APPLICATION OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

Burkhonov Karomatillo,
Tashkent University of Information Technolgies, Tashkent, Uzbekistan

ABSTRACT

Artificial intelligence (AI) has emerged as the most widely applicable field across varied industries. Being an evolving technology, it may be quite useful in sensitive areas such as cyber security where there is a dire need for implementation of AI technologies, such as expert systems, neural networks, intelligent agents, and artificial immune systems. The primary reason for AI fitment to cyber security area is its ability to detect anomalies proactively and predictively in the network, thereby working towards securing the network before the damage related to loss of data and/or reputation is done. There are different types of AI technologies as mentioned above that could be applied in cyber security in its varied forms. In this paper, the emphasis is on specific AI technologies that can bring unique benefits to the cyber security field with its unique applicability to different scenarios. The outcome of this study shows that AI technologies such as expert systems, neural networks, intelligent agents, and artificial immune systems are transforming the landscape for managing cyber threats.

Keywords Artificial Immune System, Artificial Intelligence, Cyber Risks, Cyber Security, Cyber-attacks, Cyberspace, Expert Systems, Intelligent Agent, Machine Learning, Neural Networks

INTRODUCTION

The article highlights the significance of Artificial Intelligence (AI) in cybersecurity and its broader applications across various industries. It elucidates that AI encompasses technologies like expert systems, machine learning, deep learning, neural networks, artificial immune systems, and intelligent agents, aiming to imitate human intelligence and facilitate self-learning capabilities.

Corporate concerns center around guarding against potential anomalies and cyber-attacks, necessitating a comprehensive understanding of vulnerabilities to prioritize defense strategies. The surge in cyber-attacks has spurred the need for proactive handling and predictive resolution, leveraging AI's evolving capabilities.

This article aims to explore how AI, including various tools and technologies, can transform cybersecurity practices. Traditional reactive approaches to managing cyber risks, such as incident detection and response, are considered insufficient in the face of sophisticated network attacks. The integration of AI technologies like expert systems, artificial neural networks, intelligent agents, and artificial immune systems is pivotal in enabling proactive risk management and predictive protection. It outlines four categories - Early Warning/Prevent, Detect, Reach, and Response - where AI techniques are applied to address security issues, showcasing the potential of diverse AI branches within an integrated security approach.

The article highlights the widespread adoption of AI in cybersecurity across research and corporate sectors, aiming to mitigate cyber risks using AI as an emerging and disruptive technology. It emphasizes studying the impact of AI technologies on the cyber risk management landscape and their handling, encompassing various AI tools such as expert systems, neural networks, intelligent agents, and artificial immune systems.

RESEARCH OBJECTIVES

In light of the research questions mentioned above, the following research objectives can be derived (also figuratively demonstrated below in Figure 1):

1. To understand causes of the knowledge acquisition problem impact on expert systems in decision- making or problem-solving to improve the management of cyberattacks.
2. To explore how cyberattacks can be prevented proactively using AI neural networks to prevent malicious unknown intrusions.
3. To ascertain the role and capability of Intelligent agents as cyber police to monitor the networks and fight against Distributed Denial of Service (DDoS).
4. To recognise the value of artificial immune systems in understanding the changing patterns and detecting anomalies proactively, leading to mitigation of cyber risks.

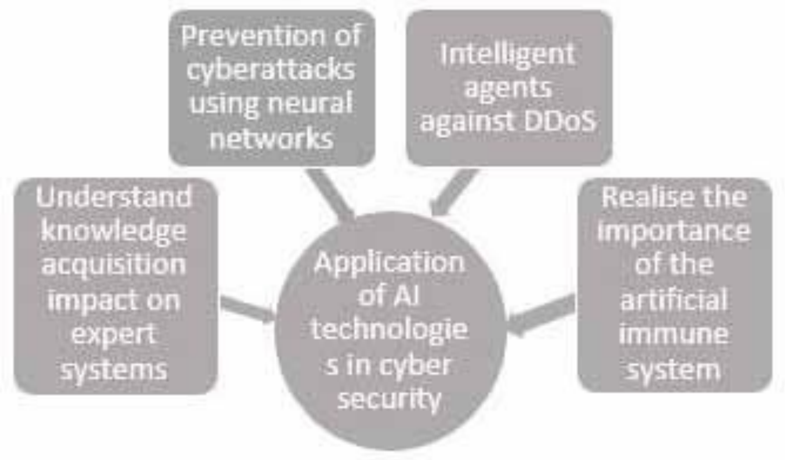
Prevention of cyberattacks using neural networks
Intelligent agents against DDoS
Understand knowledge acquisition impact on expert systems
Application of AI technologie s in cyber security
Realise the importance of the artificial immune system

