НАУЧНИ ТРУДОВЕ НА УНСС (3) 2024, ИК – УНСС
ISSN (online): 2534-8957; ISSN (print): 0861-9344; http://unwe-research-papers.org/
DOI: https://doi.org/10.37075/RP.2024.3.08

ARTIFICIAL INTELLIGENCE APPLICATIONS FOR CONFRONTING CYBERSECURITY ISSUES

Iskren Tairov[1]
e-mail: i.tairov@uni-svishtov.bg

Abstract

Due to the absence of technological advancements, it is impossible to handle the operations that regulate the multifaceted nature of knowledge for effective security on the Internet. It is difficult and complex to assemble the technology needed to efficiently and effectively defend against security threats. These challenges can be overcome by utilizing machine learning and artificial intelligence (AI) techniques. This study provides a brief overview of the applications of AI for cybersecurity via smart technologies and an assessment of the prospects for expanding protection capabilities through improved defense mechanisms. The main findings show that there are presently created AI tools that are successful in protecting data. To begin with, there are neural networks, mainly intended for shielding the outermost layer. Multiple methods using AI to resolve specific safety issues are getting traction with them. On a strategic level, however, one of the outstanding cybersecurity issues is the selection of effective protection technologies

Keywords: Artificial intelligence, cybersecurity, neural networks, expert systems

JEL: C80

Introduction

Information and communication technologies have permeated modern society and have become the foundation of all activities in the economy, government, society, and personal life. Digital infrastructures have evolved from a supportive environment to a fundamental and critical factor in the management and normal operation of all national resources and systems, the development of a competitive and innovative economy, transparent governance, and a modern democratic civil society. Simultaneously, the growing and irreversible digital dependence on society's primary functions and activities creates new substantial risks and threats. As a result, achieving a sufficiently high degree of cybersecurity is critical for the reliable and efficient operation of these activities. This is particularly noticeable in the so-called "critical infrastructures" that provide vital economic and social functions. On the other hand, in parallel with the positive phenomena of the information society, its negative antipode – global cybercrime – emerged and

[1] Head Assist. Prof., PhD, Department of Business Informatics, Faculty of Management and Marketing, Dimitar Tsenov Academy of Economics, ORCID: 0000-0002-2971-5451

quickly expanded globally. Most analysts believe it is now in its fifth generation, which is distinguished by automation of attack tool creation and distribution, as well as integration within several toolkits that perform various functions.

The complexity of determining the source of impact, goals and motives, the rapid escalation of the threat and difficult-to-predict prospects for development, the complexity and intensity of modern communication and information processes, the dynamics of logical and physical connections, and the uncertainty of processes make risks and threats in cyberspace difficult to define. The most severe destructive effects are those of a hybrid nature – a combination of a cyberattack and a physical attack, a cyberattack targeting a critical kinetic process, a cyberattack during a natural catastrophe, or a critical system malfunction. Because of cyberspace's connectivity and reliance, a security breach or defect in one communication and information system in one sector can cause a cascading effect and failure in others, with serious potential repercussions and damage to vital services. Response to such incidents necessitates coordinated actions and preventive steps to reduce the possibility of crises, as well as sufficient follow-up actions to lead to the timely restoration of system normalcy.

Experience has shown that smart technologies can effectively deal with defense against advanced cyber systems, regardless of the development of ransomware and digital weapons in the two years preceding this one (Seker, 2019). Methods based on AI and knowledge-intensive tools can be critical in defeating innovative techniques for an attack like automatically launching private boundaries and throughout its entirety emergency management (Ahmad, 2009), entirely autonomous attacks on network replies, and others (Bai, 2006).

