ISSN No:-2456-2165

Artificial Intelligence and Cybersecurity: A Comprehensive Review of Recent Developments

Dr. Naveen Kumar C.G [1]
Assistant Professor
Department of Computer Science Karnataka State Open University,
Mysuru, India

Abstract:- Due to the expansion of the internet of things and connected devices, cyber security professionals in the modern digital world face a significant number of challenges. Experts require all available resources in order to both respond to attacks and prevent further security breaches. Due to factors such as heavy traffic, an increase in the number of security attack vectors, security vulnerabilities, and many others, the number of connected workplaces renders it impossible for humans to govern cyberspace without significant automation. However, designing software systems with conventionally mounted algorithms (decision-making logic that is hardwired) can be difficult. These algorithms are necessary to provide an effective defence against the growing number of network hazards. It is now common knowledge that adopting problem-solving strategies based on artificial intelligence is the key to effectively addressing the vast majority of cyber security issues currently being addressed. This article provides a concise analysis of cyber security applications for computers. In addition, it investigates the perspectives on how to enhance cyber security capabilities by providing applications that utilise artificial intelligence, in addition to the current methods.

***Keywords*:-** *Cyber Security; Artificial Intellegence; Expert Systems.*

I. INTRODUCTION

The application of AI in security systems has the ability to lessen the rising and changing cyber security risk that is today faced by organisations all over the globe. As computing power, data collection capabilities, and storage capacity continue to advance, machine learning and artificial intelligence are being used in an increasing number of industries and applications. This is a significant shift from previous years (AI). It is anticipated that this pattern will go on. It is impossible for human people to comprehend this large data gathering in real time because it contains too much information. With the help of machine learning and artificial intelligence, this mountain of data might be reduced in a much shorter amount of time, which would be of great assistance to the organisation in determining the source of the security problem and recovering from it. It's possible that the employment of artificial intelligence in security teams will radically change the game. (2012)

- *Objective*

The research aimed to fulfil the following objectives:

- *To study taking of artificial intelligence & cyber security*
- *How may AI change the state of cyber defence ?*
- *To study tools for cyber security*

II. METHODOLOGY

Alongside the development of new technologies comes an increase in the number and sophistication of cybercrimes. Criminals operating online are using more sophisticated methods to initiate assaults, which puts contemporary security infrastructure in jeopardy. As a result, the cyber security sector is likewise undergoing change in order to keep up with the growing number of security requirements posed by businesses. However, there is a possibility that these protective techniques used by security specialists may fail at some time.

Artificial intelligence is being used by businesses in order to improve their detection methods for vulnerabilities and step up their overall game (AI). The use of artificial intelligence in the field of cyber security is assisting businesses in protecting their defensive systems. In addition to this, it helps them improve their analysis of cybercrimes.

III. ARTIFICIAL INTELLIGENCE & CYBER SECURITY

Once upon a time, there was no connection between computer security and AI. Researchers in artificial intelligence wanted to develop programmes that would reduce the amount of labour required of humans, while those working in security wanted to prevent the leak of sensitive information. However, the two domains have become increasingly intertwined as attacks have developed to attempt to replicate the genuine performance not just at the human user level but also at lower system levels. There has been an increased convergence between the two fields. An excellent example of how AI might be used to bolster safety is the "Completely Automated Public Turing test to tell Computers and Humans Apart" (CAPTCHA). In order to complete the CAPTCHA, the user must enter the characters that appear on a distorted picture. (2012) In addition to the typical login information, the user may be asked to input a secret code made up of letters and digits. Enhanced ACR software may be seen as a major

breakthrough in AI, inspiring a transition to more intricate pattern recognition. For this reason, the commercial security industry is indirectly promoting the development of artificial intelligence (AI) by working to safeguard activities like online ticket purchases. Our solutions rely heavily on AI because of its ability to rapidly identify and assess new exploits and holes, reducing the severity of future assaults.

