifying and detecting potential attacks. Predictive analytics and methodologies that use advanced algorithms to predict potential threats and high-risk areas are an important part of creating a long-term strategy, which is taken in combination with the analysis of intelligent agents that, through Artificial Intelligence Theory of Pattern Recognition, can guide developers to areas where there

is a greater risk of cyberattacks [17]. Through Figure 3, we have presented some key contributions that relate to cybersecurity and the application of ML, DL, Predictive analytics, and intelligent agents. Despite the implementation of many AI models and architectures for cyber defense, there are still many challenges, especially in terms of adversarial attacks, where attackers can fool various AI models. The black box nature of DL makes it difficult to interpret decisions and on what basis the decision was made.

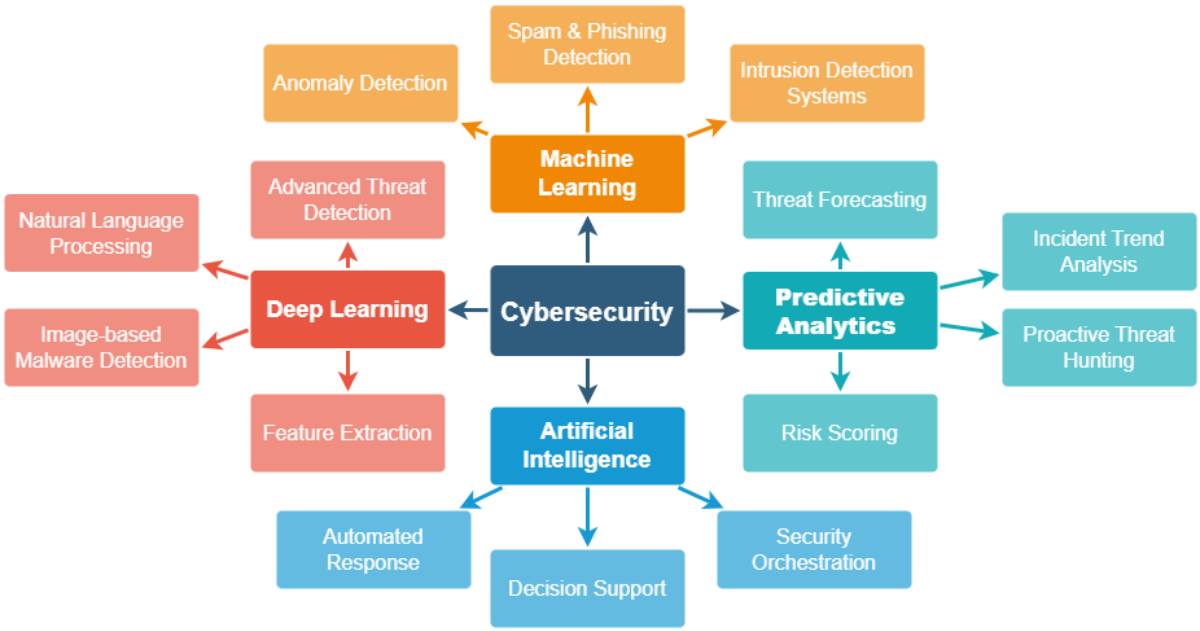

Figure 3. Contributions of contemporary technologies to protection against cyber attacks

IV. Blockchain technology in cyber security

Although BT is more widespread in cryptocurrencies, and the benefits they bring are the same, again, some aspects of this technology have found implementation in many areas, while some aspects are facing various challenges, especially those of high-capacity data management. BT is used as a synonym for creating various systems without having trust between participants, but the same trust is slowly gained through the fair and efficient work that this technology follows, and it does not allow manipulations between blockchain participants [18]. Having the characteristic of non-repudiation and transparency of transactions, BT guarantees accountability for each transaction, and in particular, the use of this technology in cybersecurity is also seen as possible, especially in services that rely on public key cryptography [19]. In cryptographic standards, different entities manage the lifecycle by protecting the keys they use, especially private keys, and this approach often requires centralized infrastructures known as Certificate Authorities (CAs), which often present weaknesses, because privacy, data integrity, and above all, the trust that participants have in the providers that provide these certificates are called into question.

Blockchain, among other things, offers a chain of decentralized blocks, which, through consensus mechanisms, a distributed ledger increases trustworthiness, because, among other things, they offer secure communication and protection of the integrity of data and digital transactions. Any data that is stored in the blockchain, the same cannot be deleted, but can only be regenerated with another unique hash value, which orients us that we are dealing with another transaction [20]. Among blockchain platforms, Hyperledger Fabric is the most preferred in cybersecurity because it has a permissioned blockchain structure, where not everyone can connect to the network, but the same must pass through several filters, and it has a more

sophisticated data protection architecture. Hyperledger enables the isolation of transactions through private channels and consensus mechanisms that developers themselves can create in a personalized form, and among other things, offers higher data security and auditing between already verified subjects. Through Hyperledger, cybersecurity is controlled more directly because there is controlled access based on roles that are created in advance, thus reducing the weaknesses associated with open networks and minimizing unauthorized data exposure. BT, among other things, has several contributions to cybersecurity, including the detection of possible unauthorized intrusions and changes, reducing the possibility of identity theft and phishing, secure communication, validating the authentication of each update on the blockchain network, and creating trust in data sharing between network participants [21]. Some other characteristics related to increasing cybersecurity through the use of BT are illustrated in Figure 4.

