Artificial Intelligence in Cybersecurity

Shivali Bhagat

Abstract-

Cyber security has become a major concern in the digital era. Data breaches, ID theft, cracking the captcha, and other such stories abound, affecting millions of individuals as well as organizations. The challenges have always been endless in inventing right controls and procedures and implementing them with acute perfection for tackling with cyber-attacks and crimes. The ever-increasing risk of cyber-attacks and crimes grew exponentially with recent advancements in artificial intelligence. It has been applied in almost every field of sciences and engineering. From healthcare to robotics, AI has created a revolution. This ball of fire couldn't be kept away from cyber criminals, and thus, the "usual" cyber-attacks have now become "intelligent" cyber-attacks.

Artificial intelligence (AI) is one of the key technologies of the Fourth Industrial Revolution (or Industry 4.0), which can be used for the protection of Internet-connected systems from cyber threats, attacks, damage, or unauthorized access. To intelligently solve today's various cybersecurity issues, popular AI techniques involving machine learning and deep learning methods, the concept of natural language processing, knowledge representation and reasoning, as well as the concept of knowledge or rule-based expert systems modelling can be used.

Keywords-Cybersecurity, Malware, Artificial Intelligence, Main Cybersecurity threats, cyber-attacks

I. Introduction

With the click of a button, today's man can send or receive any information, whether it's an e-mail, an audio or video file, but has he ever pondered how securely his data is delivered and then sent to another person without any information leaked?? The solution is cyber security. The Internet is the fastest-growing infrastructure in today's world. In today's technological environment, many new technologies are changing the face of humanity. However, because of this new technology, we are unable to protect our personal information as effectively as we would like, and as a result, cybercrime is on the rise. The scope of cyber security extends beyond securing information in the IT business to include a variety of other domains such as cyberspace. Because more than 60% of all commercial transactions are now conducted online, this area necessitated a high level of security to ensure transparent and efficient transactions. As a result, cyber security has become a hot topic.

The use of technology, procedures, and policies to safeguard systems, networks, programmes, gadgets, and information from cyberattacks is referred to as cyber security. Its goal is to limit the risk of cyber-attacks by preventing unauthorised access to systems, networks, and technology. The modern world depends more on technology than ever before. A huge amount of data is generated and gathered with the large implementation of booming technologies such as the Internet of Things (IoT) and cloud computing Although data can be used to better serve the corresponding business needs, cyber-attacks often pose major challenges. A cyber-attack is usually a malicious and concerted attempt by an individual or organization to breach another individual or organization's information system. Malware attack, ransomware, denial of service (DoS), phishing or social engineering, SQL injection attack, Man-in-the-middle, Zero-day exploit, or insider threats are common nowadays in the area. These types of security incidents or cybercrime can affect organizations and individuals, cause disruptions, as well as devastating financial losses. Therefore, to effectively and intelligently protect an information system, particularly, Internet-connected systems from various cyber-threats, attacks, damage, or unauthorized access, is a key issue to be solved urgently, in which we are interested in this paper.

II. Overview of Artificial Intelligence

Artificial Intelligence is a way of making a computer, a computer-controlled robot, or a software think intelligently, in the similar manner the intelligent humans think. AI is accomplished by studying how human brain thinks, and how humans learn, decide,
and work while trying to solve a problem, and then using the outcomes of this study as a basis of developing intelligent software and systems. Intelligence is commonly considered as the ability to collect knowledge and reason about knowledge to solve complex problems. In the near future intelligent machines will replace human capabilities in many areas. Artificial Intelligence is the study and developments of intelligent machines and software that can reason, learn, gather knowledge, communicate, manipulate and perceive the objects.

III. Exposure of AI in cybersecurity:

Machine learning and Artificial Intelligence (AI) are being connected more comprehensively crosswise over enterprises and applications than any other time in recent memory as registering power, information accumulation and capacity abilities increment. This tremendous trove of information is significant grub for AI, which can process and examine everything caught to see new patterns and subtle elements. For cyber security, this implies new endeavours and shortcomings can rapidly be recognized and investigated to help moderate further assaults. It can take a portion of the weight off human security "partners." They are cautioned when an activity is required, yet in addition can invest their energy taking a shot at more inventive, productive undertakings. A helpful relationship is to consider the best security proficient in your association. In the event that you utilize this star representative to prepare your machine learning and Artificial Intelligence programs, the AI will be as shrewd as your star worker. Presently, in the event that you set aside the opportunity to prepare your machine learning and Artificial Intelligence programs with your 10 best representatives, the result will be an answer that is as savvy as your 10 best workers set up together. Furthermore, AI never takes a wiped-out day.

IV. Usage of AI in cybersecurity

The use of Artificial Intelligence (AI) is already being used to, or is being actively explored for, some of the following areas in cyber security solutions: To identify and prevent undesirable spam and fraudulent emails, Gmail makes use of Artificial Intelligence (AI). Gmail's Artificial Intelligence was taught by the millions of current Gmail users - every time users click an email message or not spam, you are assisting in training the AI to detect spam in the future. As a result, Artificial Intelligence has progressed to the point where it can identify even the most subtle spam emails that attempt to pass unnoticed as "frequent" emails.

