IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 7, July 2022

DOI: 10.17148/IARJSET.2022.9727

A Review on Combating Cyber Attacks using Artificial Intelligence

Suchith S[1], Prashanth K[2]

PG Student, Department of MCA, RV College of Engineering, Bengaluru, India[1]

Associate Professor, Department of MCA, RV College of Engineering, Bengaluru, India[2]

Abstract- We all know in the current scenario, cyber attacks, security and artificial intelligence (AI) are growing technologies. Machine learning (ML) models have setup a foundation for Artificial Intelligence(AI) based systems.AI plays a very important role in every aspects such as authentication of user, access control, spam, malware, behavior analysis and identification botnet. Contrarily, there are several security challenges in today's world. Users now face serious security dangers from cloud computing, social media, smart phones, and the widespread use of multiple apps like WhatsApp and Vibe. Artificial intelligence-based cybersecurity has a double-edged sword in that it can both significantly increase security and open the door to new types of attack that can be launched against AI itself. Machine learning algorithms have shown to be helpful in identifying zero-day attacks and seeing odd system behaviour that could be a sign of malware or an attack. Finally, we will talk about the importance of artificial intelligence (AI) and how it can be used to address cyber security concerns and cyberthreats in this paper.

Keywords: Cybersecurity; Artificial Intelligence, Cyber attacks

.I. INTRODUCTION

The field of cybersecurity is dedicated to guarding against such dangers to our systems, data, networks, etc. To make systems secure against such attacks, it makes use of technologies like cryptography, antivirus software, and intrusion detection systems (IDS). In the past, the sector has expanded significantly and assisted in thwarting numerous attacks and malware. For these detection systems, conventional security techniques use signatures of previous assaults.They attempt to match known malware and attack types with current traffic using a database that they have on hand. It generates an alarm if it notices any unexpected activity that corresponds to a signature in the database. These techniques work well for the attacks that we are now aware of, but it is now believed that cyberattacks will continue to advance. According to recent study, new assault strategies are constantly being developed. Attacks that are zero-day, or attacks that have never been seen before, cannot be found by current systems. As attacks have advanced, attackers have begun utilising tools like artificial intelligence (AI) to make attacks quick and efficient. They employ AI technologies for advanced intrusion and anomaly detection systems, cryptanalysis, brute-forcing, and other activities. With machine learning and AI, that data surge might be reduced in a short amount of time, enabling the company to recognise and address the security problem. These technologies are always learning and developing, gathering information from the past as well as the present to identify new types of attacks that might take place right now or in the future.

II. ROLE OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

A. Artificial Intelligence(AI) :

AI is a technique for teaching a computer, a robot that is controlled by a computer, or a piece of software to think critically, much like an intelligent person might. It is possible to create intelligent software and systems by first studying how the human brain works, as well as by research and by conducting experiments on how people learn, how they make decisions based on the learning, and combine different results when attempting to solve a problem. Commonly, people define intelligence as the capacity to acquire knowledge and use knowledge to reason about difficulties. Intelligent machines will soon take over many human functions in the near future. The study and creation of intelligent computers and software that can reason, learn, gather information, communicate, operate, and perceive objects are known as artificial intelligence. The phrase was first used in 1956 by John McCarthy to refer to a field of computer science that focuses on teaching computers to act like people. The ability to discern reason and take action is made possible by the study of computing. The emphasis on computing sets artificial intelligence apart from psychology, while its emphasis on perception, thinking, and action sets it apart from computer science. Machines become wiser and more valuable as a result.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 7, July 2022

DOI: 10.17148/IARJSET.2022.9727

B. **Cyber threat Intelligence cycle**

The Cyber Threats Intelligence Cycle is a methodical, ongoing procedure for monitoring potential threats to find a suspicious collection of actions that could endanger the systems, networks, information, and personnel of the organization or clients by giving them a way to visualise and evaluating a variety of particular intrusion sensor inputs and open source data to determine specific threat scenarios action. The model validates the company's risk. the information security group's management approach decision-making. The model's application identifies proactive plans for anticipated threats and assistance with security Risk management authorities use and maximize a deeper comprehension of the defense in depth strategy cyberthreats to an organization at key junctures and creating space in the operational setting by:

