Artificial Intelligence Applications and Techniques in cyber security

Abrar Almukarram, Sara Alabdullatif, Manar Almunyif, Raneem Alqahtani
441051681, 441050270, 441960354, 442051618
Information Systems department, College of computer engineering and science
Prince Sattam bin Abdulaziz University
Al-Kharj, Saudi Arabia

Abstract: The number of cyberattacks has exceeded the business's financial resources and human capacity to analyze and prevent every new type of cyberthreat. A significant amount of personal and financial information needs to be secured from cyberattacks because of the growing digital presence. AI machine learning techniques can be used to manage this issue. The development of Information Technology can make a computer to act like a human AI is an exceptional aspect of IT that requires the event of a machine that reacts and works as a mind of human.

Keywords: Cyber security, Artificial intelligence, cyber-attack

I. INTRODUCTION

Technology is reaching a turning moment in human history. Regardless to how quickly society is capable of absorbing and comprehending information, artificial intelligence is developing at a rapid rate. Recent developments in AI have enhanced computational reasoning capabilities and surpassed human performance in a variety of tasks, including data analytics, image recognition, and natural language processing. These emerging technology have revolutionary uses. Transportation will soon be transformed by autonomous. However, when AI systems are subjected to hostile activity, they are susceptible to manipulation, trickery, and deception that can have significant security ramifications. It is crucial to establish methods and best practices to strengthen them as increasingly crucial systems, such as financial systems, self-driving cars, network monitoring tools, and military applications, use AI. Users now have a means to connect online due to the internet's explosive growth and the technical transformation in the information and communication sectors. Additionally, without significant automation, people are unable to manage the complexity of processes and the volume of data needed to safeguard cyberspace. As it tries to mimic human intelligence, artificial intelligence is becoming more and more relevant in cybersecurity. If properly utilized, AI offers enormous potential in the cybersecurity field. AI systems may be trained to produce threat alerts, spot novel malware strains, and safeguard important information for businesses. In order to effectively identify threats and safeguard their systems and data resources, businesses can also make use of the most recent AI-based techniques.[1] This paper provides a concise overview of AI implementations of various cybersecurity utilizing artificial technologies and assesses the likelihood of strengthening the defense system to increase cybersecurity capabilities.

II. PROBLEM OVERVIEW

The main problem that this paper will try to solve is to examine how cybersecurity uses artificial intelligence. As threats increase and hackers work to elude law enforcement, cybersecurity is a rapidly evolving topic that has made headlines frequently over the past ten years. Individuals cannot manage the complexity of activities and the volume of information needed to secure cyberspace without significant automation. However, it is challenging to develop technology and software with typical fixed implementations to properly protect against security threats. Artificial intelligence techniques for machine learning and simplicity can be used to treat this issue (AI).

III. LITERATURE REVIEW

A new kind of artificial intelligence may still be used by criminals as long as it is available, according to the study conducted by [1]. However, it is impossible to know how quickly general artificial intelligence has improved. This is not immediately apparent. Additionally, systems' cybersecurity capabilities would be greatly enhanced by the most recent developments in the understanding, interpretation, and administration of information, notably in the field of computer learning. Many researchers have recently begun investigating ways that AI may be used to improve cyber-security. The techniques, systems, and human behavior that help to protect electronic resources are referred to as cyber-security. AI has been recognized as a flexible method for analyzing vast amounts of data and detecting erroneous information [4-5]. Similar to this, the study by [6] revealed that AI has emerged as one of the key resources for businesses to enhance their performance in terms of cyber security. The current situation has shown that cyber security is one of the crucial elements that every firm must ensure because there is a potential that enormous amounts of sensitive data and online hackers would steal it. The personal and financial information of businesses is saved on the cloud because of fast globalization and technological advancement, and as a result of this greater reliance on digital technology, cyberattacks have increased in frequency. The study's conclusions showed that, except for the expert system, all independent variables exhibited meaningful and favorable relationships. Taddeo in [7] made the argument that using artificial intelligence to lessen the impact of cyberattacks is a successful strategy. According to the literature, the major goal of the study is to demonstrate how well AI techniques may be used to defend against cybersecurity threats. According to a study

by [8], an intelligent agent is a separate entity of AI that primarily recognizes movement through sensors while paying attention to the actual indications of the environment, such as an agent, and directs its own activity toward the accomplishment of goals. The main purpose of intelligent agents is to defend against distributed denial of service (DDoS) assaults.