Therefore, in an environment of ongoing assaults and boosting online warfare, the utilization of smartphones and tablets has grown substantially, especially because of the importance of immediate reaction online – where a great deal of data must be controlled at a considerable rate to clarify cyberspace actions and make the correct choices. In the lack of technological advances, users are unable to successfully and quickly deal with activities and the huge amount of data that has to be utilized. It should be noted, however, that developing devices with typical, fixed logical decision-making algorithms to effectively defend against hacking attempts is hard, as novel obstacles arise all the time (Bitter, 2012).

The object of research is ensuring a high level of cyber security with the use of advanced technologies such as AI.

The subject of the research is AI technologies that can be used in countering cyberattacks.

The study's objective is to demonstrate AI solutions for cybersecurity, which have several essential advantages.

Analysis

We focused our research on the application of artificial intelligence in cybersecurity on the technology‘s capacity to address security concerns, as well as the mindset and attitude toward the prospective use of AI in this field.

a) Artificial intelligence's ability to solve problems with cybersecurity

With today's proliferation of information-access devices and constantly evolving cyberattacks, machine learning and AI can be used to automate threat discovery as they react more effectively than traditional human-driven approaches or software. AI offers much-needed analytics and identifies threats to reduce the risk of breach and improve security. In security, AI can instantly identify and prioritize risk, yes spot malware on a network, target incident response, and yes identify potential breakthroughs before they occur.

At the same time, providing cybersecurity poses a significant task to businesses. This is caused by the following:

- large arrays of data;
- big systems are becoming more open and use huge data sets from public networks and platforms that can hardly be tracked and filtered;
- networks growth and the deployment of company systems on the Internet opens a huge front to attack potential evildoers;
- a severe shortage of qualified people security specialists;
- the enormous tension in the workplace can result in a security breach.

As a result, a self-learning, AI-based cybersecurity management system should be able to address many of these issues. There are machine-learning technologies of self-learning systems for continuous and autonomous data collection from data-generating devices and information systems. In the event of a potential attack, models of operation and reaction are developed. As a consequence, new cybersecurity management capabilities have emerged.

Most businesses' platforms for ensuring cybersecurity employ AI-powered tools to observe and evaluate data to provide real-time risk predictions based on vulnerability management and proactive security breach control. Corporate and business companies are currently using AI technologies as AI is capable of preserving resources and time by sifting through standardized data and thoroughly comprehending unstructured data, values, phrases, and statements. Since it is manipulated by people, machine learning can be beaten as it only functions in the way it has been designed (Hosseini, 2012). As attackers adjust to AI platforms, engineers will develop new arguments for the defense, making it a continuous process, however, AI has been demonstrated to be having a beneficial bolstering effect in the battle to protect datasets (Tyugu, 2007).

Even though AI absorbs plenty of assets the technology could prove to serve as a powerful instrument in the digital arsenal of attackers that employ innovation to launch more successful and effective hacking attempts (Kotkas, 2013).

b) Organizations' views toward the application of Artificial intelligence

To investigate attitudes towards AI for its application in cybersecurity, the Capgemini Research Institute conducted a survey of over 850 executives in 10 countries (Das, 2021). According to sources, businesses need to create an A-level cybersecurity defense as cybercriminals are turning to technological advances to carry out assaults. The following are some of the report's other key assertions:

- as stated by 75% of those surveyed, AI allows the company to react to breaches faster;
- 69% believe intelligent technology is necessary;
- 60% are convinced that applying AI increases the accuracy and efficiency of security professionals. AI could boost safety possibilities, and security solutions may aid in rebuilding the route for creating fresh ideas (Das, 2021).

As communications networks grow and get increasingly complicated, AI is going to give an important increase to company defenses. Clearly stated, the rising intricate nature of systems exceeds the abilities of people.

c) Artificial intelligence application in cybersecurity

It will take time for AI tools to work well together with present information security connections. This, as one might assume, demands work planning, directions, and arranging to guarantee that initiatives and personnel achieve the most effective utilization of it (Tyugu, 2011). In a variety of methods, AI systems may ensure the endurance of defense procedures. Creation of sensor login credentials-based precision authentication passcodes; identifying threats and unusual behaviour using forecast algorithms; enhanced reasoning and comprehension with spoken language synthesis and authentication and conjunction according to criteria are some examples.

