International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Artificial Intelligence in Cyber Security-Review

Dr.Jasmin Bhootwala

Veer Narmad South Gujarat University,Surat

ABSTRACT

In this paper, we will look at how Artificial Intelligence (AI) can be used to address cyber security concerns and threats. Since the last decade, cyber security has grown exponentially. As a result, the number of applications and threats is steadily increasing. This study discusses the applications of artificial intelligence in cyber security and sheds some insight on the drawbacks.

Keywords: Artificial Intelligence, Cyber Security, Cyber-threats, Block chain

1. INTRODUCTION

The incorporation of Artificial Intelligence into cyber security systems can help reduce the daily rising and evolving cyber security threat that global enterprises face. Machine learning and artificial intelligence (AI) are becoming more closely linked across sectors and applications than at any other time in recent memory, as computing power, storage capacity, and data collecting improve.People cannot deal with such a massive amount of information in a progressive manner. With machine learning and AI, that peak of data can be reduced in a quarter of the time, allowing the organization to discover and recover from security threats. [1]

2. ROLE OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

A. Artificial Intelligence:

Artificial intelligence is the process of making a computer, a computer-controlled robot, or software think intelligently in the same way that intelligent humans do. AI is performed by first studying how the human brain works, as well as how humans learn, decide, and work when attempting to solve a problem, and then applying the findings to construct intelligent software and systems. Intelligence is typically defined as the ability to gather knowledge and reason about it in order to solve complex issues. Intelligent machines will soon replace human capabilities in a wide range of fields. Artificial intelligence is the study and development of intelligent devices and software capable of reasoning, learning, knowledge acquisition, communication, manipulation, and object perception.

The phrase was coined by John McCarthy in 1956 to describe an area of computer science dedicated with making computers behave like people. The study of computation allows us to see reason and act. Artificial intelligence differs from psychology in that it emphasizes computation, whereas computer science focuses on observation, thinking, and action. It enhances the intelligence and functionality of machines. [2]

B. The Rise of AI in Cyber Security:

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 endeavors 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 beneficial relationship is to consider the best security expert in your organization. If you use this star representation to develop your machine learning and artificial intelligence algorithms, the AI will be as astute as your star employee. Now, if you set aside the time to create your machine learning and artificial intelligence programs with your ten finest reps, the end result will be an answer as savvy as your ten best employees put together. Furthermore, AI never has a lost day. [3]

C. How Can Cybersecurity Use Artificial Intelligence?

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 Artificial intelligence (AI) is already being utilized in, or is actively being studied for, the following areas in cyber security solutions: Gmail uses artificial intelligence (AI) to detect and prevent spam and fraudulent emails. Gmail's Artificial Intelligence was trained by millions of current Gmail users; every time you click on an email message, whether it is spam or not, you help train the AI to detect spam in the future. Gmail uses artificial intelligence (AI) to detect bogus emails. Gmail's Artificial Intelligence was trained by millions of current Gmail users; every time you click on an email message, whether it is spam or not, you help train the AI to detect spam in the future.

As a result, artificial intelligence has advanced to the point where it can detect even the most subtle spam emails disguised 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: Botnet detection is an extremely sophisticated subject that is often focused on pattern recognition and proxy server timing analysis. Because botnets are usually administered by a master script of instructions, a large-scale botnet attack will typically contain a large number of "users" all making the same queries on a site in a single attack. This could involve failed login attempts (a botnet brute force password assault), network vulnerability scans, and other breaches. It is quite difficult to convey the incredibly complex role that Artificial Intelligence plays in botnet identification in a few words, but here is a superb study paper on the subject that does an excellent job.