IV. Methodology/Approach

To get an all-round impression of the junction between cybersecurity and AI, we used: CiteSeerx, SDL Digital Library, also ScienceDirect. Along with that, We also used the Google Scholar search engine in addition to that. These databases were searched using a set of keywords that corresponded to the topics. Filters were applied to the outcomes of the preceding phase. Because the goal of this work is to highlight the most recent developments in AI in cybersecurity, the search results we received were restricted to only those papers that had been published within the previous few years. On the other hand, recently published studies with less than five citations or references but creative techniques or strategies were also chosen. The resources which meet the succeeding [1] requirements were subsequently accepted:

- Papers whose titles refer to topics that are included in this research report.
- Books, citations, technical report.
- Papers that were not English-language publications.

V. APPLICATIONS OF AI IN CYBERSECURITY

The fields of artificial intelligence and cyber security frequently cross. Cyber-attack detection and prevention have seen an increase in the use of AI tools, including expert systems, computational intelligence, neural networks, intelligent agents, artificial immune systems, machine learning, data mining, pattern recognition, fuzzy logic, heuristics, etc. [2] They can be used to discover how to make it possible for security professionals to comprehend the digital environment to spot anomalies. Artificial intelligence utilization has the potential to expand the capabilities of current cyber security solutions. Companies can use AI in the four areas of automated defense, cognitive security, adversarial training, parallel processing, and dynamic monitoring to improve current cybersecurity systems.

A. Machine Learning Applications in Cyber Security

Given the ongoing evolution of cybersecurity threats, an automatic and immediate response is necessary. In order to apply cybersecurity AI strategies, machine learning techniques—in particular, deep learning—that often do not require prior knowledge or rely on expert classifications from the past—might be especially crucial. The study [10] examined the efficiency of machine learning techniques for cybersecurity. In this study, machine learning techniques were used to detect malware, spam, and intrusions.

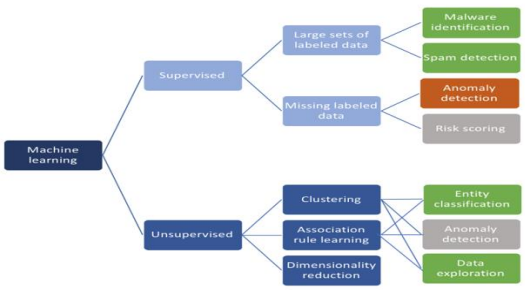

Fig. 1. Machine learning in cyber security

B. Deep Learning Applications in Cybersecurity

The lack of available data is a common issue in cybersecurity research. Even in large firms with extensive internal expertise, experience shows that security information on threats can be converted into a categorised data set suitable for machine learning. This shortfall is frequently explained by its return to secrecy issues.

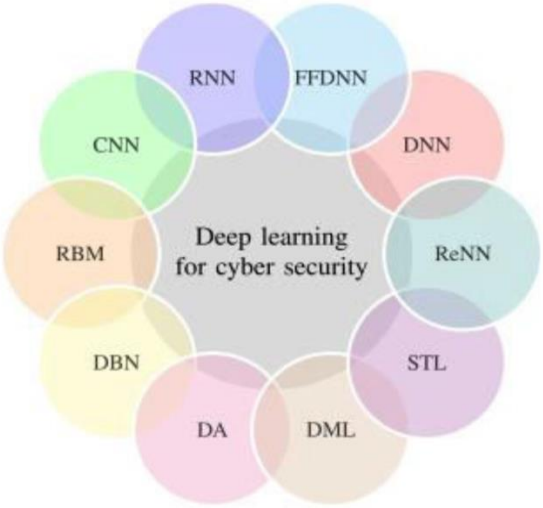

Fig. 2. Deep learning for cyber security

This can be attributed to a number of factors, including the existence of numerous sizable, unbalanced data sets, the lack of time available for manual categorization, and particular characteristics in areas like semantic categorization that widen the gap between technological proficiency and mathematical modeling.