Fig 1. Objectives – application of AI technologies in cyber security

Expert Systems

Expert systems are rule-based AI tools used extensively by security professionals for decision support in cybersecurity. They serve in various industries for decision-making tasks, especially in network intrusion detection. These systems consist of a knowledge base housing domain-specific information, an inference engine, and additional data to generate solutions. Developing an expert system involves selecting a suitable system shell, inputting expert knowledge, and ensuring the accuracy of the knowledge base, a more challenging and time-consuming task (Şeker, 2019).

For detecting network anomalies and intrusions, expert systems rely on a knowledge base containing rule sets and configurations. These rule sets, stored in a linked knowledge base database, help identify intrusion behaviors from real-time data packets. The effectiveness of expert systems heavily relies on the quality of input data. Poor-quality input impacts the system's output, emphasizing the importance of acquiring high-quality knowledge for practical application (Anwar & Hassan, 2017).

In essence, expert systems are critical for decision-making in cybersecurity but depend significantly on the quality of the knowledge base. Developing real-world applications requires addressing the "knowledge acquisition problem" to ensure effective solutions.

Neural Network

The use of Intrusion Detection Systems (IDS) in modern corporate networks has evolved from traditional pattern-based approaches to incorporating various methods like anomaly detection and machine learning for threat identification and classification (Pierazzi et al., 2017). Artificial Neural Networks (ANNs) play a vital role in proactive threat detection by analyzing patterns, distinguishing between normal and abnormal network behavior, and enabling early warning systems for both LAN and WAN, including widely used protocols like FTP, SMTP, HTTP, and newer ones like SOAP (Şeker, 2019).

ANNs, mimicking human brain neural networks, fall into shallow learning (SL) and deep learning (DL) categories, differing mainly in the number of hidden layers they possess. SL requires domain experts to identify relevant data features, while DL autonomously learns representations from input data (Apruzzese et al., 2018).

The advantage of using ANNs in cybersecurity lies in their learning ability. Unlike traditional methods that rely on manually defined patterns, ANNs can automatically identify and learn patterns from historical network data, aiding in the prevention of impending threats (Wirkuttis & Klein, 2017).

Intelligent Agents, software mechanisms with proactive, communicative, and problem-solving abilities, are crucial in managing and combating Distributed Denial of Service (DDoS) attacks. These agents possess planning and adaptability traits, contributing to effective cyber defense (Şeker, 2019). Implementing intelligent agents, possibly as mobile cyber-police units, requires infrastructure deployment ensuring their mobility and communication while safeguarding against attacker access (Anwar & Hassan, 2017).

Structure of intelligent agents Table 1. Developing cyber-police requires the deployment of infrastructure for supporting the automated agents' excellence and communication; however, it should not be accessible for attackers. This may require support from various Internet service providers. Multi-agent software or tools will provide a wide-ranging operational view of the cyber house, for example, a hybrid multi-agent and neural network-based invasion discovery technique have been anticipated. (Patil, 2016).

Table 1 Structure of intelligent agents

Type of Agent	Percepts	Actions	Objectives	Environment
Healthcare diagnosis system	Warning Signs, Outcomes, patient's response	Queries, tests, a patient's treatments	Good patient health, reduce costs	Patient, hospital and its staff
Satellite image analysis system	Pixels of different intensity, colour	Print a classification of a scene	Accurate classification	Pictures from orbiting satellite
Refinery controller	Temperature, pressure measurement	Open, close valves; regulate temperature	Maximise purity, optimise yield, wellbeing	Refinery
Interactive English tutor	Words typed	Print exercise, recommendations, evaluations	Improvement of a student's marks in exams	Number of students

