National Research Journal of Information Technology & Information Science
Volume No: 11, Issue No: 1, Year: 2024 (January-June)
PP: 21-26
ISSN No: 2350-1278 (Print)
Peer Reviewed & Refereed Journal
National Research Journal

GUARDIAN MIND: AI SHIELD FOR CYBER SECURITY

Gurjot Kaur Sidhu

Assistant Professor, Department of Computer Science, Khalsa College for Women, Civil Lines, Ludhiana

Tanu

Assistant Professor, Department of Computer Science, Khalsa College for Women, Civil Lines, Ludhiana

ABSTRACT

Computer networks are protected against cyber-attacks or unintentional unwanted access to achieve cybersecurity. Thus is the need of the hour. Cybercriminals are rising day by day in all organizations, businesses and governments, so cybersecurity solutions are of utmost importance. Artificial intelligence can play an important role in it. The security intelligence modelling based on such AI methods can make the cybersecurity computing process automated and intelligent than the conventional security systems. However, it was clear that the problems of certain cybersecurity would only be solved efficiently if artificial intelligence approaches are expandable. In strategic decision making, comprehensive information is important. This paper emphasizes how sensitive networks and data can be protected from cyber-attacks by fusing artificial intelligence with cybersecurity. In a few years, the field of cyber security has expanded rapidly. As a result, Risks of cyber threats are consistently increasing. This paper discusses various applications of artificial intelligence in cyber security. Artificial Intelligence has shown promising results in cyber security examining the data through its decision making. This paper focuses on AI techniques which are being used in various applications in the battle against the cyber-attack.

KEYWORDS: Cyber security, Cyber-attacks, Artificial Intelligence

1. INTRODUCTION

Artificial Intelligence involves the process of making computer software think and work intelligently as humans. The process of creating artificial intelligence includes how the human brain works and people are able to learn, make decisions, and cooperate to solve problems. Intelligent software and systems are created with the help of the result of this research. Intelligence means the capacity to take information from various resources and then use that information to solve the problem. Human beings are replaced by intelligent machines. Artificial Intelligence has the ability to learn, acquire information, communicate, control, and recognize objects. John McCarthy used the phrase to make computers behave like humans in 1956. By the study of computation, perceiving and acting becomes possible. Artificial intelligence is different from psychology because of its focus on computation, however computer science is different from it as it emphasizes only on perception, reasoning, and action. It gives machines more intelligence and utility (Welukar & Bajoria , 2021).

Machine learning and Artificial Intelligence are combined with various businesses and applications because of its processing speed, storage capacity and behavior like human beings. This large amount of data is mandatory for AI, as it has the ability to analyze and interpret everything that is collected to identify novel patterns and nuanced details. In other terms cyber security means to take fresh measures and flaws to stop the additional attacks. Some of the pressure may relieve human security partners. When any task is mandatory, they

ISSN No: 2350-1278 (Print)
Peer Reviewed & Refereed Journal
National Research Journal

can use their energy to become more creative ventures. Machine learning and Artificial Intelligence are combined with various businesses and applications because of its processing speed, storage capacity and behavior like human beings. In order to find new patterns and precise details, AI needs a large amount of data to examine and explain it. To stop the future attacks, it allows for the prompt examination and investigation of new projects and susceptibility. This is the suggestion for cyber safety. This could reduce some of the strain on human security partners. They are advised to channel their energy into trying more imaginative and successful ventures when an activity is required.

Artificial intelligence can be integrated into cyber security systems to alleviate the on-going threat of cyber security that affects multinational corporations. Artificial Intelligence, processing power, storage capacity, and data collecting expand, machine learning are being organized more mainly across industries and applications than at any other point in recent memory. Dwellers are unable to manipulate this large amount of information slowly. Data theft can be quickly reduced with the help of machine learning and artificial intelligence, combining the firm in identifying and reducing security threats (Sadiku et al.,2020).

2. LITERATURE REVIEW

When it comes to exclusive or sensitized information, Data Security becomes more important. By taking advantage of people's data, hackers become more and more proficient every day. There are increasing reports of data infringement, cyber warfare, data poisoning, intrusions and crashes. The people or groups who are using computer networks are at risk from cyberpunk like corporations, firms, administrations, and customers. It is one of the most likely worldwide attacks. The network attacks are getting more complicated as Cyberpunks are getting more expert every day (Sadiku et al.,2020).

