IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2024

DOI: 10.17148/IJARCCE.2024.13207

A CURRENT TREND OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

M.Vasanthi[1], R. Narmadha[2]

PG Student, Department of Computer Science, R.B. Gothi Jain College for Women, Red hills, Chennai-52[1,2]

Abstract: In recent times, there have been attempts to leverage artificial intelligence (AI) techniques in a broad range of cyber security applications. Artificial Intelligence (AI) is a powerful technology that helps Cyber Security teams automate repetitive tasks, accelerate threat detection and response, and improve the accuracy of their actions to strengthen the security posture against issues and cyber attacks. The AI is transforming the world in many ways and one of the most crucial areas is cyber security. To be created AI in cyber security template for Microsoft Power point and Google slides to illustrate the role of AI in detecting and preventing cyber risk. This paper provides a concise overview of AI implementation of various cyber security using artificial technologies and evaluate the prospects the expanding the cyber security capabilities by enhancing the defense mechanism. On the other hand, it was clear that certain cyber security problems would only be overcome efficiently if artificial intelligence approaches are deployed.

Keywords: Cyber Security, Microsoft Power point, Google Slides, Attacking, Marketing, Chat GPT.

I. INTRODUCTION

"Once a new technology rolls over you, if you're not part of the steamroller, you're part of the road"

In digital, our networks and systems are prone to more attacks and cyber crimes than ever before. They had made it difficult for only humans to analyze every possible threat and prevent them from attacking. There are over billions of time changing signals which are required to be analyzed in order to calculate the risk accurately. So, we have several new and upcoming artificial intelligence tools and technologies to help in the field of cyber security.AI powered cyber security tools are designed to identify and detect attacks in real time and can automatically response to the incident. They can also help human security expects identity emerging threats and trends, enabling them to take preventative action. And there are some major AI in cyber security applications are malware and phishing detection, knowledge consolidation, detection and prioritizing new threats, breach risk predication, task automation. The primary benefits of AI in cyber security is its ability to detect and response to threats in realtime.AI powered security systems can monitor networks, endpoints ,and other devices to detect anomalies, behavior patterns, and other indicators of comprises. And one of the key limitations of AI in cyber security lies in the accuracy of its output. While AI systems, such as generative pre-trained transformers like Chat GPT can generate text that aligns with the current trends on the internet, their responses are not always accurate or reliable.AI- powered cyber security systems can analyze vast amounts of data to identify patterns and anomalies that might indicate a cyber attack improved incident response. Therefore, the latest technologies in cyber security include AI and ML, behavioral biometrics, zero trust architecture, block chain, quantum computing, cloud security and IOT security.

II. CYBER SECURITY OVERVIEW

Cyber security is the protection of internet-connection systems such as hardware, software and data from cyber threats. To be practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems. In which cyber security strategy can provide a good security posture against malicious attacks designed to access, alter, delete, destroy or extort an organization or user systems and sensitive data. Cyber security is also involved in preventing attacks that aim to disturb a systems or device operations. In, Today's connected world why cyber security is to more important?"The extensive use of technology exposes us to a range of risks, including identity theft, scams, and data breaches. At an individual level, a cyber security attack can result in everything from fraud attempts, and to the loss of important data like family photos. Therefore the cyber security has five types are Application security, Network security, Cloud security, critical infrastructure security, IOT security and so on. Historically, Role of artificial intelligence in cyber security will go hand-in-hand Technology advancement and has been a field dominated by resource-intensive efforts. To be Remediation activities for monitoring, threat hunting, incident response, and other duties are often manual and time-intention. In AI powered system can analyze and respond to various security incidents in real-time. It can automate processes like data collection and incident response, which helps reduce response times for organization.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2024
DOI: 10.17148/IJARCCE.2024.13207

Artificial intelligence has also been used to enhance user authentication processes and to be increased data security with powered systems. It can deploy techniques like encryption, anomaly detection, and behavioral analysis for the protection of data. This help security teams in protecting database and achieve better compliance with data protection regulations. In their purest application, AI and ML are technologies that have played critical roles in advancing fields such as medicines, manufacturing and marketing. Now a day's the crowd is more frequently falling victim to cyber-attacks due to the evolutionary nature of risks in the cyberspace. Pathways are constructed through malicious and offensive activities, which give unauthorized access to predators on computer systems or networks. These activities are called cyber threats.

Predators work on the bugs and faults in the system or network to establish these pathways. Everybody possesses some valuable assets and confidential data which are under their authority and when an outsider gets access to those assets and data, they can cause extreme harms. Taking cyber space into consideration, these accesses without the consent of the owner can be the results of one or more cyber threats. Here cyber security comes into play. It ensures the availability, confidentiality, and integrity of your system or network and helps it to work efficiently without compromising with the security.

III. AI BEST TOOLS FOR CYBER SECURITY

The digital continue to grow and evolve so does the risk of cyber attacks. With the increasing amount of sensitive information stored online, companies and organization must be proactive in protecting their data. This is where AI comes to play and revolutionizing the way we approach cyber security, providing advanced solution to detect and prevent cyber threats. So, AI explore 5 best tools cyber security are

1. **DARKTRACE:** AI interrupts in progress cyber attacks, including ransom ware, email phishing, and threats to cloud environment. The features of enterprise immune system, autonomous response, dark trace threat visualize, AI and machine learning, industry leading and benefits of learn and adopt its understanding of ‘normal’; autonomously detects and respond to cyber-threats before crisis hits; provide complete visibility of every user and device.

2. **CYCLANCE:** Cyclance is enterprise level cyber security powered by advanced AI .it provides organization enhanced visibility and protection against current and future cyber attacks. To work AI predicts, prevents, and protect against zero- day threats by analyzing similar blocks of file code to identity malicious file. It blocks threats automatically in real-time through observation, pattern recognition, and predictive analytics.