Artificial Immune System

Artificial Immune Systems (AISs) are computer-based mathematical models that have sources from biological immune systems which can adapt in a flexible environment and self-learn. Immune systems are responsible for finding unknown invasions or intruders like various types of bacteria, viruses, et cetera and consequently fight against them. AISs are formed to copy natural immune systems generally in the application of cyber safety, and specifically for Intrusion Detection System (IDS) (Kamtam, Kamar, & Patkar, 2016).[5]

The primary purpose of a biological immune system is to arm the human body to fight against unknown molecules called antigens. The immune system has a wonderful recognition system which can detect changes in patterns and report abnormal behaviours in the system. AIS utilises a machine language which instils the functionality of the biological immune system. In contrast to conventional cyber security approaches, AIS principles have an edge due to their ability to detect attacks internally from the network and prevent them from occurring. The advantage of AIS-based IDS is its use of biologically influenced concepts in computation to stop a network attack by determining malicious patterns even before the attack happens (Song, Kim, Tyagi, & Rajasekaran, 2018).[6]

An IDS applied to the principles of an AIS can provide a resolution to the problems that can occur while securing information. This implementation of an IDS differs from the industry standard of implementing machine learning (Cooper, 2017).

RESEARCH FRAMEWORK

The literature review revealed the four independent variables (Fig 2) that are applied to the dependent variable – cyber security. The impact of such AI technologies on the dependent variable will be further studied. To comprehensively understand the application of independent variables on dependent variable, appropriate studies will be engaged based on secondary research, and then qualitative analysis performed.

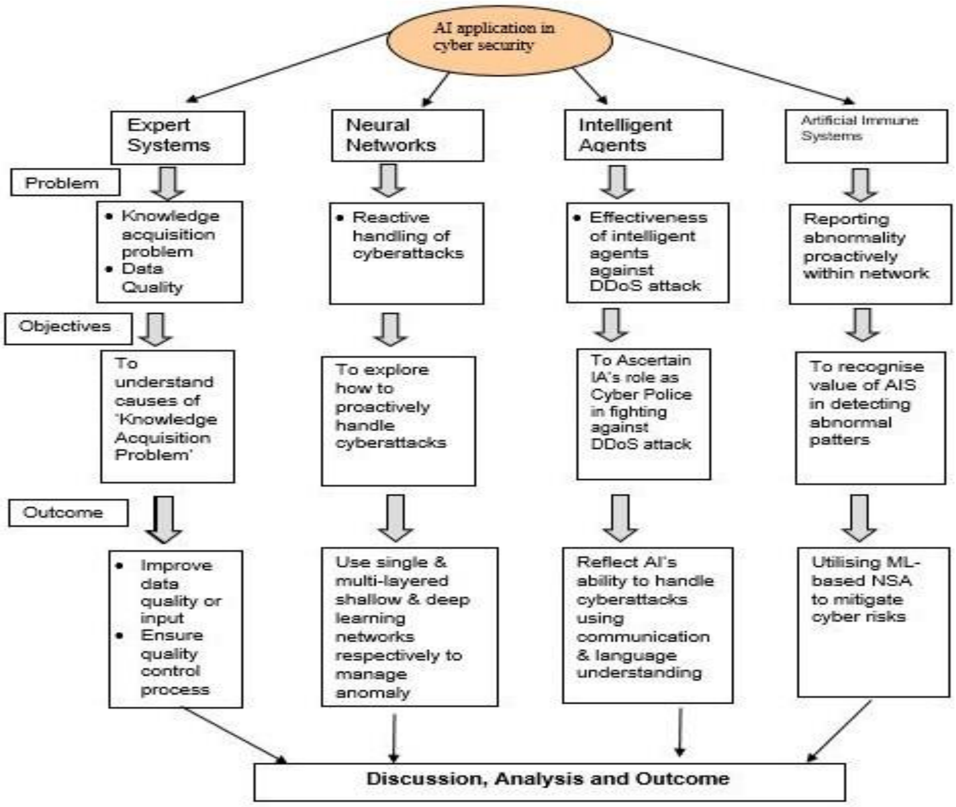
AI application in cyber security
Expert Systems
Neural Networks
Intelligent Agents
Artificial Immune Systems
Problem
• Knowledge acquisition problem
• Data Quality
• Reactive handling of cyberattacks
• Effectiveness of intelligent agents against DDoS attack
Reporting abnormality proactively within network
Objectives
To understand causes of 'Knowledge Acquisition Problem'
To explore how to proactively handle cyberattacks
To Ascertain IA's role as Cyber Police in fighting against DDoS attack
To recognise value of AIS in detecting abnormal patters
Outcome
• Improve data quality or input
• Ensure quality control process
Use single & multi-layered shallow & deep learning networks respectively to manage anomaly
Reflect AI's ability to handle cyberattacks using communication & language understanding
Utilising ML-based NSA to mitigate cyber risks
Discussion, Analysis and Outcome