Das, R. and Sandhane, R. (2021) discuss the findings of AI most widely relevant to cybersecurity. Cybersecurity implementations of neural networks are still ongoing. In several domains where neural networks aren't the most suitable technology, advanced cyber-security techniques remain imperative. Sophisticated cybersecurity techniques are needed in this context of continually increasing cyber threats and bad intelligence. DDoS prevention experience has also shown that, with the right strategies, security against large-scale threats may be achieved with relatively few resources.

According to Welukar & bajoria(2021),Many companies and organizations become aware about the risk of the internet. Therefore, the investment on cyber security will rise in the future. For example, in three years, US spending is expected to surpass $63.5 billion, or 0.35 percent of GDP, according to the Technology Industry Association (TIA). Global spending is expected to increase by 8.2 percent between 2014 and 2015, according to Gartner Inc. The US $407 billion potential net benefit of block chain technology is the highest of any technology. The largest economic opportunity (US$962 billion) is in product inventory management, or provenance management, which has gained popularity as a new area of emphasis for supply chains in many businesses.

Perwej et al.(2021) concluded that as technology develops so fastly, our lives are becoming more and more digital. Nowadays, everyone lives in a cyberspace where all information is digitized and kept online. Almost everything is done online these days, whether it be for banking, shopping, business, or education. When it comes to cyber security, the emphasis is often on trying to define the issue and assess the actual danger level. Cybersecurity concerns everyone: experts, ordinary citizens, lawmakers, and decision-makers in general.

ISSN No: 2350-1278 (Print)
Peer Reviewed & Refereed Journal
National Research Journal

Cyber Threat Information focuses primarily on defense against these attacks, but there is a need for new methods to unmask attackers.Rana et al. developed malicious files as decoys to gather information from susceptible PCs using honeypots. They used tools like Visual Studio Code and Python for data analysis and counterintelligence techniques to provide proactive adversarial system intelligence.The evaluation method uses counterintelligence techniques such as cyber deception and decoy files to obtain adversary information. Overall, this research focuses on providing better proactive adversarial system intelligence by capturing attackers' system information through accurate document-based tokens in a proactive defensive environment while executing threat hunting with TTPs (Tactics Techniques Procedures)

According to Panimalar et al.(2018), the threats in cyberspace are evolving, the general public is becoming the target of cyberattacks more often these days. Malicious and hostile actions create pathways that allow predators (hackers and crackers) to access computer systems or networks without authorization. We refer to these actions as cyberthreats. To create these routes, predators focus on the flaws and errors in the network or system. Numerous cyberthreats exist, including Man in the Middle (MITM), ransomware, viruses, worms, Trojan horses, spyware, and adware, as well as attack vectors and social engineering.

3. APPLICATIONS OF AI IN CYBER SECURITY

Artificial Intelligence is already used in some of the cyber security solution areas. Gmail uses artificial intelligence to identify and prevent unwanted spam and deceptive Artificial Intelligence is used by Gmail to identify and stop unwanted spam and deceptive emails. Artificial intelligence trained millions of Gmail users to recognize unwanted emails in the future. Before the invention of AI each time when a user clicks on an email message, regardless of whether it is deceptive or not. But with the help of artificial intelligence users can easily identify whether it is spam mail or not (Fortinet, 2024).

3.1 Fraud detection: The fraud detection system uses MasterCard Decision Intelligence to identify various transactions. It looks at numerous factors like the seller, the buyer, the transaction location, and the buyer's typical purchasing habits to examine whether a purchase is unusual (Sadiku et al.,2020).

3.2 Botnet detection: It mostly relies on timing analysis and pattern recognition of proxy servers. Botnet attacks mostly include a large number of users that make the same queries on a website in a single attack because it is mostly controlled by a master script of instructions. Different types of breaches fall under this category like Network vulnerability scans, failed login attempts and password attacks etc. Artificial intelligence plays a very difficult role in botnet examination that is difficult to explain in a few lines, however it plays a good role in explaining this complex job easily (Moorthy & Nathiya, 2023).

