Impact of Artificial Intelligence in Cyber security

[1]M.Geetha and [2]B.Jeyalakshmi

[1]*Assistant Professor, Department of Information Technology, V.H.N Senthikumara Nadar College (Autonomous), Virudhunagar, Tamilnadu, India*

E-mail: geetha@vhnsnc.edu.in

[2]*Assistant Professor, Department of Information Technology, V.H.N Senthikumara Nadar College (Autonomous), Virudhunagar, Tamilnadu, India*

E-mail: jeyalakshmi@vhnsnc.edu.in

Abstract

The relationship between artificial intelligence systems and cyber security is the focus of this research. Data protection against cyber-attacks is critical in today's data-driven environment. While protecting networks, software, and hardware has been the main focus of traditional cyber security measures, the quickly changing threat landscape has overtaken these traditional approaches. In the face of contemporary cyberthreats, traditional algorithms and defensive strategies have proven inadequate. Artificial intelligence (AI) has consequently become a potent instrument for improving cyber security. Organizations are constantly looking for innovative ways to protect their sensitive data and systems in the modern world due to the rise in sophisticated cyberattacks. AI has emerged as a promising answer to this issue since it can automate cyber security operations, detect and resolve threats instantaneously, and provide insights into potential vulnerabilities. The several technologies that augment artificial intelligence (AI) to improve cyber security are examined in this essay, along with the overall impacts, capabilities, applications, benefits, and challenges of AI in cyber security.

Keywords: Artificial Intelligence, Cybersecurity, Attacks

Introduction

Since everything is digital in today's cyber world, data is king. Never before has data security been so important, particularly when it comes to sensitive or private data. Hackers are becoming more sophisticated every day and use more inventive techniques to exploit data, governments, and weaker businesses. Nearly every day, new cyberattacks, data bridges, data breaches, hacker attacks, crashes, and data poisoning are found. Cyberattacks have been ranked as one of the top five most likely global causes of hazard. Both the complexity of network attacks and the cunning of fraudsters are growing every day [1].Cybersecurity is a set of technology, processes, and practices that protects networks, devices, software, and data from harm, attack, and illegal access [2]. Concern over cybersecurity is growing across all industries and sizes of organizations [3]. The ever-growing and evolving cyber security threat that multinational organizations confront can be mitigated by integrating artificial intelligence into cyber security systems [4].

Role of AI in cyber Security

Artificial Intelligence

The 21st century is seeing a growing trend toward Artificial Intelligence (AI) across a variety of application sectors due to technical breakthroughs and the spread of automation systems. The goal of computer science's artificial intelligence (AI) field is to build machines that can carry out tasks that normally call for human intelligence. Reasoning, learning, problem-solving, perception, and language comprehension are some of these tasks.[5].The contribution of AI is both enormous and noteworthy. Because to AI's capacity for learning, reasoning, and perception, society now has access to a wide range of extremely advanced tools that have completely changed the way humans function and view the world. But in addition to these encouraging advancements, AI has brought with it a fresh set of difficulties and risks, especially in the area of cybersecurity.[6]

AI in Cybersecurity

The practice of defending programs, networks, and systems from online threats is known as cybersecurity. In the context of cyber security, artificial intelligence (AI) refers to intelligent computing systems that are intended to recognize, stop, and lessen threats and attacks in a cyber environment. These cyberattacks typically target sensitive data in order to access, alter, or destroy it.By identifying intricate data patterns, offering practical suggestions, and facilitating autonomous mitigation, artificial intelligence (AI) in cybersecurity helps security professionals. It facilitates decision-making, expedites incident response, and improves threat detection.

Uses of AI in Cybersecurity

Enhanced Threat Detection & Analysis

Artificial intelligence (AI) systems can evaluate massive amounts of data from several sources in real-time and find patterns and abnormalities to indicate potential cyberthreats. Machine learning algorithms will be able to continuously learn new data to improve the accuracy of detection and track the dynamic evolution of cyberthreats. Threat intelligence platforms with AI capabilities can be used to extract various conclusions from many sources, ultimately providing a comprehensive and current risk picture.

Automated Incident Response (AIR)

By automating incident triage and response, artificial intelligence (AI) can expedite an early reaction to security vulnerabilities. Additionally, AI may extend the protective windows by enabling quicker threat detection and repair. When functioning, AI systems can consider the necessity and parametricity of the alerts thanks to machine learning. This could let the staff focus on the issues that require more engagement by relieving them of the pressure of evaluating hundreds of notifications.AI-powered incident response systems can be made to work in tandem with other software programs to enforce rules throughout the whole IT infrastructure of the company.[7]

Improved Security Risk Assessment

Deep intelligence-based analysis of the entire IT structure, applications, and data can be made possible by AI technology. After that, details regarding every possible security risk and weakness are given. Security managers can determine the likelihood and degree of effect of potential security instances by using the advanced analytics provided by machine learning algorithms. The businesses will be able to concentrate their mitigation efforts on the most important instances as a result.By collecting historical data and adopting industry best practices as their paradigm, AI-embedded risk detection solutions provide practical advice for improving security.

Analytics of User Behavior (UBA)

Artificial intelligence (AI) algorithms can monitor user behavior based on usage patterns, revealing any unusual activity that deviates from normal use and could indicate an insider threat or unauthorized access. Algorithms using artificial intelligence are able to recognize anomalies in behavior related to locales, lambda times, and access manners in a variety of contexts.Through auditing systems, UBA services enable businesses to find any irregularities regarding employee knowledge access, hence lowering the risk of insider threats and data breaches.