Fig 2. Research framework showing one dependent variable, four independent variables, problems, objectives and outcome, leading to the 'discussion, analysis and outcome'

DISCUSSION, ANALYSIS AND OUTCOME

This paper aims to improve the current understanding of the application of various AI technologies in cyber security and how these emerging technologies may change the way cyber risks are handled by companies today. An in-depth analysis shall lead to concrete outcomes of the influence of various constructs on the main research topic.[7]

Expert Systems – Analysis and Outcome

As expert systems are the leading and most known applicable AI technology in combating against cyber-attacks, they are considered the primary tool to safeguard a company's network.

An expert system consists of a knowledge base in which expert opinion or knowledge is saved regarding a specific application area. Additionally, it implements an inference engine for leading answers considering current information and enhanced knowledge regarding a situation. An expert system shell consists of a vacant knowledge base and inference engine before the loading of its relevant knowledge. To enter information or data based on facts in the knowledge base software, it must support the expert system shell, and it can be loaded with programs for client support, in addition to varied projects that may be used as a part of hybrid expert system (Anwar & Hassan, 2017).

Figure 3 below demonstrates the concept of an expert system at a very basic level:

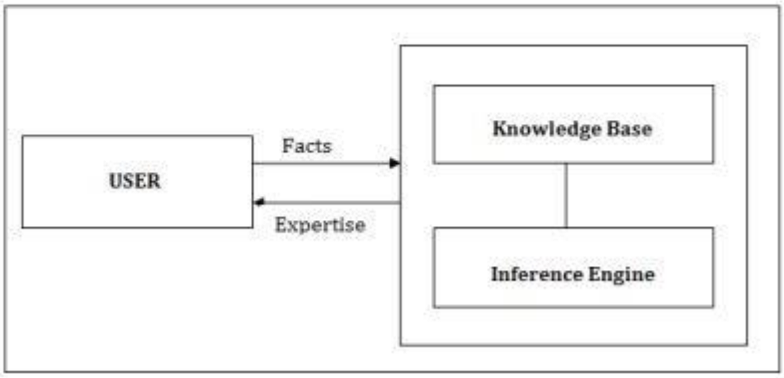

Fig 3. The expert system concept (Nicolau, Augusto, & Schirru, 2017)

Expert systems are categorised as per the view that knowledge is showcased in its knowledge base. The data or knowledge can be shown or presented in many forms, which are usually rules but can also be logic trees and logical frameworks. If the knowledge base is rule-based, its data or knowledge is coded as IF-THEN rules. Otherwise, the same data could be represented via a logic tree model. Hence, the knowledge base model ought to be selected based on the closest illustration to the actual issue or in the most expressive way (Nicolau, Augusto, & Schirru, 2017, June).

The output is only as good as the input. With this in mind, to ensure that knowledge base includes quality data, it is crucial to ensure or implement a quality assurance and control process to verify the accuracy and relevance of data before it goes in the knowledge base. Various quality-oriented models, such as TQM, Deming Cycle and Kaizen, could be applied to improve the quality of data in a knowledge base. Michael Porter's cost leadership strategy is apt as with a smaller number of attacks, the unit cost of products or services of a company would be minimised, leading to a better quality.[8]

Neural Networks – Analysis and Outcome

ANNs are webs of connected processing neurons. Each neuron receives a set of mathematical data input from different areas and based on this data, an outcome or output is formed. The outcome is applied to the situation, otherwise is advanced as input to further network neurons (Demertzis, Iliadis, Avramidis, & El-Kassaby, 2017).