Following integrating AI into security measures for information infrastructure, IT and managerial staff have to figure out the way to do this successfully, which requires patience and preparation.

Self-learning machine learning methods are accessible for the ongoing and autonomous collection of knowledge from data-generating devices and information systems. In the case of a prospective attack, models of operation and reaction are developed. As a result, new capabilities for cybersecurity management are created, such as:

- inventory of IT assets – receiving complete and accurate information for all devices, users, and applications having access to information systems. In the process of taking inventory, the classification and assessment of business criticality are also very important;

- predicting a threat's potential exposure. AI-based cybersecurity systems can offer current information on regional and sector-specific threats to assist in prioritizing the use of defense mechanisms based not only on what can be used to attack the particular organization but also on what is likely to be used for attack;
- the potency of the control systems. It's critical to evaluate the effects of the different security technologies and security procedures. AI can assist in identifying the individual information protection's strengths and weaknesses;
- inventive risk prediction. AI-based systems can forecast how and where a breakthrough is most likely to occur based on the inventory of IT assets, the exposure of threats, and the effectiveness of controls, allowing for the planned allocation of resources and tools to vulnerable areas in defense;
- reacting to situations as they happen. AI-powered systems may prioritize security breach warnings, respond to incidents quickly, and identify the underlying causes of breaches to reduce vulnerabilities and, yes, avert future issues;
- ability to explain. The ability of recommendations to be explained to employees at all levels and behaviour analysis are critical components of employing AI to enhance cybersecurity in company management systems. This is crucial for top management to have a deeper knowledge of potential risks and to respond appropriately to any threats.

Leading industry innovators are at present using AI defense solutions (Rajani, 2020). Despite there are numerous advantages when utilizing AI in protection, there are also dangers to be aware of. One of the main obstacles to applying AI in protection is that it requires more time and resources for execution than typical non-AI safety procedures.

This is owing, in part, to the high cost of AI-based information protection technologies. However, new security-as-a-service solutions are becoming available, lowering the expense of AI cyberdefense systems for organizations.

d) Tackling risks induced through Artificial intelligence defense technologies

The use of AI in cybersecurity generates novel obstacles for safeguarding assets. Whereas AI solutions help detect and prevent infections by malware, cybercriminals can additionally utilize AI techniques to carry out intricate psychological attacks. Access to modern AI tools and machine learning strategies is growing, thanks in part to reduced generation and execution costs (Rosenblatt, n.d.). The result guarantees that technological criminals can create more complicated and efficient harmful programs at ever-increasingly low costs.

Methodology

This study makes use of scientific and expert breakthroughs concerning the use of AI in cybersecurity which involves threat intelligence, anomaly detection, and automation of cybersecurity-related tasks. Criteria were created during the design selection process to eliminate unsuitable concepts. These criteria are illustrated in Table 1 and include the choice procedure of credible studies and articles published in the Google Scholar and Science Direct databases under the keywords artificial intelligence and cybersecurity. Some of the materials chosen are based on empirical study, but the majority are literature surveys of available scientific works.

Furthermore, due to the complexity of the topic, as well as the development and progress and the attitude toward AI over time, the selected research includes concepts, statements and studies from different eras. Content analysis is utilized as a scientific study method in examining the outcomes.

Table 1: Research inclusion criteria

Included	Excluded
Studies that focus on the Impact of AI on Cyber Security	Studies that do not focus on the Impact of AI on Cyber Security
Literature published in English only	Non-English written articles
Peer-reviewed journal articles, Books and conference proceedings whose content appears in any of the following database sources: Google Scholar and Science Direct	Non-peer-reviewed literature source
Literature sources published between 2018 and 2023	Studies published before 2018. Several studies conducted before 2018 were included since they were critical to the conclusions obtained.