Artificial intelligence has a small number of applications in the field of cyber security. But nowadays there are many research studies that indicate that artificial intelligence is very useful for cyber security. Approximately 85 to 99 percent of cyber-attacks are examined by artificial intelligence. DarkTrace is an artificial intelligence development company which contains many global clients and 99 percent success rate (Moorthy & Nathiya, 2023).

3.3 Automated defense: Expert (analyst-driven) and automated (machine-driven) are the two types of cyber security systems.. Humans create and manage expert systems whereas artificial intelligence (AI) tools are used by automated systems. AI based systems are made by Self-learning, autonomous agents. The example of an automated system is: CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart).

ISSN No: 2350-1278 (Print)
Peer Reviewed & Refereed Journal
National Research Journal

Automation techniques require high speed and large volume of data because humans cannot handle the speed and large volume of data which is required to defend cyberspace. When networks grow larger and more difficult then Cyber defences organizations can mostly improve by the use of Artificial Intelligence (ReasonLabs,2023).

The main goal of the perfect cyber-defense is to ensure complete user protection without sacrificing any functionality. Systems with AI automation can be incorporated into current cyber security operations. Among these roles are:

1. Accurate finger print based sign in methods are developed.
2. Prophetic validations are used to identify risks and spiteful activity.
3. Natural language processing is used to improve analysis and learning.
4. Accessing and verification have to be protected from unauthorized access.
5. To protect endpoints from spiteful attacks, humans can be used.
6. Common security task automation is utilized with the help of AI

3.4 Cognitive security: This method consists of the benefits of both artificial and human intelligence. An advanced type of artificial intelligence among a variety of AI technologies is cognitive computing (CC). It includes devices like hardware or software that behave the same as the human brain. The main objective of cognitive computing is to go on the different side of what is possible with von Neumann computers.Cognitive Computing and Artificial Intelligence have the same objectives whereas their tendency to capture in natural human interaction are different. The latest technologies embedded with artificial intelligence require human intelligence. (Huang.& Zhu , 2023).

3.5 Adversarial training: Adversarial training is mostly used for offensive ends to describe the creativity and applications of Artificial Intelligence .To investigate AI susceptibility, cybersecurity engineers are making adversarial attack models in advance . It has the courage to make the algorithms behave differently or disclose details about their internal operations. AI systems that are used in adversarial training become stronger and system susceptibility is found more easily. If we use an adversarial approach, then we have a safer AI application (Sadiku et al.,2020).

3.6 Parallel and dynamic monitoring: Throughout deployment, some kind of continuous monitoring is necessary due to the targeted systems' capacity for learning. To make sure that discrepancies between a system's expected and actual behavior are identified and appropriately handled, monitoring is required. There should be some control system that works as a standard to evaluate the behaviour of the original system (Sadiku et al.,2020).

4. CHALLENGES OF ARTIFICIAL INTELLIGENCE IN THE FIELD OF CYBER SECURITY

Future research, development, and use of AI in cybersecurity will require you to distinguish between short-term objectives and long-term projections. Various types of Artificial Intelligence techniques may be easily applied to cybersecurity, and cybersecurity issues require more accurate and precise solutions than are now being deployed. It would be great to see completely new ideas in information processing for situation management and decision making in the future. The topic of knowledge management in cyberwarfare is quite demanding in terms of technology. Even if AI solutions may be quickly used to handle pressing cybersecurity issues, a more intelligent strategy is needed. Although there are potential solutions available with current AI applications, the ultimate objective is to create

ISSN No: 2350-1278 (Print)
Peer Reviewed & Refereed Journal
National Research Journal

completely new information processing ideas for situation management and decision-making in the future.

Since the threats are becoming more sophisticated and are being launched by highly skilled hackers, it has become a major concern in recent years. As a result, numerous patches and solutions have been developed in anticipation of these attacks, since risk management dictates that if the platform is not defended, a significant loss will occur. To prepare for the upcoming problems, all known assaults are thus examined, their patterns of occurrence monitored, and the variety of attacks demonstrates further attack types that may arise in the future.

By almost all measures, cybersecurity attacks are becoming more prevalent and complex every day, which is bad news for the IT sector, which is already grappling with a lack of security expertise. Because of the shortage of security experts, organizations are starting to worry as they would not have the necessary skills in the coming years to stop data breaches and network attacks since there is a shortage of security experts.