The figure below demonstrates that ANNs have three layers, namely an input layer, hidden layer, and output layer. Figure 4 is a classic example of shallow learning (SL) where there is only one hidden layer. Consecutively, if the neural network model has multiple hidden layers, then it is called Deep Learning (DL).

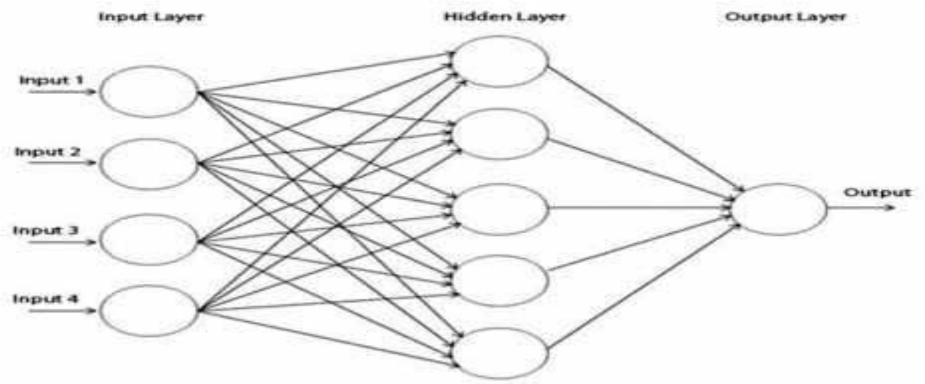

Fig 4. Basic architecture of a typical multilayer feed-forward ANN (Demertzis, Iliadis, Avramidis, & El-Kassaby, 2017)

All deep learning algorithms (also called a set of rules or coded mathematical formulae) are set upon Deep Neural Networks (DNN), which are huge neural networks prearranged in multiple levels meant for representation learning on their own. Deep learning is recognised to outdo shallow learning in a few application areas, for example, computer vision. This may not always be the case for cyber security in which a few better configured SL algorithms might succeed despite the rarity of DL applications regarding SL procedures in this field (Apruzzese, Colajanni, Ferretti, Guido, & Marchetti, 2018).

Thus, both shallow learning and deep learning neural networks proactively have a significant impact on managing cyber security today, though they may have a separate application. However, each one is important and plays a different role in detecting network anomalies. Various shallow and deep learning models can be implemented as per the requirement in managing Cyber threats, including but not limited to Supervised SL Algorithms such as Random Forest, Support Vector Machines and Logistic Regression and Unsupervised SL Algorithms such as Clustering and Association. Similarly, Supervised DL Algorithms include fully connected feedforward deep neural networks (FNNs), convolutional feedforward deep neural networks (CNNs) and recurrent deep neural networks (RNNs), whereas unsupervised dl algorithms include deep belief networks (DBNs) and stacked autoencoders (SAEs). Since all these models fall under a cybernetics model, a cost leadership strategy could be applied here.

Intelligent Agent – Analysis and Outcome

Intelligent agents play a crucial role in cybersecurity due to their communication skills, adaptability, and ability to combat Distributed Denial of Service (DDoS) attacks, which overwhelm websites or networks with excessive traffic.

These agents exhibit traits surpassing standard tools like calculators, possessing a wider range of intelligence. Their functionality involves aspects such as natural speech and data processing, thus qualifying as AI systems (Shankar, 2017).

Intelligent agents utilize two primary modules for anomaly detection in networks. Firstly, they learn from cyberattacks and establish rules based on previous data to identify incoming data that breaks these rules. Secondly, when an alert rule triggers, they conduct comprehensive information analysis to understand the situation and take appropriate actions (Wang & Govindarasu, 2016).

During a DDoS attack, intelligent agents primarily investigate unusually high incoming volumes directed at the targeted application server. If the volume exceeds predefined thresholds, the system immediately identifies an attack (Bawany & Shamsi, 2019).

These intelligent agents encompass various models like learning agents, utility-based agents, goal-based agents, and simple reflex agents, each exhibiting distinct levels of intelligence and capabilities. The application of a cybernetics model, particularly Michael Porter's cost leadership strategy, could be suitable in this context for efficient cyber defense.