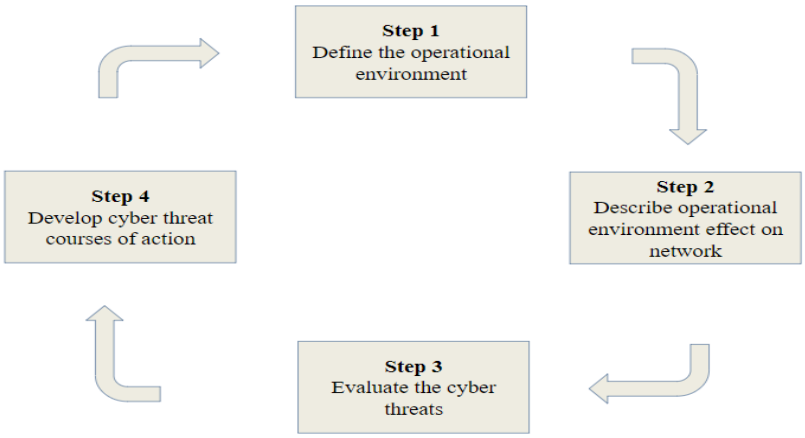

Fig 1 : Intelligence cycle of cyber threats

1) The operational environment should be defined,
2) Operational environment effects on network defense should be described,
3) Cyber threats should be evaluated, and
4) Cyber threat response strategies should be developed.

C. **What Applications Does Artificial Intelligence Have for Cybersecurity?**

Artificial intelligence (AI) is already being applied in various areas of cyber security solutions or is currently being investigated in these areas: Gmail uses artificial intelligence to detect unwanted spam and fraudulent emails and block them (AI). Each time a user marks or clicks an email, consider it as not spam, you are helping to educate the AI to recognise spam in the future. Millions of current Gmail users trained the artificial intelligence that powers Gmail. Because of this advancement, artificial intelligence is now capable of detecting even the subtlest spam emails that try to pass as "regular" emails.

• Detection of fraud: Using Decision Intelligence deployed by MasterCard, a fraud detection system powered by artificial intelligence that uses algorithms based on expected consumer behaviour to spot fraudulent transactions. To assess if a purchase is odd, it looks at the buyer's typical buying habits, the seller, the location of the transaction, and many more intricate algorithms.

• Botnet Detection: A particularly challenging field, botnet detection often relies on proxy server timing analysis and pattern recognition. A botnet assault often involves a large number of "users" performing the same queries on a website since botnets are typically managed by a master script of instructions. This may entail failing login attempts, other breaches, and network vulnerability scans (a botnet brute force password assault). The role artificial intelligence plays in identifying botnets is one that is exceedingly difficult to describe.

• Spotting new dangers

AI can be used to spot suspected criminal activities and internet threats. Artificial intelligence can be particularly helpful in this case because traditional software systems cannot handle the massive amount of new malware that is produced every week. Before malware or ransomware attacks reach the system, AI systems are being trained to recognise trends, detect malware, and even the minute details of those attacks.

With the use of natural language processing, which collects data by itself by reading articles, news stories, and research on cyberthreats, AI enables higher predictive intelligence. This can provide information on brand-new oddities, cyberattacks, and defense tactics. Since cybercriminals also follow trends, what is popular with them is continuously shifting. AI-based cybersecurity solutions may offer the most recent information on both general and industry-specific

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 7, July 2022

DOI: 10.17148/IARJSET.2022.9727

risks, helping you to better prioritize important decisions based not just on what could be used to attack your systems but also on what is most likely to do so.