Bias in AI systems is also one of the biggest problems. Bias can find ways to get into Artificial intelligence algorithms as it is used to train the various systems, it makes incorrect forecasts and possibly missing serious risks. This may reduce Artificial Intelligence's ability to recognize and respond to threats, underscoring the necessity of objective, high-quality data for AI system training.

5. CONCLUSION

Thus, we saw in this paper the significance of artificial intelligence in cyber security as well as the different issues it raises and how to address them. Even with its limitations, artificial intelligence is still very important to cyber security. Artificial Intelligence will help improve cybersecurity by helping to overcome the drawbacks. Undoubtedly, AI may enhance cyber security in a variety of ways if it is used and educated carefully. It requires fewer resources and can provide real-time protection against cyberattacks. A machine learning technique can quickly integrate new patterns in data which are difficult for human analysts to gather and examine due to the evolution of cyber threats. Machine learning offers various analysis capabilities, with the help of this human analysts can concentrate on deciphering the data and coming up with innovative ways to take the fight to criminals head-on. Cybersecurity will thus undoubtedly reach a new level of sophistication with the application of deep learning and machine learning in defense systems.

REFERENCES

Banafa, A. (2021, January 11). *Challenges Facing Using AI in Cybersecurity | OpenMind*. OpenMind.https://www.bbvaopenmind.com/en/technology/artificial-intelligence/challenges-f acing-using-ai-in-cyber security/

Bhatele,K,R.,Shrivastava,H.,Kumar, N.(2020). The Role of Artificial Intelligence in Cyber Security (PDF) The Role of Artificial Intelligence in Cyber Security (researchgate.net).DOI:10.4018/978-1-5225-8241-0.ch009

Cognitive Security. (n.d.). SpringerLink. https://link.springer.com/book/10.1007/978-3-031-30709-6

Das, R., Sandhane, R., Artificial Intelligence in Cyber Security(2021) https://www.researchgate.net/publication/353419449_Artificial_Intelligence_in_Cyber_Security.DOI:10.1088/1742-6596/1964/4/042072

Grover, T., Malhotra, H. (2022). Artificial Intelligence in Cyber Security: Review Paper on Current Challenges Faced by the Industry.DOI: https://dx.doi.org/10.21275/SR231206140043

How Artificial Intelligence (AI) Can Help With Cybersecurity Threats | Fortinet. (n.d.). Fortinet.https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity

ISSN No: 2350-1278 (Print)
Peer Reviewed & Refereed Journal
National Research Journal

https://doi.org/10.1016/j.procs.2023.01.119

Lutkevich, B. (2023, April 18). expert system. Enterprise AI. https://www.techtarget.com/searchenterpriseai/definition/expert-system

Moorthy, R.S.S., Nathiya,N. (2023). Botnet Detection Using Artificial Intelligence.

Natural Language Processing (NLP) [A Complete Guide]. (2023, January 11). DeepLearning.AI. https://www.deeplearning.ai/resources/natural-language-processing/

Odogwu, C. (2022, November 8). 6 Downsides of Using Artificial Intelligence in Cybersecurity.MUO.https://www.makeuseof.com/downsides-artificial-intelligence-cybersecurity/

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., Jaiswal A. K. (2021). A Systematic Literature Review on the Cyber Security .DOI:10.18535/ijsrm/v9i12.ec04

Rout, M. (2020, July 5). A review on Cybersecurity and its challenges. Lovely-professional-university.https://www.academia.edu/43455923/A_review_on_Cybersecurity_and_its_challenges

Sadiku, M. N. O., Fagbohungbe, O. I., Musa, S. M. (May -2020). Artificial Intelligence in Cyber Security.DOI: 10.31695/IJERAT.2020.3612

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. Sensors, 23(16), 7273.https://doi.org/10.3390/s23167273

Welukar, J. N., Bajoria, G. P. (30 Dec 2021). Artificial Intelligence in Cyber Security - A Review. https://doi.org/10.32628/IJSRST218675 What is Automated Defense? The Power of Cybersecurity Vigilance. (n.d.). https://cyberpedia.reasonlabs.com/EN/automated%20defense.html