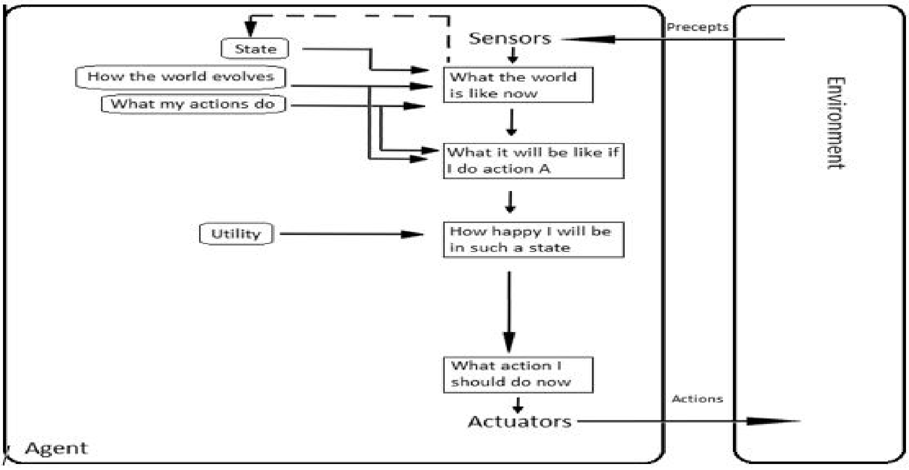
State
How the world evolves
What my actions do
Utility
Sensors
What the world is like now
What it will be like if I do action A
How happy I will be in such a state
What action I should do now
Actuators
Agent
Precepts
Actions
Environment

Fig 5. Utility-based agent model (Source: Wikipedia)

Artificial Immune System – Analysis and Outcome

The negative selection algorithm is a generation algorithm used to create accurate and efficient detectors that distinguish between self and non-self. The components needed in the negative selection algorithm are the threshold, number of detectors, and the number of features. In the human immune system, an antibody is used by the immune system to neutralise pathogens like viruses and bacteria. Similarly, the Artificial Immune System (AIS) detects its version of an antigen, the intrusion, by the negative selection algorithm. The threshold is what determines an intrusion. The artificial body uses the sensory attribute of the negative selection algorithm whereby a specified number of detectors tripped will cause the data record to be classified as an intrusion (Cooper, A. 2017).

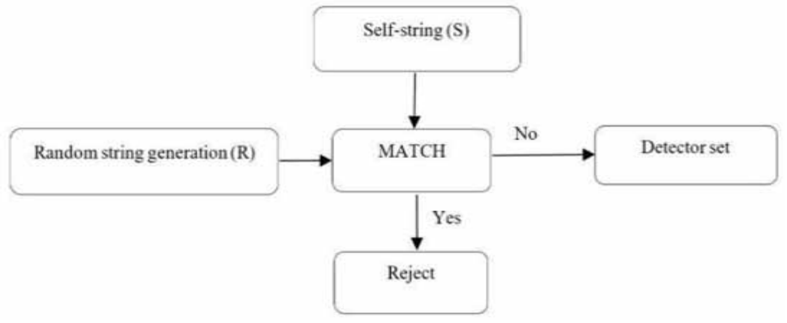

Fig 6. Negative selection algorithm learning model (Sarkohaki, Fotohi, & Ashrafian, 2017)

The concept of Artificial Immune Systems (AIS) draws inspiration from the natural immune system's ability to detect and respond to unknown anomalies in a network. This framework consists of two layers of defense: the innate system, functioning as the initial security layer resembling the natural innate immune system, and the adaptive system, which mirrors the adaptive immune system by incorporating mechanisms similar to T-cells and B-cells. Research indicates that this proposed framework effectively detects invasions or anomalies in a network after introducing malicious occurrences (Dutt, Borah, & Maitra, 2016).

AIS harnesses features from the immune system, such as pattern recognition, feature extraction, learning, and adaptability. It logically remembers and adapts based on experience, continually evolving to achieve higher precision levels (Chen, Chang, & Wu, 2016).

In essence, AIS serves as an intelligent rule-based learning system inspired by the human immune system. Leveraging learning and memory characteristics akin to the immune system, AIS is employed for problem-solving in preventing cyberattacks. The Negative Selection Algorithm is a model commonly researched and applied within this AI technology, particularly for classification and pattern recognition problems.