• Prediction of Breach Risk

AI algorithms are used to create the IT asset inventory, which is a precise and comprehensive record of all devices, users, and apps with different levels of access to various systems. Based on your asset inventory and threat exposure, AI-based solutions may now assess how and where you are most likely to be compromised, enabling you to plan and direct resources to areas with the biggest risks. Prescriptive insights from AI-based analysis enable you to create and improve policies and procedures to increase your cyber resilience.

Better Endpoint Protection

AI is crucial for protecting all of the endpoints used for remote work, which is using an exponentially rising number of devices. Users of antivirus software and VPNs can undoubtedly be protected from remote malware and ransomware attacks, but these tools typically rely on signature-based operations. This implies that it becomes essential to stay current with signature definitions in order to remain safe against the most recent threats. If antivirus software is not updated or the software manufacturer is unaware that virus definitions are out of date, this may be cause for alarm. Therefore, signature protection may not be able to defend against a new sort of malware assault if it arises. "AI-driven endpoint protection adopts a different strategy, establishing an endpoint's baseline behaviour through recurrent training. AI may detect anomalies and take appropriate action, such as alerting a technician or returning to a secure state following a ransomware assault, if necessary. Instead of waiting for signature updates, this offers proactive protection against threats, according to Tim Brown, VP of Security Architecture at SolarWinds.

These are only a few applications of artificial intelligence that have been made to improve cyber security. There are several study studies available right now that present convincing evidence in favour of artificial intelligence's efficiency in the area of cyber security. The bulk of research have found that between 85 and 99 percent of attempts to identify cyberattacks are successful. Dark Trace, a company that creates artificial intelligence, claims to have a success record of 99 percent and already has thousands of customers worldwide.

C. Benefits of AI in Cyber Security:

One of the numerous areas in which AI is useful and has applications is cybersecurity. In today's environment of swiftly evolving cyberattacks and rapidly proliferating electronics, AI and machine learning are more effective than conventional software-driven or manual processes at identifying threats, automating threat identification, and responding to them.

• IT asset inventory - creating a complete, accurate account of all the equipment, software, and users who have access to information systems. Measurement of business criticality and inventory classification are both crucial.

• Threat Exposure: Just like everyone else, hackers follow fashion trends, so what's in style changes frequently. AI-based cybersecurity solutions can offer current information on regional and sector-specific threats to assist in prioritising crucial actions based not just on what could be used to attack your organisation but also on what is likely to be used to attack your enterprise.

• Effectiveness of Controls - It is crucial to comprehend the effects of the many security instruments and security processes that

To maintain a robust security posture, you have employed. AI can assist in identifying the areas of your infosec program's strengths and weaknesses.

• Incident response: AI-powered systems can offer more context for prioritising and responding to security warnings, for quick response to incidents, and for uncovering root causes to minimise vulnerabilities and prevent future problems.

• Assessments and recommendations for AI to support human infosec teams must be clear to understand. This is necessary for securing the backing of all significant internal stakeholders, comprehending the effects of various infosec programmes, and communicating crucial information to all interested parties, including end users, security operations, the CISO, auditors, CIO, CEO, and board of directors.

D. The Biggest Challenges In Cybersecurity

The company and cybersecurity specialists must deal with more challenges than only the active usage of AI and machine learning. Others result from flaws in the way security is currently handled.

• The far-flung infrastructure. Systems may now connect with one other across continents and deliver sensitive data anywhere in the world. These transfers don't receive enough security and are simpler to hack into.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 7, July 2022

DOI: 10.17148/IARJSET.2022.9727

• Hand-held detection Human teams cannot continuously pay attention to security concerns and ominous patterns. Systems are frequently not monitored.
• Security teams' responsiveness. Instead of predicting dangers, most security specialists concentrate on dealing with them.
• Threats that change.Hackers use a range of strategies to hide their physical locations, IP addresses, identities, and methodologies. In contrast, because thieves have easy access to data generated by businesses, the cybersecurity sector is far more visible and open to inquiry.

