International Journal of Electrical, Electronics and Computer Engineering **13**(1&2): 56-60(2024)

ISSN No. (Online): 2277-2626

Securing the Future: A Deep Dive into Ai's Role in Cyber security

Sourav*, Vishal Chauhan and Anshul Kumar

Department of School of Computer Science and Engineering,
Govt. P.G College Dharamshala, Himachal Pradesh Technical University (HPTU), India.

(Corresponding author: Sourav)*

(Received: 10 February 2024, Accepted: 19 April 2024)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: The frequency and sophistication of cyberattacks have significantly increased in the last few decades. This has brought to light how important it is to take a cyber-resilient strategy to security. In the face of these changingdangers, traditional security measures are frequently insufficient to prevent data breaches. Cybercriminals have mastered the use of cutting-edge methods and strong instruments to compromise networks andsteal data. Fortunately, a fresh approach to thwarting these threats has been made possible by the integration of Artificial Intelligence (AI) technology into cyber security.

AI is a useful technology in cyber security because it can be used to build intelligent models that quickly adapt to difficult conditions. By promptly detecting and notifying security teams of problems, artificial intelligence (AI) approaches can assist in the identification and response to a variety of threats, including malware assaults, network intrusions, phishing emails, and data breaches.

Keywords: cyber security, artificial intelligence, machine learning, deep learning, bio-inspired computing.

INTRODUCTION

The swift growth of computer networks has led to an increase in cyber attacks, endangering vital infrastructures, corporations, and governments. Since the initial denial-of-service (DOS) assault, the number and severity of these attacks, which aim to steal data or disrupt systems, have increased. In the current digital era, cyber security the process of defending against assaultson devices, networks, and data is essential.

Static security measures that respond to threats are the main emphasis of conventional cyber security techniques. However, because cyber threats are getting more frequent and sophisticated, these measures are no longer sufficient. The Equifax hack, for instance, revealed millions of customers' personal information and showed the flaws in conventional cyber security techniques.

Businesses, law enforcement, and national security are all impacted by the global scarcity of cyber security specialists. Attackers obtain sensitive data by taking advantage of holes in IT systems. Cyber attacks must be prevented with a more aggressive strategy; passive protection tactics are no longer adequate (John McCarthy, 2018).

Enhancing cyber security protections with artificial intelligence (AI) is a viable approach. Artificial intelligence (AI) technologies, such machine learning and deep learning, can identify and address cyber threats instantly. AI systems are capable of spotting trends and anomalies that point to a cyber attack by evaluating enormous volumes of data.

AI integration into cyber security plans can greatly strengthen defences against changing cyberthreats. This essay addresses several AI-based cyber security strategies and investigates the application of AI in cyber security. It also offers suggestions foradditional study in this area in the future.

In conclusion, to counter the growing threat posed by cyber attacks, cyber security methods need to adapt. AI technologies provide a potent instrument to strengthen cyber security barriers and guard against new dangers. Organizations may strengthen their cyber security posture and protect their digital assets by implementing AI.

OVERVIEW OF ARTIFICIAL INTELLIGENCE

The idea of artificial intelligence (AI) as a branch of computer science has become widely accepted within the past ten years. John McCarthy coined the term artificial intelligence in. He defined AI as a methodology that formalizes fundamental truths about events and their consequences through mathematical reasoning. Artificial Intelligence, or AI for short, is intelligencedisplayed by a machine. It makes it possible for programmers to create their programs simply. AI uses sophisticated mathematical algorithms to mimic human thought processes. Artificial intelligence (AI) systems can comprehend, learn, andrespond using data from events and effects. "AI attempts not just to understand but also to build intelligent entities," according to Stuart Russell and Peter Norvig, who also provided a definition of AI that is divided into two primary groups, like:

Reasoning and the mental process: these gauges one's ability to think, which can be divided into two categories: rationaland human thought.
Behavior: this divides behavior into two categories: acting rationally and acting humanely. It evaluates performance based onthe ideal performance and action. The following table presents a definition for each category.

Table 1: AI definitions.

"The exciting new effort to make computers think ... *machines with minds*, in the full and literal sense"(Haugeland, 1985)	"The study of the computations that make it possible to perceive, reason, and act." (Winston)
"The study of how to make computers do things at which, at the moment, people are better" (Rich andKnight, 1991)	"The branch of computer science that is concerned with the nautomation of intelligent behavior" (Luger and Stubblefield, 1993)