SCOPE FOR FUTURE RESEARCH

This paper observed how some of the AI technologies, such as expert systems, artificial neural networks, intelligent agents and artificial immune systems, are applied to cyber security, indicating their use cases and clear applications benefitting companies or users. However, a myriad of other technologies within and beyond AI, including but not limited to fuzzy logic control systems, search and optimization, and probabilistic methods for uncertain reasoning, can be explored and applied in the cyber security field or industry. AI application and impact could be studied further in terms of the benefits or limitations this technology could bring. It indeed opens the door to a much broader field of application for further study. Also, there is very little information available on AI handling computer virus attacks, which may be largely due to human intervention. Nevertheless, this remains an area requiring more research.

CONCLUSION

Artificial Intelligence (AI) and cybersecurity complement each other, with expert systems relying on quality knowledge acquisition to tackle cyber threats effectively. Expert systems' success hinges on robust knowledge representation, emphasizing the pivotal role of choosing suitable representation techniques (Muhammad et al., 2018).

Neural networks, notably shallow and deep learning, have significantly advanced cybersecurity by autonomously learning patterns from data, particularly in unsupervised learning. Techniques like Self Organization Maps (SOMs) and Adaptive Resonance Theory (ART) aid in discovering patterns from unlabeled data. Hybrid artificial neural network methods have shown promise as effective intrusion detection systems, considering detection rates, false positives, false negatives, and cost-effectiveness (Hodo et al., 2017).

Intelligent agents, capable of communication and learning independently from historical anomalies, function as cyber police to combat Distributed Denial of Service (DDoS) attacks. These agents enable real-time and distributed DDoS detection, simultaneously identifying and mitigating various sources of attacks (Osei, 2018).

Artificial Immune Systems (AIS), mimicking the human immune system using a Negative Selection Algorithm (NSA), detect unknown intrusions effectively. By leveraging NSA, AIS aim to reduce system training time while maintaining detection accuracy by distinguishing normal and anomaly behaviors (Xu et al., 2019). This method relies on self-patterns called detectors to recognize anomalies (Hosseini & Seilani, 2019).

In conclusion, AI technologies play a significant role in managing cybersecurity tasks. However, caution is necessary, especially in unsupervised learning where systems operate autonomously. The advancement of attackers emphasizes the potential crucial role of AI in the future, demanding a regulatory environment to ensure controlled processes and procedures in AI technologies.

REFERENCES

1. Anwar, A., & Hassan, S. I. (2017). Applying artificial intelligence techniques to prevent cyber assaults.
International Journal of Computational Intelligence Research, *13*(5), 883–889.
2. Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018,

May). On the effectiveness of machine and deep learning for cyber security. In *2018 10th International Conference on Cyber Conflict (CyCon)* (pp. 371–390). IEEE. doi:10.23919/CYCON.2018.8405026

3. Bawany, N. Z., & Shamsi, J. A. (2019). SEAL: SDN based secure and agile framework for protecting smart city applications from DDoS attacks. *Journal of Network and Computer Applications*, *145*, 102381. doi:10.1016/j. jnca.2019.06.001

4. Calderon, R. (2019). *The Benefits of Artificial Intelligence in Cybersecurity*. Economic Crime Forensics Capstones. 36. https://digitalcommons.lasalle.edu/ecf_capstones/36

5. Chen, M. H., Chang, P. C., & Wu, J. L. (2016). A population-based incremental learning approach with artificial immune system for network intrusion detection. *Engineering Applications of Artificial Intelligence*, *51*, 171–181. doi:10.1016/j.engappai.2016.01.020

6. Cooper, A. (2017). *Experiments with Applying Artificial Immune System in Network Attack Detection*. Academic Press.

7. Demertzis, K., Iliadis, L., Avramidis, S., & El-Kassaby, Y. A. (2017). Machine learning use in predicting interior spruce wood density utilising progeny test information. *Neural Computing & Applications*, *28*(3), 505–519. doi:10.1007/s00521-015-2075-9

8. Dutt, I., Borah, S., & Maitra, I. (2016). Intrusion detection system using artificial immune system. *International Journal of Computers and Applications*, *144*(12).