The ability to identify and react to previously undiscovered threats is a major draw for the use of artificial intelligence (AI) techniques in intrusion detection. For example, when it comes to understanding particularly novel types of cyber-attacks, artificial intelligence systems that are programmed to learn and adapt and can detect even the smallest of changes in their surroundings can respond much more quickly - and on the basis of vast troves of data - than humans can. (Dunn Cavelty, 2018)

- *Expert Systems*

One kind of artificial intelligence, or AI, is a "expert system," which is a computer programme designed to mimic human experts' level of expertise and decision-making skills. Knowledge-based systems like this one are composed of two components: a knowledge base and an inference engine. The assertions and examples that make up the knowledge base are a portrayal of the world as we know it. An automated reasoning system, the inference engine examines the current state of the knowledge base, implements the rules that are relevant to that state, and then asserts fresh information into the database. The Cyber Security Artificial Intelligence Expert System, often known as CSIA, is comprised of the following essential elements in its knowledge base and Inference Engine: In order to protect against cyber attacks, the Security expert system goes through a series of processes. It compares the process to the knowledge base to determine whether or not it is a well-known process that should be ignored; if not, the system should end the process. If there is no such process in the knowledge base, the expert system will use inference engine methods, also known as rule sets, to determine the current state of the machine. The condition of the machine has been broken down into three distinct categories: safe, moderate, and severe. According to the current condition of the machine, the notification is sent to the administrator or user, and the knowledge base has been updated with the inference. (Bradbury, 2021)

- *Neural Nets*

Deep learning, which sometimes refers to neural networks, is an advanced subfield of artificial intelligence. The processes of the human brain served as an inspiration for it. Our neurons, which for the most part have no specialized function and are independent of certain domains, have the ability to learn any kind of information. Frank Rosenblatt invented the artificial neuron known as the Perceptron in 1957, which paved the path for the development of neural networks. Through interaction with other perceptron's, these ones are able to learn and find solutions to challenging problems. They learn to recognize the thing on which they are taught on their own by learning and digesting the high-level raw data, much as our brain learns on its own from the raw data utilizing the inputs from our sense organs. When this kind of deep learning, which has been taught, is used to computer security, the system is able to determine, without the need for human interaction, whether a file is harmful or lawful. In comparison to traditional methods of machine learning, our approach yields much better results while searching for malware. The rapid speed at which neural networks may be implemented in hardware or graphics processors is the key to their success in the field of cyber security. The exact identification of emerging malware threats and the filling in of important gaps that leave businesses vulnerable to assault are both capabilities that may be enabled by neural nets. (Gostev, 2012)

- *Intelligent Agents*

An intelligent agent (IA) is a self-sufficient organism that monitors its surroundings with the use of sensors, responds to its surroundings by employing actuators (thus the name "agent"), and focuses its actions with the ultimate aim of accomplishing certain objectives. To accomplish their objectives, intelligent agents may acquire new information or make use of existing information. They might be quite simple or extremely complex; one example of an intelligent agent is a reflex mechanism like a thermostat. They exhibit the following behaviors: responsiveness, pro-activeness, and a comprehension of the agent communication language. They are able to adjust to real-time situations, pick up new skills rapidly via engagement with their surroundings, and have the capacity to store and retrieve examples from memory. In order to defend against Distributed Denial of Service (DDoS) assaults, an intelligent agent is being created. The creation of a "cyber police" force that is equipped with mobile intelligent agents ought to be feasible in the event that there is a conflict involving legal or economic matters. Because of this, we need to put in place the infrastructure that will support the quality of the intelligent agents and their communication with one another. The use of multi-agent technologies, such as a hybrid multi-agent and Agent-based distributed intrusion detection, will provide the cyber police with a more comprehensive and effective operational appearance. (Raiu, 2012)