These are just a few of the ways Artificial Intelligence has been applied in cyber security. There are currently numerous research articles that provide persuasive evidence in support of Artificial Intelligence's usefulness in the realm of cyber security. According to the bulk of research studies, the success rate for detecting cyber attacks is between 85 and 99 percent. Dark Trace, an Artificial Intelligence development firm, claims a 99 percent success record and already has hundreds of clients throughout the world. [4]

D. Benefits of AI in Cyber Security:

A assessment of the benefits of artificial intelligence in the field of cyber security finds that institutions that have incorporated AI in cyber security reap significant benefits. This is clear from the fact that two out of three firms boosted their ROI on cyber security technologies. For example, Siemens AG, a global leader in electrification, automation, and digitalization, chose Amazon Web Services (AWS) to build an AI-powered, high-speed, self-controlled, and extremely elastic platform for its Siemens Cyber Defense Center (CDC). The AI deployed was capable of estimating 60,000 potential assaults per unit time. As a result of the AI deployment, this capacity was managed by a team of fewer than a dozen people with no detrimental influence on system performance.

AI in cyber security enables organizations to understand and reapply previous danger patterns in the detection of emerging threats. As a result, time and effort are saved while discovering and investigating incidents, as well as

remediating hazards. Approximately 64% of administrators report that AI reduced the cost of detecting and responding to breaches. Rapid response is critical in avoiding cyber-attacks. Organizations reduce costs by an average of 12%. AI provides prospects for cyber security primarily because the cyber security landscape is fast transitioning from identification, manual response, and mitigation to automated mitigation. AI can detect novel and sophisticated changes in attack extensibility. [5]

E. Disadvantages of AI in Cyber Security:

1) Cost effectiveness: Sometimes the cost of using AI services surpasses the limit, therefore not everyone can benefit from them.

2) Cyber threats: Your data and privacy are more vulnerable to hacker attacks. If no precautions are taken, they will be able to effortlessly follow your location and hack your personal information.

3) Machine gaining control over humans: This is the oldest AI-related worry. This worry has previously been depicted in a number of movies and literature. Steps must be done to prevent this from occurring.

4) Loss of jobs: Artificial intelligence is viewed as a threat since some studies indicate that a large portion of the workforce would lose their employment and be replaced by AI apps and machinery.

5) Not everyone is familiar with AI: Not everyone wants to work with and comprehend modern technologies.

F. Future Aspects:

As businesses become more aware of the cyber hazards they face, all sources predict that cyber security spending will rise in the next years. For example, the Technology Industry Association (TIA) forecasts that US spending would top $63.5 billion, or 0.35 percent of GDP, in three years. Gartner Inc. expects that global spending will increase by 8.2% between 2014 and 2015. Block chain technology has the biggest potential net benefit in the United States of America ($407 billion).

The largest economic opportunity (US$962 billion) is in product inventory management, also known as provenance, which has emerged as a new priority for many companies' supply chains. Block chain technology may benefit firms ranging from heavy industries, such as mining, to fashion labels, in response to the public's and investors' growing interest in sustainable and ethical procurement. Banking and financial institutions, such as the use of digital crypto currencies and the promotion of digital payments through cross-border remittances, are meant to help minimize fraud and identity theft. [4]

3.CONCLUSION

So, in this paper, we discussed the importance of Artificial Intelligence in cyber security, as well as the many issues that arise as a result of it and how to mitigate them. Despite various limitations, Artificial Intelligence plays a crucial role in cybersecurity. To overcome the disadvantages, artificial intelligence will help to develop cyber security.

4. REFERENCES

[1] Arockia Panimalar.S, Giri Pai.U, Salman Khan.K, “ARTIFICIAL INTELLIGENCE TECHNIQUES FOR CYBER SECURITY”,International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 03 | Mar-2018, e-ISSN: 2395-0056, p-ISSN: 2395-0072.

[2] Rajneesh Kumar, “Artificial Intelligence : A Path to Innovation”, International Journal of Scientific Research in Science and Technology (IJSRST), 2017 IJSRST | Volume 3 | Issue 1 | Print ISSN: 2395-6011 | Online ISSN: 2395- 602X.

[3] 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).

[4] 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.

[5] Shidawa Baba Atiku, Achi Unimke Aaron, Goteng Kuwunidi Job, Fatima Shittu and Ismail Zahraddeen Yakubu, "Survey On The Applications Of Artificial Intelligence In Cyber Security", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 9, ISSUE 10, OCTOBER 2020, ISSN 2277-8616.