According to the above definitions, the AI strategy builds intelligent agents by first concentrating on human behaviors, knowledge representations, and inference techniques. Agents can communicate and share knowledge with one another. The information that agents share with one another helps them solve problems. Each agent has a decision-making system that it has built using the principles of decision-making theory.
The two facets of decision-making theory are look-ahead and diagnosis. According to Jean Pomerol, AI has numerous connections to diagnosing, encoding, and portraying human knowledge. AI ignores multi-attribute human reasoning and does not give enough consideration to this element since look-ahead decisions are unclear. To account for the fact that people consider multiple factors at different points during the decision-making process, Simon proposed a bounded rationality model. As a result, tradeoff reasoning may be a reasonable approach. Consequently, the goal of AI is to create anew kind of automated intelligence that behaves like human intellect. Machines must be trained by learning algorithms to learn precisely, which is a prerequisite for achieving this goal. Algorithms are used in AI techniques. But even with limitedadvancements in algorithms, AI can still learn by brute force using large datasets and powerful computers.
There are three ways AI operates:
Autonomous intelligence, which refers to aspects of computers that act on their own; *Augmented intelligence*, which enables people to perform things that they could not; and *Assisted intelligence,* which enhances what people are already doing.
Based on these three categories, one could argue that artificial intelligence (AI) seeks to address some of the most challenging issues. Cyber security fits under this category because cyber attacks have evolved into highly sophisticated, possibly catastrophic, and complicated issues in cyberspace.

AI TECHNIQUES IN CYBER SECURITY

This section provides a quick summary of learning algorithms, which are fundamental ideas in artificial intelligence. It alsoprovides a brief overview of some of the AI subfields that are commonly used in the cyber security space, including expert systems, machine learning, deep learning, and biologically inspired computation.
In addition to teaching machines, learning algorithms are utilized to improve performance through experience-based learning and training. "A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P, if its performance at tasks in T, as measured by P, improves with experience E," states Mitchel's definition. To teaching machines, there are three common learning algorithms, which are described below:
Supervised learning*:* This kind uses a sizable labeled data collection during the training phase. A test data set must be usedto verify the system following the training phase. Typically, these learning algorithms are employed as regression or classification mechanisms. Based on the input, the regression method produces outputs, or prediction values, which are one or more continuous-valued numbers. Algorithms for classification divide data into groups and produce distinct results, unlike regression procedures.
Unsupervised learning: Using an unlabeled training data set, unsupervised learning differs from supervised learning. Unsupervised learning is typically applied to estimate density, decrease dimensionality, or cluster data.
Reinforcement learning: This kind of algorithm learns the optimal behaviors in response to rewards or penalties. One way to think of reinforcement is as a hybrid of supervised and uncontrolled learning. In circumstances where data is scarce or unavailable, reinforcement learning can be helpful.
There are several subfields within AI technology, some of which are listed here (Jian-hua, 2018).
Knowledge-based systems, or expert systems (ES), are another name for them. The two primary parts of ES are an inference engine, which is used to reason about predefined knowledge and find solutions to given issues, and a collection of knowledge, which forms the basis of a knowledge-based system and incorporates acquired experiences. The reasoning technique states that expert systems are capable of handling both rule-based and case-based reasoning difficulties. Case-based reasoning: It looks back at earlier, comparable cases and presupposes that the answers to those examples may be applied to more recent ones. The new answer will then be assessed, and if necessary, changed before being added to the knowledge base. This method gradually picks up new issues and helps the system become more accurate over time.
Rule-based reasoning: This approach solves issues by

applying rules that are established by specialists. A rule is made up of two components: an action and a condition. Two steps are involved in problem analysis: first, the situation is assessed, and then the appropriate course of action is implemented. Rule-based systems, in contrast to case-based systems, are unable to automatically pick up new rules or alter ones that already exist

In cyberspace, ESs can be utilized to support decision-making. Altered security system data are assessed before the security expert system decides whether a system or network behavior is malicious. Security professionals typically scan and evaluate a sizable amount of updated data in a reasonable amount of time using statistical approaches. Expert systems that monitor in real time in cyber settings can effectively assist these efforts. Security experts can choose the proper security measures based on the pertinent information and warning message that security expert systems provide in the event of harmful intrusions.

Machine learning (ML): As defined by Arthur Samuel, ML is "a collection of techniques that endows computers with the capacity to learn without explicit programming." Without being explicitly coded, machine learning (ML) gives systems the power to identify and formalize the principles underlying the data, learn from the data, and get better with time. *The process of learning begins with observing data through examples to look for patterns in* provided examples, the learning process starts with the observation of data through instances. The algorithm can reason the properties of cases that have not been observed before using this information. Machine learning (ML) leverages statistics to identify trends, extract information, and draw conclusions from vast amounts of data. Different kinds of machine learning algorithms exist. They can be divided into three primary groups: reinforcement learning, unsupervised learning, and supervised learning. In the cyber security domain, the most used algorithms are: decision tree, support vector machine, Bayesian algorithms, k-nearest neighbor, random forest, association rule algorithms, ensemble learning, k-means clustering, and principal component analysis.

