ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

Ms. Krutika Bane	**Ms. Sheetal Mahajan**	**Dr. Jayalekshmi K.R.**
Student, Sterling Institute of Management Studies, Nerul, Navi Mumbai	Student, Sterling Institute of Management Studies, Nerul, Navi Mumbai	Assistant Professor, Sterling Institute of Management Studies, Nerul, Navi Mumbai
banekrutika1@gmail.com	sheetalmahajan208@gmail. com	jayalekshmikr@ncrdsims. edu.in

ABSTRACT

With the age of digital technology, cyber security has grown to be a big worry. Data breaches, identity theft, captcha cracking, and other similar issues frequently affect millions of people as well as corporations. Inventing the proper rules and processes and putting them into practice with exacting perfection to combat cyberattacks and crimes has always been a struggle. Recent advances in artificial intelligence have significantly increased the risk of cyberattacks and other crimes. It has been used in practically all branches of engineering and research. AI has sparked a revolution in fields like robotics and healthcare.

Cybercriminals were unable to avoid this ball of fire, and as a result, "ordinary" cyberattacks have evolved into "intelligent" ones. Researchers began to have very high expectations for AI research in the 1960s and 1970s, but they pretty much went in vain without any major discoveries. Artificial intelligence is the branch of science that seeks to comprehend and simulate human intelligence. Many researchers have their own interpretations of AI, citing works like Artificial Intelligence: A Contemporary Perspective by Peter Norvig and Stuart Russell as an example. "The study of agents that exist in the environment, perceive, and act" is the definition of artificial intelligence. For many years, researchers have worked to develop systems that think, learn, and act like humans. We'll go over some of the key strategies for AI that have advanced the field's understanding (Russell, S., J., & Norvig, P., 2000).

Keywords: *Cybersecurity, artificial intelligence, Intelligent Agents, Cyber Security, Neural Nets, Expert Systems, cyber-attacks.*

1. INTRODUCTION

The number of cyberattacks has greatly increased as a result of the exponential growth of computer networks. Your sensitive digital data is more at risk from cyber or online attacks as hackers are constantly seeking for new ways to penetrate security. In reality, they use social engineering techniques and artificial intelligence to go beyond recognised internet security standards. Any type of data can be shielded from injury or theft via cybersecurity. This category includes sensitive data, protected health information, industrial and governmental data, as well as personal and intellectual property, among many other things. An important component that uses automation to boost an organization's output and efficiency is artificial intelligence (AI).

As a result of the digital revolution, AI has emerged as one of the most crucial tactics for thwarting cyberattacks. Data trends can be identified by cyber AI, which also enables security systems to make informed decisions. Also, by applying AI and machine learning techniques, businesses may reduce short response times and enhance security measures.

2. LITERATURE REVIEW

The use of artificial intelligence (AI) in cybersecurity is gaining in value for its ability to identify and respond to cyber threats in real time, improving security measures. A brief introduction to AI in cybersecurity:

Javed, K., Gani, A., & Qureshi, K. N., Yang, Q. and Chen, H. (2019). Intelligent network security protection systems based on machine learning algorithms. The report introduces an intelligent network defense system that uses machine learning algorithms to identify and respond to network threats.Gharibi, W., Medjahed, B.and Boukelif, A. (2019). Review of artificial intelligence technologies for cybersecurity. This article reviews recent research on the use of artificial intelligence in cybersecurity. Hussain, M. Abbas, H. and Mirza F. (2019).

a) **Identifying Emerging Threats:** Artificial Intelligence is being used to detect cyber risks and potentially malicious activities. This is an area where artificial intelligence can really help. Because traditional software systems cannot handle the flood of new viruses created every week. It is an artificial intelligence system designed to detect malware, perform predictive modeling, and use sophisticated algorithms to detect even the smallest malware or ransomware attacks before they penetrate your system.