Malware Identification and Avoidance

AI-powered malware scan systems are able to accurately identify malware by matching patterns in a file, including its properties and actions. Machine learning algorithms can identify patterns in previously undetected malware variants and their traits and behaviors that they may share with known malware threats by observing and analyzing a variety of malware samples.In order to stop malware from spreading throughout the network, AI-based Watch Point solutions have the ability to quarantine various endpoint types or automatically fix them when they detect infection.

Identification of Phishing and Email Scams

Artificial intelligence (AI) systems can accurately identify phishing and email fraud efforts by analyzing email contents, sender activity, and other metadata. In order to qualify a message as a phishing assault, the most recent machine learning algorithms are able to detect hidden indicators such as the phony sender, attachments, or domain names mentioned in the emails.The amount of successful phishing attempts is significantly decreased by AI-based email security solutions' integrated blocking and quarantining sophisticated systems, which stop users from viewing illicit phishing emails.

Patch Prioritization and Vulnerability Management

AI aids in determining the likelihood of an exploitation site and how serious it is for the company's safety posture. Machine learning development algorithms can be utilized to analyze threat intelligence feeds and historical data to identify a group of the most significant vulnerabilities that require quick attention. An AI-powered vulnerability management and patching solution can monitor vulnerabilities and streamline the patching process byPatch management for important applications can be automated by AI-powered vulnerability management platforms according to your priority schedule. Your exposure window for known vulnerabilities will be shortened as a result.[8]

An opportunities of AI in cybersecurity

It is obvious that traditional security methods cannot shield businesses from the sophisticated cyberattacks of today. As a result, numerous artificial intelligence (AI) solutions are being developed to aid in cyber security. We look at some of the most innovative applications of AI in cyber security here. Artificial intelligence (AI) is a rapidly evolving field of technology that has the potential to drastically alter a variety of industries, including cyber security, as everyone is aware. Businesses can use AI to help identify attacks and respond to them more quickly and effectively if its internal cyber security personnel have received advanced level cyber security training. Additionally, AI may be used to automate a number of cyber security-related tasks, such as incident response and malware analysis. Other potential include threat detection and response. One of the key benefits of using AI in cyber security is its capacity to instantly evaluate enormous amounts of data in order to identify trends and anomalies that might indicate a cyberattack.[9]

Limitations and Drawbacks of AI Use in Cybersecurity

Some of the drawbacks of AI technology keep it from being a widely used security tool.

- Resources: Data, memory, and processing power are just a few of the many resources that businesses require.
- Data sets: To train the AI system, security firms must use a variety of data sets containing abnormalities and malware codes. Some businesses cannot afford the time and resources needed to obtain correct data sets.
- AI is also used by hackers to develop and enhance their malware. Because AI-based malware may learn from existing AI tools to create increasingly sophisticated attacks, it can be quite harmful.
- Neutral fuzzing: This technique tests a lot of random input data to find software flaws. Neural fuzzing and neural networks can be used by a threat actor to learn about a target software or system and identify its vulnerabilities.

AI's role in cybersecurity in the future

AI in cybersecurity has a promising future. We may anticipate significantly more advanced threat identification, automated incident response, and predictive capabilities as AI technology develops further. In order to secure future smart cities and networked gadgets, artificial intelligence is probably going to be essential. However, to guarantee appropriate and successful AI application in protecting our digital environment, ethical issues pertaining to data privacy, bias, and human oversight will need to be addressed.

Conclusion

AI's impact on people's lives will only grow as more technology is integrated into daily life. While some scientists believe AI has a negative impact on technology, others believe it may greatly improve our lives. This study covered the importance of artificial intelligence in cyber security, the various problems that can occur, and how to address them.

Artificial intelligence is still crucial for cyber security in spite of its drawbacks. To combat these drawbacks, artificial intelligence will contribute to improved cyber security.

References

Artificial Intelligence in Cyber Security, S. Dandge, U. I. Dawre, R. F. Shirshikar, Volume 44 Issue S-8 Year 2023, ISSN: 0253-7214

Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions, Ramanpreet Kaur, Tomaz Klobucar, April 2023.

Yeruva, A. R., Choudhari, P., Shrivastava, A., Verma, D., Shaw, S., & Rana, A. (2022). Covid-19 Disease Detection using Chest X-Ray Images by Means of CNN. 2022 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS), 625–631.

Artificial Intelligence in Cyber Security - A Review Jenis Nilkanth Welukar, Gagan Prashant Bajoria,Article Info Volume 8, Issue 6 Page Number : 488-491 Publication Issue November-December-2021 Article History Accepted : 15 Dec 2021 Published : 30 Dec 2021

The impact of ai on cyber security - Yousef Al-Alwan, Al-Hussein Bin Article · October 2024.

The Ethical Challenges of “Locked” Versus “Continuously Learning” and “Autonomous” Versus “Assistive” AI Tools in Healthcare, The American Journal of Bioethics, Youssef, A., Abramoff, M., and Char, D. ,2023.

eHealth Cloud Security Challenges: A Survey,” Journal of Healthcare Engineering, Y. Al-Issa, M. A. Ottom, and A. Tamrawi, “, vol. 2019, no. 7516035, Sep. 2019.

A survey on security challenges in cloud computing: issues, threats, and solutions, The Journal of Super computing, Tabrizchi and M. K. Rafsanjani, vol. 76, no. 12, pp. 9493–9532, Feb. 2020.

"Explainable Artificial Intelligence in CyberSecurity: A Survey. "Capuano, Nicola, et al. IEEE Access 10 (2022): 93575-93600