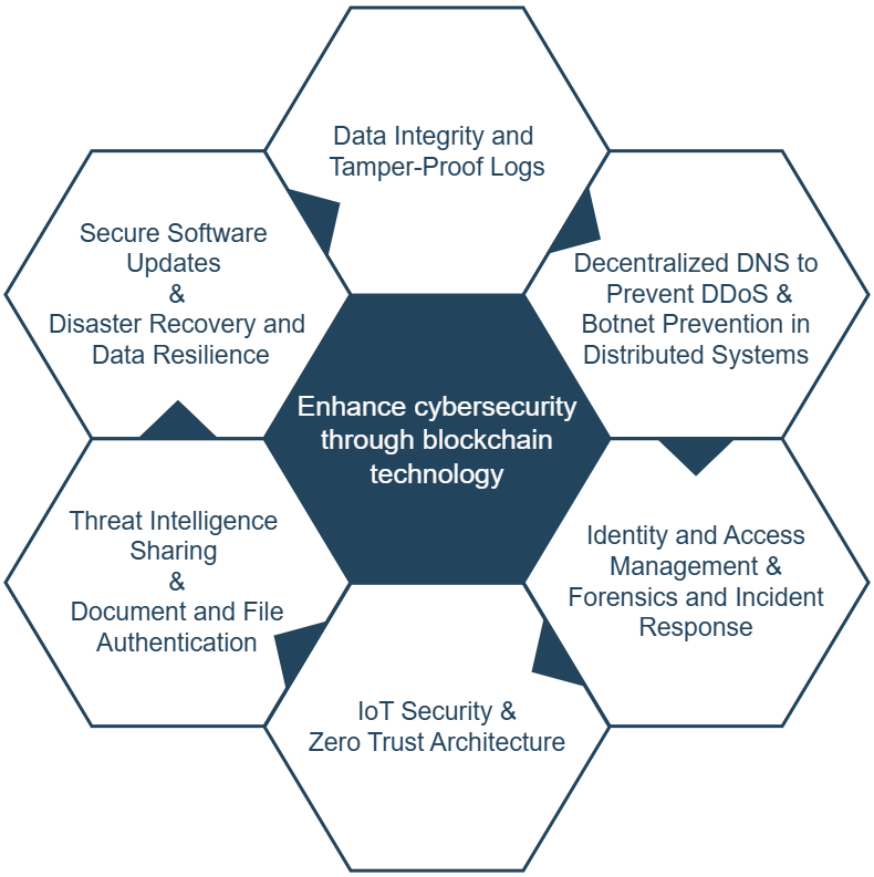

Figure 4. Blockchain technology application to cybersecurity

V. Conclusion and future work

Homomorphic encryption is a cryptographic approach that aims to manage data without requiring decryption. Homomorphic encryption promotes the deployment of AI models, effectively attempting to do so without exposing data to potential leaks. AI is primarily used to improve threat detection and response, including real-time detection and automated responses. ML detects system anomalies, predicts threats based on predictive analytics, while blockchain is primarily used for identity verification, data traceability, integrity maintenance, and IoT device management. Cyber threats are increasingly growing and more sophisticated, intelligent robots, blockchain technology, IoT, and contemporary technologies represent an important step towards creating autonomous systems, more reliable and resistant to the various attacks that can be threatened. These intelligent robots, supported by AI, ML, DL, and other techniques, can identify, among other things, anomalies, risks in real time, and analyze unexpected behaviors

in networks, to make quick decisions and detect whether it is an attack or a system release. Intelligent robots can improve automated processes that protect the system by reducing dependence on human intervention and minimizing errors. The integration of technologies such as blockchain undoubtedly increases transparency, security, making it more reliable and resistant to unauthorized manipulations. Even though contemporary technologies are increasingly attempting to advance cryptographic algorithms for cyber protection, there are still many challenges and obstacles during practical implementations. Therefore, with the development of Industry 5.0 and the advancement of these technologies in terms of addressing the real practical challenges they have faced, there is an urgent need for implementation in every sphere of life, including cybersecurity. Future work in this direction is the analysis of the various models that have been presented in terms of cyber defense involving AI, BT, and IoT, and the proposal of a new framework, where we will give special emphasis to BT as the hope for secure transfer, unauthorized protection, and transparency above all.