b) **Battling Bots:** Bots now make up the majority of internet traffic and can be dangerous. Bots can pose a real threat, from account takeover and password theft to fake accounts and data theft. Manual responses alone cannot defeat automated threats. AI and machine learning can help you gain a deeper knowledge of your website traffic and differentiate good bots (e.g. search engine crawlers) from bad bots and people

c) **Breach Risk Prediction:** The AI system helped determine the IT Asset Inventory, a complete and accurate inventory of all devices, users and applications with varying degrees of access to various systems. In today's environment, AI-based systems can predict how and when they are likely to be hacked in terms of corporate governance and threat exposure (as described above), and can therefore plan and direct resources to the most vulnerable areas

d) **Better Endpoint Protection:** The number of remote work devices is growing rapidly, and AI can help protect them all. Antivirus software and Virtual Private Networks (VPNs) can help prevent malware and virus attacks from afar, but they often rely on signatures. This means that the definition of signatures must be followed in order to stay safe from recent threats [9]. If the virus definitions are mostly behind , this could be a problem because the antivirus solution has not been updated or the software vendor has not realized

e) **How Is Artificial Intelligence Trained for Cybersecurity?** When cybercriminals attempt to gain access to internal systems, they leave digital traces known as intrusion signatures. Security experts generate large fingerprinting datasets that help identify specific vulnerabilities and attacker habits for further exploitation. If sufficient fingerprint and intrusion pattern libraries are available, AI systems can be trained to detect intruders in real time.

3. PROBLEM DEFINITION

This paper's primary goal is to investigate how artificial intelligence functions in cybersecurity. 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. Hackers have become more skilled, despite the fact that the initial motivations for attacks have largely stayed stable over time . After certain types of attacks take place, established approaches to cybersecurity issues typically defend consumers against assaults. The latest cyberattacks' patterns are also prone to change, which adds to their unpredictability.

Machine learning, on the other hand, is becoming more popular as a cutting-edge method for identifying infiltration. The management and prioritisation of the numerous new vulnerabilities that are released every day is difficult for businesses. Traditional approaches for managing vulnerabilities only respond to incidents after the vulnerability has been exploited.

4. OBJECTIVE

The paper's goal is to lower the risk of cyberattacks and safeguard against illegal use of systems, networks, and technology. In the event of cyberattacks, traditional security measures are insufficient to prevent data leaks. Thankfully, artificial intelligence (AI) technology have been applied to the creation of intelligent models for securing systems against attackers.

Technology is advancing quickly, and artificial intelligence has demonstrated encouraging outcomes in cyber security by analysing data and making decisions. This study demonstrates an AI technique that is applied in a number of ways in the fight against cyberattacks. Some of the primary advantages of employing AI in cyber security are as follows:

- Better threat identification and prevention: AI can instantly scan huge volumes of data to find patterns that might point to a threat. This may make things quicker and more precise.
- Improved efficiency: AI can automate many of the duties associated with cyber security, including as analysing network traffic and discovering weaknesses in systems. This will improve the detection of attacks and allow for more timely and effective responses. This can free up human cyber security specialists to concentrate on harder problems and work faster.
- Constant learning and adaptation: AI algorithms are an effective tool for continuously enhancing cyber security because they can learn from previous attacks and adapt to new threats.
- Improved data analysis: AI can look at a lot of data to find trends and forecast. It is a useful tool for threat intelligence since it anticipates potential dangers. Better fraud detection: AI can spot fraudulent activities by analysing trends in data, such as transactions and user behaviour.

5. RESEARCH METHODOLOGY

The research methodology had the objective of selecting and using an artificial intelligence techniques in cyber security which uses to detection and make it possible to respond to anonymous threats before spreading itself. Some of the techniques are:-

a) Expert Systems:

An expert system is a computer system that reproduces human decision-making abilities. This is the best example of a knowledge base system. These knowledge base systems consist of two subsystems: the knowledge base and the inference engine. The knowledge base is illustrations and real statements. An inference engine is an automated inference system. Evaluate the current state of the knowledge base, apply appropriate rules, and validate new knowledge.

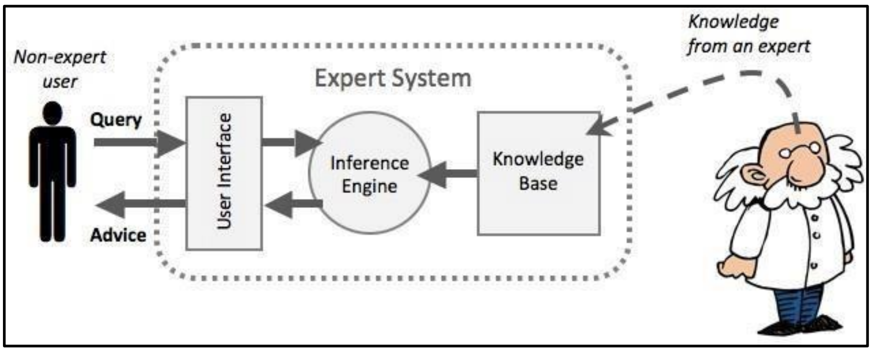

Figure1: Expert System (Source:https://sites.google.com/site/mrstevensonstechclassroom/hl-topics-only/4a-roboticsai/5-expert-systems)