- Fraud detection: An Artificial Intelligence-based fraud detection system that employs algorithms based on expected consumer habits to identify fraudulent transactions through MasterCard deployed Decision Intelligence. It examines the customer's normal purchasing patterns, the seller, the location of the transaction, and many other complex algorithms to determine if a purchase is unusual.
- Botnet Detection: A very complicated area, botnet detection is usually based on pattern recognition and timing analysis of proxy servers.

Since botnets are usually managed by a master script of instructions, a wide-scale botnet assault will usually include a large number of "users" all making the identical queries on a site in a single attack. This may include unsuccessful login attempts (a botnet brute force password attack), networks vulnerability scans, and other breaches. It is very difficult to explain the incredibly complicated function that Artificial Intelligence plays in botnet identification in just a few words, but here is a fantastic study article on the subject that does a great job. These are just a handful of the areas in which Artificial Intelligence has been used for cyber security. There are currently a large number of research articles that provide compelling data in support of Artificial Intelligence's effectiveness in the field of cyber security. According to the majority of study studies, the success rate for identifying cyber assaults is between 85 and 99 percent. One Artificial Intelligence development firm, Dark Trace, claims to have a 99 percent success rate and already has thousands of clients across the world.

V. Advantages of using AI in cybersecurity

A review on the advantages of Artificial Intelligence in the field of cyber security reveals that institutions that implemented AI in cyber security realize significant benefits. This is evident as ROI of two out of three organizations increased on cyber security tools. For example, Siemens AG, leader of Global electrification, automation, and digitalization used Amazon Web Services (AWS) to create AI based, high speed, self-controlled, and extremely elastic platform for its Siemens Cyber Défense Centre (CDC). The AI deployed was able to estimate 60,000 potential assaults per unit time. As a result of the AI deployed, this capability was managed with a team consisting of less than dozen members without any negative impact on system performance. Employing AI in cyber security permit institutions to comprehend and reapply prior threat patterns in identification of novel threats. This results to preservation of time and effort in identifying and investigating incidents, and remediate threats. About 64% of administrators reveal that AI cut down the cost to identify and react to breaches. Fast response is essential in evading cyberattacks. Cost reduction for organizations is within an average of 12%. AI offers opportunities for cyber security largely because the cyber security landscape is rapidly moving from identification, manual response and mitigation towards automated mitigation. AI can identify novel and complex modifications in attack extensibility.

VI. Disadvantage of AI in Cybersecurity:

1) Cost effectiveness: Sometimes the cost of using AI services exceeds the limit, so everyone is not able to take its advantages.
2) Cyber threats: Your data and privacy now a days is too vulnerable to attacks by hackers. They can easily track your location and hack your private data if preventive measures are not taken.
3) Machine gaining control over humans: It's the oldest concern over AI. This concern has been depicted in many movies' books before. Steps must be taken to prevent this from happening.
4) Loss of jobs: Artificial Intelligence is considered as a threat as some studies are predicting that a big slice of the workforce is going to lose their jobs and replaced by Artificial Intelligence applications and machinery.
5) Not everyone is familiar with AI: Not everyone wants to work with new modern-day technologies and is willing to understand it.

VII. Conclusion:

So, in this paper we saw the importance of Artificial Intelligence in cyber security and the various problems that come along with it and how they can be minimized. Though there are some drawbacks, but still Artificial Intelligence plays a significant role in cyber security. For overcoming the drawbacks, Artificial Intelligence will assist to advance cyber security.

VIII. References:

[1] Ravi Sharma Study of Latest Emerging Trends on Cyber Security and its challenges to Society International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1ISSN 2229-5518.

[2] https://cyware.com/category/internet-cyber-security-threats

[3] https://www.embroker.com/blog/top-10-cybersecurity-threats-2022/

[4] A. Cardenas, T. Roosta, G. Taban, S. Sastry **Cyber security basic defenses and attack trends** Fujitsu Lab. http://www.flacp.fujitsulabs.com/~cardenas/Papers/Chap4v2.pdf

[5] https://www.sciencedirect.com/science/article/pii/S0022000014000178

[6] https://www.aura.com/learn/emerging-cyber-threats

[7] MdLiakat Ali Kutub Thakur Beatrice Atobatele Challenges of Cyber Security and the Emerging Trends BSCI’19, July 8, 2019, Auckland, New Zealand

[8] VeenooUpadhyay, SuryakantYadav Study of Cyber Security Challenges Its Emerging Trends: Current Technologies International Journal of Engineering Research and Management (IJERM) ISSN: 2349- 2058, Volume-05, Issue-07, July 2018

[9] Jagadeeshwar Podishetti and Kadapala Anjaiah, “Role of Artificial Intelligence in Cyber Security”, International Journal of Research in Advanced Computer Science Engineering, Volume No:3, Issue No:3 (August-2017), ISSN No : 2454-423X (Online).

[10] Ishaq Azhar Mohammed, “ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY: A SYSTEMATIC MAPPING OF LITERATURE”, INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT], VOLUME 7, ISSUE 9, Sep.-2020, ISSN: 2394-3696.

[11]https://www.researchgate.net/publication/330569376_The_Role_of_Artificial_Intelligence_in_Cyber_Security.

[12] https://iopscience.iop.org/article/10.1088/1742-6596/1964/4