Deep learning (DL): Using data, deep learning (DL), also called deep neural learning, is a technique that teaches computers how to undertake activities that are normally performed by humans. It is a branch of machine learning (ML) that allows computers to become more intelligent via experience and perform better on their own without the need for human assistance. Like people, DL algorithms get expertise through practice. They repeat a task and make minor improvements to get better at it. DL uses techniques akin to neuronal signal processing to simulate how the human brain processes information and looks for patterns to make judgments. Building larger networks and training them with vast amounts of data are key components of deep learning (DL), which aims to improve neural network performance. Since these algorithms need a large amount of data to learn properly, the massive amount of data generated every day in a variety of applications highlights the necessity for deep learning (DL). There are benefits to using DL over ML, especially when managing big data sets. Like ML techniques, DL techniques cover a variety of learning approaches, such as supervised learning, unsupervised learning, and reinforcement learning. Feed forward neural networks, convolutional neural networks, recurrent neural networks, deep belief networks, stacking autoencoders, generative adversarial networks, restricted Boltzmann machines, and other types of deep learning networks are examples of DL approaches that are frequently employed in cyber security.

Biologically inspired computation: This is an array of sophisticated algorithms and techniques that leverage biological traits and behaviors to address a broad spectrum of challenging issues. The ways that traditional AI and bio-inspired approaches learn differ from one another. Programs produce other programs, including intelligence, which creates this intelligence. But the foundation of bio-inspired computing is made up of a few basic laws and little creatures that strictly follow them. The bio- inspired computations that are most frequently employed in the cyber security field include the following methods: The genetic artificial immune systems, particle swarm optimization, ant colony optimization, evolution techniques, and algorithms.

AI-BASED APPROCHES IN CYBER SECURITY

Thanks to developments in computing technologies, our society is changing quickly and has a big impact on people's daily lives and jobs. With the use of some of these technologies, machines are now able to think, learn, make decisions, and solve problems just like people do. For instance, artificial intelligence (AI) absorbs intellect and can process massive volumes of data to solve issues while performing real-time analysis and decision-making. Artificial intelligence techniques can benefit numerous scientific and technological domains. It goes without saying that the Internet is a goldmine of personal data, which leads to several cyber security problems. First, the volume of data makes manual analysis all but impossible. Second, risks are evolving or they could be AI-based. Additionally, the high expense of hiring specialists drives up the cost of threat prevention. Developing and deploying algorithms to identify those dangers also requires a significant investment of time, funds, and resources. Using AI-based techniques is one way to address those problems.

AI is capable of quickly, precisely, and effectively analyzing vast amounts of data. An artificial intelligence (AI) system can forecast similar attacks in the future, even if their patterns vary, by using threat history. AI can be applied in cyberspace for the following reasons: AI can handle large data, AI can identify novel and significant changes in attacks, and AI security systems can continuously train to improve their response to threats.

But artificial intelligence (AI) is not without its drawbacks. For example, an AI-based system needs a large quantity of data, and processing this massive data takes time and resources. False alarms are a problem for end users, and delaying necessary responses reduces

efficiency. In addition, the AI-based system is vulnerable to attacks such as model stealing, data poisoning, and adversarial input insertion.

Recently, scientists have discovered how to use AI approaches to identify, thwart, and respond to cyberattacks. The four primary groups that comprise the most prevalent forms of cyberattacks are as follows:

Software exploitation and malware identification.

Software exploitation: Software exploitation refers to the act of exploiting vulnerabilities in software to gain unauthorized access or control over a system. Common vulnerabilities include buffer overflows, integer overflows, SQL injections, cross- site scripting, and cross-site request forgeries. While developers strive to identify and address vulnerabilities during the design and development phase, it is challenging to eliminate all vulnerabilities given the complexity of software development and the need to release software quickly. Continuous monitoring and identification of vulnerabilities are essential processes.

The internet is considered one of the most complex machines built by mankind, and securing it is a daunting task. Manually reviewing code to patch software defects is time-consuming, but AI can be trained to identify vulnerabilities efficiently. Benoit Moral proposed using AI methods, such as probabilistic reasoning and Bayesian algorithms, to detect software exploits, particularly in web applications.

Malware identification is crucial for defending against cyber attacks. Malicious software, such as Trojan horses, worms, and viruses, can have significant impacts on politics and the economy. Researchers have developed various AI-based approaches for malware identification. For example, data mining and machine learning classification systems have been used to categorize and identify malware. Support vector machines and k-nearest neighbors have been employed to detect unknown malware, while deep learning architectures have been utilized for intelligent malware detection. Recent studies have focused on mobiledevice malware detection using deep convolutional neural networks and innovative machine learning techniques like rotation forest and bio-inspired computation.

Network intrusion detection

Denial of Service (DoS): One of the most popular types of assaults, this one happens when hackers prevent authorized users from accessing data, hardware, or other network resources. A system utilizing two distinct approaches—anomaly-based distributed artificial neural networks and signature-based approach—was presented by the authors in.