b) Security Expert System:-

The security expert system follows a set of rules to fight against network attacks. It uses the knowledge base to check if the process is a well-known process, then the security system ignores the otherwise the system kills the process . If there is no such process in the knowledge base, the expert system finds the state of the machine using the inference engine algorithm (set of rules) . The state of the machine is compiled into three states, which are safe, moderate, and severe. Based on the state of the machine, the system alerts the administrator or the user of the state and then provides the inferred to the knowledge base.

c) Neural Nets:-

Neural networks are also defined as deep learning. This is the advanced branch of AI. Inspired by how the human brain works and how it works. Our brain contains many neurons, mostly general purpose and region independent. You can learn from any type of data. In 1957, Frank Rosenblatt created artificial neurons (perceptrons), paving the way for neural networks. This perceptron can learn and solve the absorption problem by combining with other neurons, i.e. the perceptron. Perceptrons learn by themselves to recognize the entities on which they are trained by learning and processing high level raw data just as our brains learn on their own from raw data using our sensory inputs.When we apply this type of deep (trained) learning to cybersecurity, systems can identify whether a file is malicious or legitimate without human intervention. The technique produced strong results in detecting malicious threats compared to conventional machine learning systems.The rapidity of neural networks' ascent in cybersecurity is the reason. Forcing the use of hardware or GPU will speed things up. Neural networks can accurately detect new malware and patch dangerous vulnerabilities that leave organizations vulnerable.

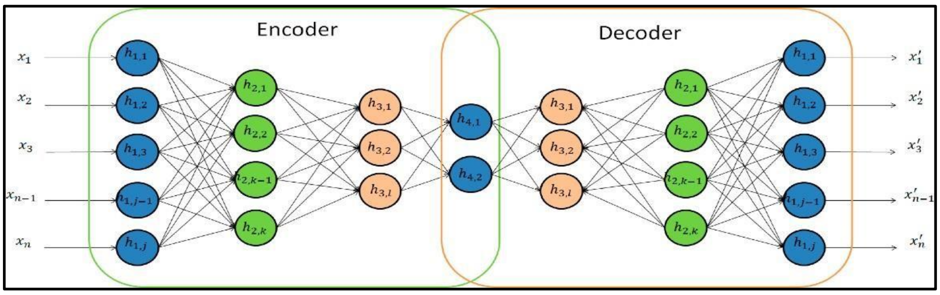

Figure2: Neural nets for cyber security (Source: https://www.mdpi.com/2078-2489/10/4/122)

d) Intelligent Agents:-

An intelligent agent (AI) is an autonomous agent that detects motion through sensors and uses actuators (i.e. it is an agent) to sense the environment and direct its actions to achieve goals." An intelligent agent can also learn or use knowledge Libraries come to to achieve their goals. For example, "The reflex mechanism, a thermostat, is an intelligent agent. It has behaviours such as understanding the agent's interaction language, proactivity, and reactivity. They can adapt in real time, and easily learns new information by engaging with the world, and has standard retrieval and memory-focused retrieval skills.

Intelligent agents can also learn or use knowledge bases to achieve their goals. A reflector, for example, the Thermostat is an intelligent agent. Ability to understand agent interaction language, initiative and responsiveness, and other behaviors. They can adapt in real time, learn new things quickly 4044 by communicating with the environment, and have standard memory-based storage and retrieval capabilities.

Smart proxies were created to combat Distributed Denial of Service (DDoS) attacks. If there are any legitimate or business concerns, the development of a "cyber police" should be manageable. A must-have mobile intelligence agent for internet police. For this, we need to adapt the infrastructure to support the interaction between quality agents and intelligent agents. Multi- agent tools will give the cyber police a very complete visibility on operations.