C. Data Mining Applications in Cybersecurity:

Searching for significant patterns and trends in huge databases is known as data mining. The technique of data mining helps to collect useful knowledge and identify hidden patterns from a large number of datasets that cannot be discovered through computational approaches. It is a large research field that involves machine learning, databases, analytics, expert systems, visualisation etc.

VI. AI TECHNIQUES USED FOR CYBER SECURITY

To handle problems that require intelligence from a human perspective, a vast array of techniques have been developed in the field of artificial intelligence. Based on the current procedures, several of these methods have created and precise stages. These techniques are well-known in fields of application like data mining, which emerged from an area of artificial intelligence. The methods and architectures have been divided into several categories, including machine learning, neural networks, intelligent agents, data mining and constraint solving, expert systems, and search. As a result, an overview of this kind may not provide a comprehensive analysis of all practically useful artificial intelligence techniques. We outline these divides and give examples of how the individual approach has been used in cyber security.

A. Artificial Neural Networks (ANN)

Frank Rosenblatt first developed the ANN as a perception in 1957. The ANN is a statistical learning model that mimics the anatomical and functional activity of the human brain. In a variety of challenging domains, ANN can learn and find solutions. By fusing with various neurons, it may handle absorption concerns and learn from

facts in any domain. ANNs have been utilized in the early warning phase, prevention phase, detection phase, and reactive/response phase of the integrated security strategy, which is a comprehensive classification of the cyber defense framework. When ANN is used in conjunction with cyber security, it can be utilized to monitor network traffic, allowing for the early detection of harmful incursions and eventual perimeter defense against cyber-attacks. In order to prevent future attacks, ANN can learn from prior network activities and assaults. When deep learning (DL), an advanced ANN technique, is used in cyber security, the system can autonomously identify both lawful and questionable files. Compared to the traditional approaches used in cyber defense, this method produces superior results when it comes to spotting threats. Figure 1 below shows an ANN in its general form

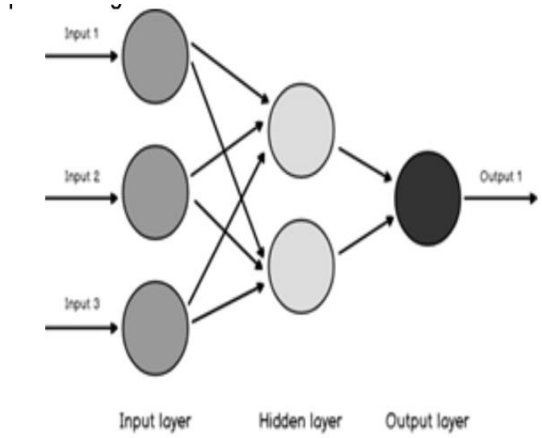

Fig. 3. Artificial Neural Network

The key benefits of ANN over manual approaches employed by seasoned security specialists are its ability to spot patterns in extremely non-linear issues and its quick classification times. Using previously transmitted data via the network, artificial neural networks are capable of automatically identifying normal and problematic network patterns. In order to scan network traffic, ANNs are used by network security technologies including firewalls, network hubs, and intrusion detection systems. Deep neural network (DNN), also known as deep learning, is a more sophisticated type of ANN with a high cost of computation. It has demonstrated significant advantages because it not only defends against cyberattacks but also forecasts when they will occur. DNN is now more appropriate because of advancements in data processing among network resources and increased storage capabilities brought about by hardware enhancements. High application chances are offered by recent advances in DNN technology, such as spiking neural networks that simulate living neurons; for instance, using field programmable gate arrays (FPGAs) enables rapid development of neural networks and their modifications to alter threats.