Intrusion Detection System (IDS): An IDS guards against unforeseen happenings, security breaches, and direct dangers to a computer system. Artificial intelligence (AI)-based technologies are suitable for creating because of their flexibility, speed, and ease of learning. IDS.AI- based techniques aim to reduce false alarms by improving classifiers and optimizing characteristics (Benoit Morel 2019). To construct a model for IDS, the authors in mergeda modified version of k-means with a support vector machine. The authors of described a reinforcement learning strategy for IDS that is based on fuzziness. To improve the performance, they employed supervised learning on unlabeled sample datasets. Another method, predicted network traffic over a specified time using fuzzy logic and evolutionary algorithms for network intrusion detection.

Phishing and spam detection:

Phishing attack: The goal of a phishing attack is to get user identity. Phishing attacks include, for example, dictionary and brute-force attacks. Here are some noteworthy AI-based solutions to address this problem. A phishing email detection system, which made use of reinforcement learning and a modified neural network, was presented by the authors in. In, Feng et al. used a neural network with the Monte Carlo method and a risk- minimization strategy to detect phishing websites.

***Spam detection*:** Uninvited bulk emails are referred to here. Inappropriate material in spam emails might cause security problems. Algorithms powered by AI have been employed recently to filter spam emails. As an example,consider the system showed. The naive Bayes algorithm and support vector machine were integrated by this system to screen spam emails.

Artificial intelligence (AI) can be used to analyze data for attack detection and response in a variety of cyberspace domains. Processes can also be automated using AI, which makes it easier for security analysts to identify cyberattacks rapidly by utilizing semi-automated systems. The following list includes some well-liked AI cyber security approaches:

(a) Threat detection and classification:

Artificial intelligence (AI) techniques are employed to anticipate and prevent cyberattacks. This involves creating models to analyze vast amounts of cyber security data, identifying suspicious activity patterns, and mitigating threats. These models are built using recorded Indicators of Compromise (IOC) and historical data to detect and respond to threats promptly. They automatically recognize similar activities and use Machine Learning (ML) classification algorithms to identify and categorize malware behaviors. Behavioral-based analysis utilizes ML clustering and classification algorithms to analyze millions of malware behaviors, enabling the automation of threat identification and categorization. Security analysts and automated systems benefit from these patterns, which can also be used to detect emerging threats. For instance, historical datasets of WannaCry ransomware attacks can help ML algorithms automatically identify similar attacks.

(b) Network risk scoring:

Network risk scoring is a measurable measure that assesses the risk level of different network segments. It helps prioritize cyber security resources based on these risk scores. Artificial intelligence (AI) can automate this process by analyzing past cyber security data, identifying network segments that are more vulnerable to certain types of attacks (Lidestri *et al.*, 2020).

(c) Automated processes and optimize human analysis:

Security analysts can use AI to automate repetitive tasks during security operations, freeing up their time for more complex analysis. One way to automate

processes is by analyzing historical activity data generated by security analysts to identify and effectively respond to specific attacks. AI systems can create models based on this data to detect similar cyber activity in the future, enabling them to respond to attacks without human intervention. However, fully automating the security process can be challenging. In such cases, AI can be integrated into the cyber security workflow to facilitate collaboration between system analysts and computers. This integration allows AI to assist analysts in making informed decisions and optimizing human analysis, ultimately enhancing the overall effectiveness of cyber security measures.

CONCLUSION

As the increasing sophistication of cyberattacks and the rapid increase of cyber threats, new, more resilient, adaptable, and scalable techniques are needed. According to recent study, phishing and spam detection, malware detection, and network intrusion detection are the three primary goals of AI-based cyber security algorithms. Numerous studies have combined various AI techniques, such as ML/DL approaches with bio-inspired computation or supervised learning with reinforcement learning, with other learning methods. These pairings produce very good outcomes. While AI will undoubtedly play a part in resolving cyberspace challenges, there are concerns around AI trust as well as threats and attacks utilizing AI.

REFERENCES

Benoit Morel (2019). Artificial Intelligence a Key to the Future of Cyber security. In Proceeding of Conference AISec'11, October 2011, Chicago, Illinois, USA.

John McCarthy (2018). Artificial Intelligence logic and formalizing common sense. Stanford University, CA, USA 1990. Myriam Dunn Cavelty. *The Routledge Handbook of New Security Studies*, 154-162.

Jian-hua LI (2018). "Cyber security meets artificial intelligence: a survey," School of cyber security, Shanghai Jiao Tong University, Shanghai, China, 2018.

Lidestri, N., Maher, Stephen J., & Zunic, Nev (2018). The Impact of Artificial Intelligence in Cyber security. ProQuest Dissertations and Theses, 2018.