3. **IBM WATSON**: To maintain a specialized corpus of security knowledge, which includes formerly invisible unstructured information with inside the shape of blogs, websites, danger Intelligence feeds.IBM security tool provide transformative AI powered solutions that optimize analysts time by accelerating threat detection, and protecting user identity and data flow while keeping security teams in the loop and in charge.

4. **LOGRHYTHM:** Log Rhythm is an enterprise class platform that seamless combines SIEM, log management, file integrity tracking and gadget analytics with host and community forensics in a unified safety intelligence platform. The tools aggregate and analyze volumes of data from an organization’s applications, devices, servers, and user’s in real time so security teams can detect and block attacks.

IV. REAL TIME USECASES OF AI IN CYBER SECURITY

1. **Security screening:** Security screening done by departure officers and customs can detect people that are false about their intentions. However, the screening process is choosing to mistakes. In addition, human-based screening can lead to errors because people get tired and can be distracted easily. The United States Department of Homeland Security has developed a AVATAR that screens body signal and facial expressions of people. It indicates changes in their answers as well as differences in their voice tone. The collected data is compared against elements that indicate that someone might be untruthful.

2. **Reducing Threat Response Time:** A global bank faced civilized cyber threats and advanced attacks. The existing solution could not effectively detect and help new generations of threats. The bank security team located Pala don’s AI-based Managed Detection and Response Service. Threat hunting service is based on data science and machine learning capabilities. The bank blackmail and response capabilities for advanced attacks were reinforced. This includes data exit , advanced under attack ransom ware, malware, zero-day attacks, social engineering, and encrypted attacks.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 2, February 2024

DOI: 10.17148/IJARCCE.2024.13207

The key to securing an organization's network is sensitivity management. An average company has to deal with many threats daily and it firstly has to detect them, then identifies the type of it and takes necessary counter measures to prevent all of them in order to be safe from any type of damage. In order to manage all the sensitivity we need to analyse and then assess the security measures which are available to us through AI research which can prove to be a great help. The future, the security of an organization or a system can be improved with the help of artificial neural networks by learning the patterns in at last. It searches basically for potential threats which follow a similar quality and the threats which get identified are blocked very early enough. The technology of artificial intelligence when applied with cyber security makes it difficult for hackers to hack something due to the fact that AI keeps learning through various situations which makes it difficult for them to beat its intelligence as the system keeps on improving over the point it is learning.

V. CONCLUSION

AI considered as one of the most promising developments in the information age, and cyber security flexibly discipline that could benefit rest from it. This technology a strong interdependent between AI system and human factors is necessary for enhance cyber security's maturity. Therefore, AI can be powerful in the ongoing battle against cyber threats, helping to create a safer and more secure digital landscape.

REFERENCES

[1]. B. McMahan et al., "Communication-Efficient Learning of Deep Networks From Decentralized Data", *Artificial Intelligence and Statistics Proc. PMLR*,vol. 10, no. 1, pp. 1273-82, 2017.

[2]. C. En Guo, S.-C. Zhu and Y. N. Wu, "Primal Sketch: Integrating Structure and Texture", *Computer Vision and Image Understanding*, vol. 106, no. 1, pp. 5-19, 2007.

[3]. Hogade, N., Pasricha, S. and Siegel, H.J,"Energy and Network Aware Workload Management for Geographically Distributed Data Centers". *IEEE Transactions on Sustainable Computing*, vol.7, no. 2, pp.400–413. 2021

[4]. A. Wierman, Z. Liu, I. Liu and H. Mohsenian-Rad, "Opportunities and challenges for data center demand response", *Proc. Int. Green Comput. Conf.*,vol.7, no. 6, pp.1-10, 2014.

[5]. J. D. Jenkins et al., "The benefits of nuclear flexibility in power system operations with renewable energy", *Appl. Energy*, vol. 22 no. 2, pp. 872-884, 2018.

[6]. Haoying Dai, Yanne Kouomou Chembo, "RF Fingerprinting Based on Reservoir Computing Using Narrowband Optoelectronic Oscillators", *Journal of Lightwave Technology*, vol.40, no.21, pp.7060-7071, 2022.

[7]. Floris Van den Abeele, Jeroen Hoebeke, Girum Ketema Teklemariam, Ingrid Moerman, Piet Demeester, "Sensor Function Virtualization to Support Distributed Intelligence in the Internet of Things", *Wireless Personal Communications*, vol.81, no.4, pp.14-18, 2015.

[8]. J. Hwang, J. Kim and H. Choi, "A review of magnetic actuation systems and magnetically actuated guidewire-and catheter-based microrobots for vascular interventions", *Intell. Serv. Robot*., vol. 13, no. 1, pp. 1-14, 2020.

[9]. D. G. Feitelson, D. Tsafrir and D. Krakov, "Experience with using the parallel workloads archive", *J. Parallel Distrib. Comput*., vol. 74, no.3, pp. 2967-2982, 2014.

[10]. B. Accou, J. Vanthornhout, H. V. Hamme and T. Francart, "Decoding of the speech envelope from eeg using the vlaai deep neural network", *Scientific Reports*, vol. 13, no. 1, pp. 812, 2023.

[11]. Serim Lee, Nahyun Kim, Junhyoung Kwon, Gunhee Jang, "Identification of the Position of a Tethered Delivery Catheter to Retrieve an Untethered Magnetic Robot in a Vascular Environment", *Micromachines*, vol.14, no.4, pp.724, 2023.

[12]. Napoleon D. and Praneesh M. "Detection of Brain Tumor using Kernel Induced Possiblistic C-Means Clustering", volume no.3, issue no.9, pp 436-438, 2013