Source: Author's elaboration

Results

The literature search and review yielded a total of 18 articles suitable for detailed synthesis by the study objectives. Figure 1 depicts the breakdown of the synthesised publications, highlighting that the majority of the synthesised sources were 9 journal articles, 4 conference papers and 5 books, indicating that peer-reviewed sources were used to derive specific results in this research.

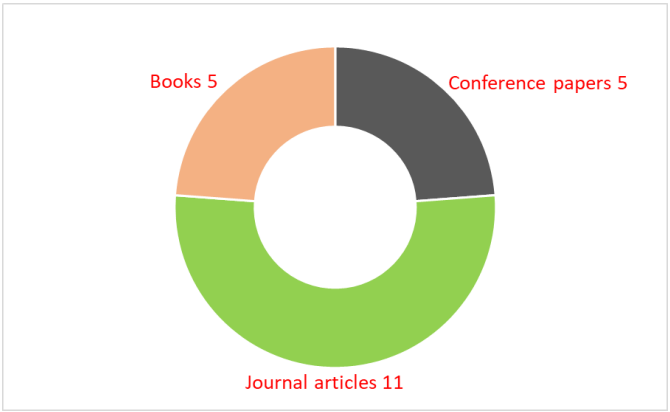

Figure 1: Structure of publications synthesized

The results of the performed research show several prospects and perspectives for the use of established artificial intelligence technologies in the sector of cyber security.

Reviewing the works on AI solutions for cybersecurity reveals that this area now has numerous essential advantages and application potential (Aarthi). We take into account some of them.

a) Neural networks

Neural networks can perform simultaneous dispersed instruction and choice-making. Their functioning speed is their primary noticeable characteristic. They are excellent for pattern recognition, clustering, threat reaction compilation, and other similar tasks. Neural nets are frequently found in both software and hardware. Monitoring and prevention methods may assist neural networks (Venkatesh, 2017). Protocols for denial of service, program infection recognition, spam prevention, ghost verification, evaluation of malware, and evidence have been developed (Venkatesh, 2017).

Deep learning is presently popular in IT safety because of its instant versatility, the way it can be utilized in advances in technology, or how well it is used in visual hardware (Bhandari, 2023). The most recent advancement in neural networks is the latest version of cognitive systems – rapid machine learning, which generates artificial nerve cells with greater precision and offers a broader range of opportunities. Field gate arrays are an excellent way to rapidly construct and modify neural networks while preventing disturbances so they have tremendous promise.

b) Expert systems

Particular applications are with no question the most widely utilized AI methods. An expert system is a piece of equipment that answers concerns presented by an end user or a person with expertise. Optimization methods are used to handle complex problems with multiple parameters, ranging from modest empirical tests to extremely complex combination structures.

The skill set of the credentials' database of information includes a detailed examination of a particular application domain (Wu, 2009). The development of an advanced system requires the selection and modification of an AI shell, in addition to the collection of professional knowledge and the supply of instruction. The following phase is far more challenging and time-consuming compared to the initial one. There are numerous approaches to creating intelligent technologies. In general, the equipment has an intelligent layer and may supplement the knowledge repository with functional comprehension.

In expert systems, there are multiple kinds of depictions, among which the most prevalent of which is the moderator's analysis. For example, AI may introduce new features to frameworks. However, the significance of the basic structure is determined mainly by the unity of the information in the set of abilities of the main system, instead of by the regional character of the expertise classification. Cyber Security Device Specialist is a qualified cybersecurity instruction system which allows significant collection and education of safety efforts to maximize optimal utilization of limited assets.

c) Intelligent agents

Intelligent agents are computer programs that can set up, arrange, and assess data (Kott, 2018). They are regarded as objects in the application programming industry that at least explicitly use an agent's system interface (Panimalar, 2018). Subjects, unlike agents, can be inert and lack interactive comprehension.