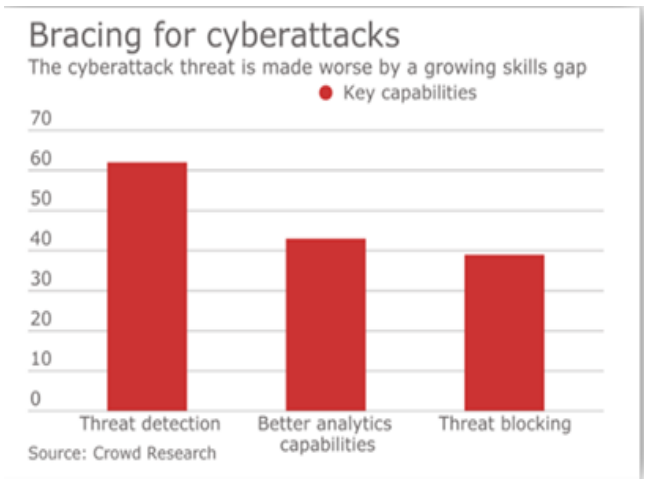

Fig 1 Cyber Attacks

ISSN No:-2456-2165

IV. HOW MAY AI CHANGE THE STATE OF CYBER DEFENCE

Companies are placing an unprecedented amount of emphasis on the need of cyber security right now. This is due to the fact that sophisticated cyber-attacks have resulted in data breaches that have cost businesses millions of dollars. The first step is to design a multi-layered security system that will be responsible for protecting the network infrastructure. Installing a firewall that will block unwanted network traffic is the first thing that has to be done.

After that, antivirus software is applied to the infrastructure in order to remove any dangerous files and viruses that may be there. Data is backed up on a consistent basis as part of their contingency strategy for handling emergencies. (Bockus, 2015)

Artificial intelligence has had an effect on network security by assisting experts in spotting anomalies in the network via the study of trends and the analysis of user behaviors. AI now makes it possible for security experts to analyses network data in order to identify weaknesses and thwart malicious attempts. The following are some of the ways that AI will assist to improve the conventional security approach:

- *Monitoring and responding to security incidents will be done with the help of cutting-edge security solutions driven by artificial intelligence.*
- *The most up-to-date firewalls will come equipped with machine learning technology that can instantly identify any deviation from the normal flow of network traffic and block it if it is deemed to be harmful.*
- *Professionals in the field of information security are able to determine the origin of a cyberattack by using the natural language processing function of AI. The use of natural language processing is also beneficial for doing vulnerability assessments.*
- *By conducting data searches throughout the internet and making use of predictive analysis, dangerous threats may be found ahead of time.*
- *Enhanced safety via the use of authentication and controlled access*

Biometric sign-in systems are an additional significant breakthrough brought about by artificial intelligence in the field of cyber security. The usage of fingerprints, retina scans, and palm prints are all components of these very safe login methods. (Alsmadi, 2019) Along with these fingerprints or other biometric data, you are also able to log in securely by using a password. This technology is utilized in businesses to allow workers to log in, and it is even integrated into certain smartphone operating systems.

Fig 2 AI in Cyber Security

- *Tools for Cybersecurity*

These days, businesses are also using machine learning, a kind of AI, to bolster the safety of their internal networks. Its primary use is assisting security professionals in identifying malicious assaults, but it also has the following uses:

	Preventive	Detective	Retrospective
Application	Application Static Security Testing, Web Scanners, Web Application Firewalls, Intrusion Detection Systems, Application Self Protection Technologies		Application Remediation
Network	Network Traffic Analysis, Firewalls/Next Generation Firewalls, Intrusion Prevention/Detection Systems, Secure Web, Gateways, Malware Analysis Platforms, Threat Intelligence	Security Information and Event Management, Intrusion Detection Systems, Security Analytics, Network Traffic Analysis, Honeypots, Payloads Analysis, Threat Intelligence	Network Forensics Tools, Security Orchestration Engine, Threat Intelligence
Endpoint	Host-based Intrusion Detection, Anti Virus, Anti spyware, Personal Firewalls, Application Control, Patch and Configuration Management, Containers, Data Loss Prevention, Mobile Device Management	Host-based Intrusion Detection, Malware Analysis	Endpoint Forensics
Cloud	Risk/Compliance, Data Discovery/Classification, Configuration Management, Anomaly Detection	Anomal/Intrusion Detection	Cloud Forensics

Fig 3 Framework for Cyber Security Tools

- *Protection for mobile endpoints*

Mobile endpoint security uses machine learning since smartphones, tablets, and laptops are all vulnerable to cyberattacks. Recently, Wandera released their MI: RIAM threat detection engine, which is driven by machine learning. This engine has found many samples of mobile-focused SLocker Ransomware that has been repackaged.