B. *Security Expert Systems*

Expert systems are computer programs created to support decision-making for complex issues within a particular domain. It is made up of an inference engine for reasoning and problem-solving and a knowledge base that stores information relevant to the topic under study [16]. Expert systems have applications in a variety of fields, including banking, healthcare, and the internet. To address complicated difficulties, expert systems come in a wide range of sizes, from modest to large technical diagnostic systems and complex hybrid systems. Theoretically, an expert system consists of an inference engine for retrieving answers from the knowledge base and, maybe, additional knowledge about the issue, as well as a knowledge base where the knowledge about the domain under examination is kept. Expert systems are used to many problem types based on the reasoning process. When using a case-based reasoning (CBR) technique, problems are first solved by recalling similar past situations, and then a solution is offered by applying the previous case's solution to the current problem scenario. The system's accuracy and capacity for learning are then improved by evaluating and revising the new answers as necessary. Rule-based systems (RBS) use rules that have been developed by experts to solve issues. The condition component and the action make up rules. The condition component of a problem is first evaluated, and only then is the appropriate course of action established. To stop cyberattacks, security expert systems adhere to a set of rules.

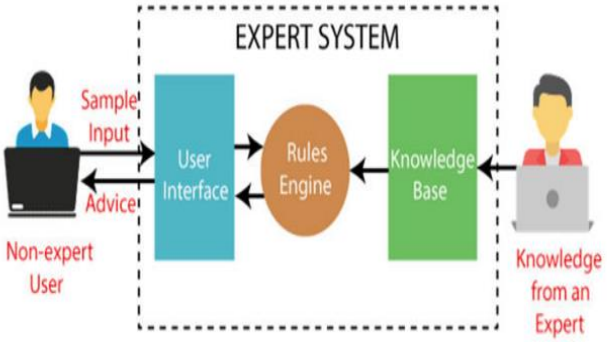

Fig. 4. An expert system for cybersecurity

An automated reasoning framework is the inference engine. It evaluates the condition of the knowledge base at the time, applies the relevant rules, and then declares new knowledge.

C. *4.3 Intelligent Agents*

A self-managing entity with a unique internal decision-making process and a personal goal is referred to as an intelligent agent (IA). It uses sensors to observe, actuators to monitor, and regulate its operations to accomplish the goals. In order to accomplish their goals, intelligent beings may also study or utilize information. They might exhibit responsive traits, and when interacting with other autonomous agents, they might comprehend and react to alterations in their domain. As they gain experience over time from learning about and interacting with their surroundings, this enables them to adopt themselves. Distributed Denial of Service (DDoS) assaults are prevented by IA. Building artificial digital police, which should be made up of mobile intelligent agents, is a powerful technique to deploy agents against distributed cyberattacks .Infrastructure must be put in place to support the mobility and communication of cyber agents.