Intelligent distributed denial of service (DDoS) defense agents have been implemented, and models of collaborating agents effectively safeguarding from DDoS attacks have been detailed. This will include technological advances to guarantee the flexibility and connectedness of security workers who need to be untraceable from enemies. However, by utilizing extra search guidance expertise, task productivity can be substantially enhanced. Nearly every smart system makes use of a kind of search, and the caliber of the inquiry can often be essential to the system's functionality.

d) Intelligent search methods for solving problems

A wide range of methods for searching are being designed to focus in-depth on specific search-related issues (Sriram, 1997). While numerous AI search techniques are being created and are widely used in an array of applications, they are not commonly utilized as AI. To begin, search has been integrated into the software and is not considered an AI function. In this regard, computational

processing has mainly been used to address ideal privacy issues. Possibly a large number of choices can be ignored, greatly speeding up the search.

e) Learning

Learning and training improve the data framework by developing, restructuring, or enhancing the expertise foundation. The following represents just one of many significant AI topics to learn. Computerized approaches for acquiring new concepts, abilities and creative methods of integrating existing information are required (Chio, 2018). Learning difficulties vary from fundamental quantitative learning to more advanced types of conceptual understanding.

AI can perform both guided and autonomous learning. When dealing with large amounts of information, this section is particularly helpful. It is also extensively used in digital safety, where large records of activity can be gathered. Initially, unsupervised AI learning was used to extract important information from data using various approaches. In general, unsupervised learning may be a consequence of autonomous neural networks. As a production generated in concurrent hardware, simultaneous neural networks, a separate class of learning techniques, are used. These approaches to learning are defined by genetic algorithms and neural networks. For example, in the aforementioned threat detection techniques, genetic data was used alongside neural networks.

All of the listed applications and technology indicate how artificial intelligence can be successfully employed to tackle modern cyber threats (Dawson, 2021), which achieves this study's objective. The successful deployment of these technologies necessitates a thorough examination and assessment of the possibilities and conditions surrounding their unique application (Tetaly, 2022).

Future research directions

Whenever examining the possibilities of AI research, development, and implementation in the area of cybersecurity, a user must differentiate between immediate and distant goals. A lot of AI precautions are fast to be put into effect, and challenging concerns like security necessitate higher-level approaches than are presently accessible. So far, these contemporary instantaneous tools have been discussed. It could be stimulating in the future to introduce completely new ideas of processing data in predicament control and making choices. Knowledge control is a challenging scientific field to grasp in network core operations. Simply using automated administration of data may executives and lawmakers to generate rapid evaluations of the circumstances, giving them the ability to take control at any time.

Individuals may not be capable of depending solely on limited AI for at least a few decades, given the potential horizon. Certain experts consider that the main

objective of AI – intelligent consciousness or AI creation – will be achieved by the turn of the last century, but it remains for the next decades of the 21st century.

Further research will be aimed at detailing the results of artificial intelligence applications used for cybersecurity by region and the stability of the regional security system.

Conclusion

Today's AI systems are programmed to complete a specific job. A fraud detection system cannot operate a vehicle or provide legal guidance. In reality, the AI system that detects healthcare fraud is incapable of detecting tax or warranty fraud. To put it another way, these technologies are extremely specialized. They are oblivious to their surroundings and act inhumanely.

Similarly, self-learning algorithms are not autonomous. The AI systems depicted in movies and television are still science fiction. However, computers that can analyze complex data to learn and perfect specific tasks are becoming more prevalent.

In a world where criminal activity and online dangers are multiplying at an unsustainable pace, advanced digital safety measures must not be ignored. Furthermore, experience has shown that with an intelligent strategy, massive threat protection may be accomplished with a limited number of assets. Research on artificial neural networks, based on publication reviews, provides the most relevant AI results for cybersecurity so they are still being used in the protection of computers.