6. ADVANTAGES OF AI TECHNIQUES

A. Expert Systems:

- Decision Support
- Intrusion Detection
- Knowledge Base
- Inference Engines

B. Neural Nets:

- Intrusion Detection and Prevention System
- High Speed Operation -DoS Detection
- Forensic Investigation

C. Intelligent Agents

- Proactive
- Agent Communication Language
- Reactive
- Mobility
- Protection against DDoS

7. ANALYSIS FINDING

AI is used for finding cyber threats and malicious activities. Traditional software systems cannot keep pace with the sheer number of new malware created every week, so this is an area where AI can really help with.

Artificial intelligence (AI) enables superior predictive intelligence with natural language processing that automatically organises data by gathering information from articles, news, and research on cyber dangers.

While using sophisticated algorithms, Artificial Intelligence systems are being trained for detecting malware, run pattern recognition, and detecting even the small and minute behaviour of malware or ransomware attacks before it enters into the system.

Bots is making a huge chunk of internet traffic today, and they can be dangerous. You will not able to tackle automated threats with manual response. AI and machine learning help build a detailed understanding of website traffic and distinguish between good bots and bad bots, and humans. AI enables us to analyze a huge amount of data and allows teams of cyber security to adapt their strategy to a continually altering landscape.

AI helps define IT asset inventory. It is an accurate and detailed record or information about all devices, users and applications with different levels of access to different systems.AI powered systems can predict where and how they are most vulnerable, so they can plan and allocate resources according to areas of greatest vulnerability.

8. LIMITATION

AI in cybersecurity is used as a security from threats or as a attacker. AI-based security systems are used to protect against the cyber threats malware etc. such that Attacker can also utilize the AI technology for conduction malicious activities to harm others system such as phishing attacks and fraud. There are certain risk while using AI in cybersecurity and it hard to control and manage that.

- Cybercriminal can purchase AI System for creating more advanced attacks. They can utilize the AI and ML for launching more advance attacks .
- Attacker can create a identical website or fake website which looks same to a legitimate one and they can able to trick the AI based security in thinking that it is the real one .
- AI systems are not always perfect they can make mistakes as well this means AI can generate false positives which happens when system incorrectly flags an activity as a malicious. This happens when there is an incorrect data labelling and overfitting of training data.
- AI can be biased sometimes means the data or results can be skewed on training data It means that If the training data is biased then the AI also will be biased which lead to false negatives.

- Even if AI is introduce in business that doesn’t mean that you are now protected from all other threats. Viruses and malware improves and updates all the time so even AI need to be redesign, Updated and maintenance.

9. CONCLUSION

A Startup company or a big company faces a huge traffic daily as there are a lot of activity that are happening on daily basis in organization. A Lot of data is being transferred daily between the servers and customers thus the data which is being transferred has to be protected from attackers or hackers so that they will not able to read the data and tamper with this data which leads to damage to company .It is impossible for cyber security to detect all the threats AI has become highest priority for all the IT company as it improves the performance of security. It provides good understanding of computer networks.AI analyze the data and identifies the threats which is useful for security experts to increase the security and limit breach risks. AI focuses on risks and before the malware comes in picture it identifies it .Hence AI will be useful for organization to assist them for more powerful security .

10. REFERENCES

[1] https://www.upgrad.com/blog/artificial-intelligence-in-cyber-security/

[2] https://www.computer.org/publications/tech-news/trends/the-impact-of-ai-on-cybersecurity

[3] https://www.weforum.org/agenda/2021/06/4-ways-ai-new-age-of-cybersecurity/

[4] https://www.ibm.com/security/artificial-intelligence

[5] C. Tschider, "Regulating the IoT: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age", SSRN Electronic Journal, 2018

[6] https://www.forbes.com/sites/forbetechcouncil/2023/03/15/why-artificial-intelligence-isbetting-a-cybersecurity-imperative-and-how-to-implement-it/?sh=66a26f82610d

[7] https://www.cnbc.com/2022/09/13/ai-has-bigger-role-in-cybersecurity-but-hackers-may-benefit-the-most.html

[8] https://www.boozallen.com/s/insight/publication/role-of-artificial-intelligence-in-cyber-security.html

[9] https://www.techtarget.com/searchdatacenter/delltechnologies/Industry-Transformation-

[10] N. Bakar and A. Selamat, "Agent systems verification: systematic literature review and mapping", Applied Intelligence, vol. 48, no. 5, pp. 1251-1274, 2018

[11] Kamtam, A., Kamar, A., &amp; Patkar, W. K. (2016). AI approach information security. International Journal of the Latest Innovations in Computing and communication