- *There are no known exploits with zero-day potential.*

To put it simply, a zero-day vulnerability is a kind of security risk for which no known workaround exists. A zero-day vulnerability is one that has been discovered by security researchers but has not yet been exploited by a malicious actor. Unprotected Internet of Things gadgets might occasionally harbor such dangers. (CRUZ LOBATO)

Algorithms trained with machine learning may spot zero-day threats by looking for unusual behavior in network data. Using machine learning, vulnerabilities are patched out and exploits are avoided.

➢ *Optimizing Analysis by Humans*

Vulnerability assessment, threat detection, network analysis, and endpoint security are all areas where human analysis may be supplemented by machine learning. Machine learning algorithms may identify potentially harmful information in a network and forward the results to a human security expert. Thus, there is potential for much improved warning detection rates.

➢ *Eliminating Human Error from Security Procedures*

With the use of machine learning, tedious security duties may be automated away. Working in this manner allows experts to better priorities tasks. Machine learning can automate a wide variety of tasks, including monitoring network traffic, blocking threats like ransomware, cleaning up infections, and analyzing network data. (Goyal & Rajput, 2020)

Machine learning may also be used to effectively allocate human security resources.

V. CONCLUSION

In light of the recent rise in malicious software and hacking attempts, the implementation of an intelligent security system has become essential. AI approaches are more adaptable and resilient when compared to contemporary cyber security solutions; as a result, they increase security execution and better guard systems from an expanding variety of sophisticated cyber threats. Despite the profound shift that AI has brought about in the field of cyber security, associated frameworks are not yet prepared to totally transform and, as a result, adapt to changes in their state. Although there are numerous advantages to using AI methods for cyber security, it is important to keep in mind that AI is not the sole solution to security problems. The intelligent security system will be rendered ineffective when it is attacked by a human adversary with the intention of circumventing it. This doesn't imply we shouldn't use AI approaches; nevertheless, we should be aware of the constraints they have. AI requires ongoing engagement and training from human beings. This combined strategy has shown success on numerous occasions, and it collaborates with security experts in an effective manner.

REFERENCES

[1]. Alsmadi, I. (2019). Cyber Security Management. The NICE Cyber Security Framework, 243–251. https://doi.org/10.1007/978-3-030-02360-7_10
[2]. Behavioural science in cyber security. (n.d.). Cyber Security: Law and Guidance. https://doi.org/10.5040/9781526505897.chapter-027
[3]. Bockus, N. F. (2015). Cyber in space: 2035. Advances in Information Security, 39–57
[4]. Bradbury, R. (2021). Educating for cyber (security). The Oxford Handbook of Cyber Security, 394–408. https://doi.org/10.1093/oxfordhb/9780198800682.013.24
[5]. CRUZ LOBATO, L. U. Í. S. A. (n.d.). Unraveling the cyber security market: The struggles among cyber security companies and the production of Cyber (in)security. https://doi.org/10.17771/pucrio.acad.27784
[6]. Cyber security 2019. (2019). 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). https://doi.org/10.1109 /cybersecpods.2019.8885065
[7]. Cyber security 2020 cover page. (2020). 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). https://doi.org/10.1109/cybersecurity49315.2020.9138881
[8]. Cyber security evolution. (2012). Cyber Security Policy Guidebook, 15–38. https://doi.org/10.1002/9781118241530.ch2
[9]. Cyber Security Objectives. (2012). Cyber Security Policy Guidebook, 39–67. https://doi.org/ 10.1002/9781118241530.ch3
[10]. Dunn Cavelty, M. (2018). 27. cyber-security. Contemporary Security Studies, 410–426. https://doi.org/10.1093/hepl/9780198804109.003.0027
[11]. Gostev, A. (2012). Cyber-threat evolution: The Year Ahead. Computer Fraud & Security, 2012(3), 9–12. https://doi.org/10.1016/s1361-3723(12)70052-0
[12]. Goyal, D., & Rajput, R. S. (2020). Cloud computing and security. The Evolution of Business in the Cyber Age, 293–319. https://doi.org/10.1201/9780429276484-12
[13]. Raiu, C. (2012). Cyber-threat evolution: The past year. Computer Fraud & Security, 2012(3), 5–8. https://doi.org/10.1016/s1361-3723(12)70051-9
[14]. Security and Trust in Cyber Space. (n.d.). Cyber Law and Cyber Security in Developing and Emerging Economies. https://doi.org/10.4337/9781849803380.00005