In numerous fields where neural networks are not the most effective solution, enhanced safety measures remain urgently required. Decision aid, contextual awareness, and data management are examples of such fields. The most fascinating aspect of this situation is the advancement of expert algorithms.

Although it is uncertain what speed general AI will develop, criminal abusers can profit via novel forms of AI as long as they are accessible. This is far from obvious. Furthermore, advances in information comprehension, interpretation, and leadership, especially in the area of machine learning, would significantly enhance the system's safeguarding powers.

Acknowledgement

This research was funded by The Bulgarian National Science Fund at the Bulgarian Ministry of Education and Science, Funding Competition for financial support for projects of junior researchers and postdocs – 2022, Project title: "Artificial intelligence in the economic perspective", Administrative contract: No. КП-06-М65/2 from 12.12.2022.

References

Aarthi, J. (n.d.). Design Of Advanced Encryption Standard (AES) Based Rijindael Algorithm.

Ahmad, I. A. (2009). Application of artificial neural network, Application of artificial neural network, pp. 229-234.

Bhandari, G.m Lyth, A., Shalaginov, A., Gronli, T, -M. (2023). Distributed deep neural-network-based middleware for cyber-attack detection in smart IoT ecosystem: A novel framework and performance evaluation approach, Electronics, 12(2).

Bai, J. W. (2006). A Novel Intrusion Detection Model Based on Multi-layer Self-Organizing Maps and Principal Component Analysis, 3973 LNCS, pp. 255-260.

Bitter, C. N. (2012). An introduction to the use of neural networks for network intrusion detection, Studies in Computational Intelligence, pp. 5-24.

Chio, C. F. (2018). Machine learning and security, Octal Publishing.

Das, R. S. (2021). Artificial Intelligence in Cyber Security, Journal of Physics: Conference Series.

Dawson, M. (2021). Cybersecurity impacts for artificial intelligence use within industry 4.0, Scientific Bulletin, 26(1), pp. 24-31.

Hosseini, R. Q. (2012). An automatic approach for learning and tuning gaussian interval type-2 fuzzy membership functions applied to lung CAD classification system, IEEE Transactions on Fuzzy Systems, pp. 224-234.

Kotkas, V. P. (2013). A model-based software technology proposal, Proceedings of the 1st International Conference on Model-Driven Engineering and Software Development, pp. 312-315.

Kott, A. (2018). Intelligent Autonomous Agents are Key to Cyber Defense of the Future Army Networks, The Cyber Defense Review journal.

Panimalar, A. P. (2018). Artificial intelligence techniques for cybersecurity, International Research Journal of Engineering and Technology (IRJET), pp.122-124.

Rajani, P. A. (2020). Artificial Intelligence: The New Age, pp. 1398-1403.

Rosenblatt, F. (n.d.). The Perceptron – A Perceiving and Recognizing Automaton, Cornell Aeronautical Laboratory, pp. 460-461.

Seker, E. (2019). Use of Artificial Intelligence Techniques / Applications in Cyber Defense.

Sriram, R. D. (1997). Problem Solving: Introduction to Search Methods, In: Intelligent Systems for Engineering, London: Springer.

Tetaly, M. & Kulkarni, P. (2022). Artificial intelligence in cyber security – a threat or a solution.

Tyugu, E. (2007). Algorithms and Architectures of Artificial Intelligence, IOS Press.

Tyugu, E. (2011). Artificial intelligence in cyber defense, International conference in cyber conflict, Tallinn.

Venkatesh, G. K. (2017). HTTP Botnet Detection Using Adaptive Learning Rate Multilayer Feed-Forward Neural Network To cite this version: HAL Id: hal-01534315 HTTP Botnet Detection Using Adaptive Learning Rate Multilayer Feed-forward Neural Network.

Wu, C. H. (2009). Behaviour-based spam detection using a hybrid method of rule-based techniques and neural networks, Expert Systems with Applications, pp. 4321-4330.