References

[1] Plėta, Tomas & Tvaronavičienė, Manuela & Casa, Silvia & Agafonov, Konstantin. (2020). Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases. Insights into Regional Development. Volume 2. 703-715.

[2] Tyugu, Enn. (2011). Artificial Intelligence in Cyber Defense. 3rd International Conference on Cyber Conflict (ICCC). 3. 1-11.

[3] Wirkuttis, N.; Klein, H. Artificial intelligence in cybersecurity. Cyber Intell. Secur. 2017, 1, 103–119.

[4] González, Ariel & Moreno Espino, Mailyn & Moreno Román, Ariadna Claudia & Pérez, Nayma. (2024). Ethics in Artificial Intelligence: an Approach to Cybersecurity. Inteligencia Artificial. 27. 38-54. 10.4114/intartif.vol27iss73pp38-54.

[5] Sontan, Adewale & Samuel, Segun. (2024). The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities. World Journal of Advanced Research and Reviews. 21. 1720-1736. 10.30574/wjarr.2024.21.2.0607.

[6] A. A. Zainudin, A. Siswanto, and Y. Z. Pratama, “Enhancing IoT Security: A Synergy of Machine Learning, Artificial Intelligence, and Blockchain,” Data Science Insights, vol. 2, no. 1, pp. 9–19, 2024

[7] Alshehri, Mohammed. (2022). Blockchain-assisted cyber security in medical things using artificial intelligence. Electronic Research Archive. 31. 708-728. 10.3934/era.2023035.

[8] Kuzlu, Murat & Fair, Corinne & Güler, Özgür. (2021). Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. Discover Internet of Things. 1. 10.1007/s43926-020-00001-4.

[9] D. Jonas, N. A. Yusuf, and A. R. A. Zahra, “Enhancing Security Frameworks with Artificial Intelligence in Cybersecurity,” Int. Trans. Educ. Technol. (ITEE), vol. 2, no. 1, pp. 83–91, 2023.

[10] Tao, Feng & Akhtar, Muhammad & Jiayuan, Zhang. (2021). The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey. EAI Endorsed Transactions on Creative Technologies. 10.4108/eai.7-7-2021.170285.

[11] Ansari, Meraj Farheen & Dash, Bibhu & Sharma, Pawankumar & Yathiraju, Nikhitha. (2022). The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review. IJARCCE. 11. 81-90. 10.17148/IJARCCE.2022.11912.

[12] A. Rustemi, F. Dalipi, V. Atanasovski and A. Risteski, "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," in IEEE Access, vol. 11, pp. 64679-64696, 2023, doi: 10.1109/ACCESS.2023.3289598.

[13] Mattos, D.M.F., Krief, F. & Rueda, S.J. Blockchain and artificial intelligence for network security. Ann. Telecommun. 75, 101–102 (2020). https://doi.org/10.1007/s12243-020-00754-7

[14] Rafy, Md. Fazley. (2024). Artificial Intelligence in Cyber Security. 10.13140/RG.2.2.19552.66561.

[15] Thwaini MH. Anomaly Detection in Network Traffic using Machine Learning for Early Threat Detection. Data and Metadata. 2022;1:34. https://doi.org/10.56294/dm202272

[16] Rustemi, A., Dalipi, F., Atanasovski, V. et al. DIAR: a blockchain-based system for generation and verification of academic diplomas. Discov Appl Sci 6, 297 (2024). https://doi.org/10.1007/s42452-024-05984-1

[17] Salem, Aya & Azzam, Safaa & Emam, O. & Abohany, Amr. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. Journal of Big Data. 11. 10.1186/s40537-024-00957-y.
[18] Ejjami, Rachid. (2024). Enhancing Cybersecurity through Artificial Intelligence: Techniques, Applications, and Future Perspectives. Journal of Next-Generation Research 5 0. 1. 10.70792/jngr5.0.v1i1.5.
[19] Salman, Tara & Zolanvari, Maede & Erbad, Aiman & Jain, Raj & Samaka, Mohammed. (2018). Security Services Using Blockchains: A State of the Art Survey. IEEE Communications Surveys & Tutorials. PP. 1-1. 10.1109/COMST.2018.2863956.
[20] Taylor, Paul & Dargahi, Tooska & Dehghantanha, Ali & Parizi, Reza & Choo, Kim-Kwang Raymond. (2019). A systematic literature review of blockchain cyber security. Digital Communications and Networks. 6. 10.1016/j.dcan.2019.01.005.
[21] A. Rustemi, F. Dalipi, V. Atanasovski and A. Risteski, "Enhancing Academic Credentials: The Synergy of Blockchain and Artificial Intelligence," 2024 7th International Balkan Conference on Communications and Networking (BalkanCom), Ljubljana, Slovenia, 2024, pp. 206-211, doi: 10.1109/BalkanCom61808.2024.10557185.