D. Downsides of AI in Cyber Security:

The advantages of AI for improving cybersecurity are not limited to those listed above. But using AI in this industry has drawbacks, just like anything else. An enormous increase in resources and capital expenditures would be required for the development and upkeep of an AI system for organisations. You also need to gather several distinct sets of malware codes, non-malicious codes, and irregularities because data sets are utilised to train AI algorithms. The majority of businesses are unable to afford the time and money required to obtain all of these data sets.AI systems may generate false positives or erroneous conclusions in the absence of enormous volumes of data and events. Additionally, getting erroneous information from questionable sources might be harmful.

The ability of attackers to use AI to analyse their infection and conduct more sophisticated attacks is a big additional disadvantage.

1) Cost-effectiveness: Because some AI services can be prohibitively expensive, not everyone can benefit from them.
2) Cyberthreats: In the modern world, hackers have too much access to your data and privacy. If precautions are not followed, they can easily track your whereabouts and hack your personal information.
3)The third AI worry is that machines will start to rule over people. This issue has previously been covered in numerous movie books. It is necessary to take action to stop this from happening.
4) Job loss: Artificial intelligence is viewed as a threat since some studies indicate that a significant portion of the workforce will be replaced by AI apps and machinery.
5) Not everyone is knowledgeable about AI: Not everyone is eager to learn about and use cutting-edge technologies.

III. CONCLUSIONS AND FUTURE WORKS

Therefore, in this essay, we examined the significance of artificial intelligence in cyber security as well as a number of related issues and solutions. Despite its limitations, artificial intelligence still plays a big part in cyber security. Artificial intelligence will help to enhance cyber security in order to overcome the limitations.

Block chain technology may help companies, from those in the heavy industry, like mining, to those in the fashion industry, in response to the public and investors' growing interest in sustainable and ethical sourcing. In order to help decrease fraud and identity theft, banking and financial institutions use strategies including the use of digital crypto currencies and the promotion of cross-border and remittance digital payments.

ACKNOWLEDGMENT

We would want to express our gratitude to everyone who has helped the study succeed and assisted us in coming to a final conclusion, whether directly or indirectly.

REFERENCES

[1] Ankush Mehra, Sumit Badotra “Artificial Intelligence Enabled Cyber Security”, 6th International conference on Signal processing, commuting and control(ISPCC), 2021 978-1-6654-2554-4/21
[2] Nir Kshetri, “Economics of Artificial Intelligence in Cybersecurity” ,2021 IEEE International Conference on Artificial Intelligence
[3] Xiaohua Feng, Yunzhong Feng, Edward Swarlat Dawam“Artificial Intelligence Cyber Security Strategy”,2020. IEEE international Conference on Autonomic and secure computing
[4] Stephen R. Gulliver and Isaac Wiafe “Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature” , Published by the IEEE Computer Society, July 30 2020
[5] Roumen Trifonov, Ognyan Nakov, Valeri Mladenov “Artificial Intelligence in Cyber Threats Intelligence” ,Published by IEEE European , 2018, doi: 10.1109/ICACEA.2013.7164748.

DOI: 10.17148/IARJSET.2022.9727

[6] Roumen Trifonov, Ognyan Nakov, Slavcho Manolov, Georgi Tsochev, Galya Pavlova "One method of network cyber-security, based on artificial intelligence", Proc. 27-th National Conference with International Participation "TELECOM 2019", October 30 - 31, 2019, Sofia, Bulgaria

[7]Sagar B.S, Niranjan S, Nithin Kashyap, Sachin D.N "Providing Cyber Security using Artificial Intelligence – A survey" ,Third International Conference on Computing Methodologies and Communication (ICCMC 2019)

[8] Haining Zhao, Liquan Chen "Artificial Intelligence Security Issues and Responses" , 2020 IEEE 6th International Conference on Computer and Communications