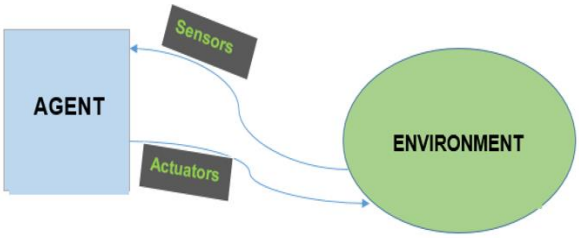

Fig. 5. Intelligent agents

TABLE I. COMPARISON BETWEEN AI TECHNIQUES

	Artificial Neural Networks	**Expert system**	**Intelligent Agents**
Definition	Its name and structure are derived from the human brain because it closely resembles how biological neurons communicate with one another.	A computer program that has the ability to learn new techniques by examining how prior events have turned out or that has a knowledge base of rules that can be used in situations when the developer hasn't specifically planned for them.	A program known as an intelligent agent can decide what to do or provide a service depending on its surroundings, user input, and past experiences.
Content	An input layer, one or more hidden layers, and an output layer are all included in the layers of nodes that make up this structure. Each node, or artificial neuron, is linked to the others and carries a single load.	Knowledge base, Inference engine, Knowledge acquisition & learning module, User interface, Explanation module.	sensors, actuators, and effectors.
Advantages	As the ANN is like the human brain in that it acquires knowledge by training and stores this knowledge using connections within neurons	It gives flexibility for choosing the necessary values for the security analysis.	Mobility Rationality Adaptability
Examples	Using to control the movement of a multi-fingered prosthetic robot's hand	The Google search box's recommendation of spelling problems is one of the typical examples of an ES.	AI assistants, like Alexa and Siri
Types	Feedforward Neural Network – Artificial Neuron. Radial basis function Neural Network. Kohonen Self Organizing Neural Network.	Frame-based, fuzzy, neural, and neuro-fuzzy expert systems are examples of expert systems.	Simple Reflex Agents. Model-Based Reflex Agents. Goal-Based Agents. Utility-Based Agents. Learning Agents

VII. FINDINGS/RESULTS:

Through this research, we found that artificial intelligence is one of the most prominent technological developments in recent times and has many uses in various sectors and fields. And it can detect electronic threats and protect personal information, and artificial intelligence is also the most effective tool against cyber threats. Also, throughout the comparison we did in this research, we find that these three techniques will benefit us in the future, and some of them we use often nowadays, such as Alexa and Siri.

VIII. CONCLUSION:

Cyber attackers target the massive number of data that businesses generate every day in the form of billions of transactions, making it impossible to manually verify for infiltration. AI for defense is a useful feature in the cybersecurity domain and continues to demand changes for future security measures, companies and enterprises must invest in AI to meet probable future defensive and offensive needs of cybersecurity. To identify cyber risks, it is essential to have an intelligent defense architecture with AI applications that can differentiate between appropriate and inappropriate computer network activities. A company's network is continuously monitored and reported on by AI programs, speeding up the reaction to events. Existing cyberattacks can be stopped and prevented by these AI applications.

REFERENCES:

[1] R. Das and R. Sandhane, "Artificial Intelligence in Cyber Security," J. Phys. Conf. Ser., vol. 1964, p. 042072, Jul. 2021, doi: 10.1088/1742-6596/1964/4/042072.

[2] S. Dilek, H. Çakır, and M. Aydın, "Applications of artificial intelligence techniques to combating cyber crimes: A review," International Journal of Artificial Intelligence & Applications, vol. 6, no. 1, January 2015, pp. 21-39.

[3] C. Crane, "Artificial intelligence in cyber security: The savior or enemy of your business?" July 2019, https://www.thesslstore.com/blog/artificial-intelligence-in-cyber-security-the-savior-or-enemy-of-your-business/

[4] S. Zeadally, E. Adi, Z. Baig, I.A. Khan, Harnessing artificial intelligence capabilities to improve cybersecurity, IEEE Access 8 (2020) 23817– 23837.

[5] I.Z. Chaloob, R. Ramli, M.K.M. Nawawi, Using simulation and data envelopment analysis to evaluate Iraqi regions in producing strategic crops, AIP Conf. Proc. 1635 (1) (2014) 525–529.

[6] Alhayani, Mohammed, Chaloob, Ahmed, "Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry" (2021)

[7] K.R. Bhatele, H. Shrivastava, N. Kumari, The Role of Artificial Intelligence in Cyber Security, in Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems, IGI Global, 2019, pp. 170–192.

[8] .S. Ahmed, H.J. Mohammed, I.Z. Chaloob, Application of a fuzzy multi- objective defuzzification method to solve a transportation problem, Mater. Today Proc. (2021).

[9] Ramasubramaniam,Venkateswarlu,Yerram"Applications and Techniques of Artificial Intelligence in Cyber Security" (2021)

[10] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018, May).

[11] On the effectiveness of machine and deep learning for cybersecurity. In 2018 10th

[12] International Conference on Cyber Conflict (CyCon) (pp. 371-390). IEEE.