International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

IJIEMR Transactions, online available on 28 Aug 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 08

10.48047/IJIEMR/V12/ISSUE 08/56

Title **Artificial Intelligence in Cyber Security**

Volume 12, ISSUE 08, Pages: 375-377

Paper Authors **K.V.Rajesh, Dr. C.V.P.R Prasad**

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Artificial Intelligence in Cyber Security

K.V.Rajesh
Asst. Professor, Malla Reddy Engineering College for Women, Maisammaguda, Hyderabad, 500100,
kvrajeshh@gmail.com
Dr. C.V.P.R Prasad
HOD & Professor-CSE Dept., Malla Reddy Engineering College for Women, Maisammaguda, Hyderabad, 500100
cvprprasad@gmail.com

ABSTRACT

Cyber security refers to the process of protecting computer networks from cyberattacks or unauthorized access. It is critical at this time. Organizations, corporations, and governments all require cyber security solutions as a result of the threat that cybercriminals pose to everyone. Artificial intelligence has a lot of potential in this regard. By combining artificial intelligence with cyber security, security experts are better equipped to secure sensitive data from online attackers. This paper provides an overview of the application of artificial intelligence to cyber security.

Key Words: Cyber security, Cyber-attacks, Artificial Intelligence.

1. INTRODUCTION

We now live in a digital age when data is king and everything is digital. Data security, especially for sensitive or private information, is more crucial than ever. Hackers are become more intelligent and creative at exploiting the sensitive data of people, businesses, and governments every day. Data poisoning, hacker attacks, and crashes are reported practically daily due to new cyberattacks, data bridges, and data breaches. Organizations, companies, governments, and customers who use computer networks are at risk from cybercriminals. One of the top five most likely sources of serious, worldwide danger has been identified as cyberattacks. Network attacks are getting more intricate, and cybercriminals are getting more skilled every day.

Information networks and data are protected from loss or illegal access using technology and procedures known as "cyber security." Because so much data is gathered, processed, and stored by businesses, governments, and military groups, it is essential. There are many distinct types of cyber security, including those used by the military, law enforcement, judicial system, business, infrastructure, interior, intelligence, and information systems. Cybersecurity is an active, multidisciplinary area that integrates criminology, information systems, and computer science. Availability, authentication, confidentiality, non-repudiation, and integrity have been the security goals. includes several problems including people, processes, and technology, as demonstrated.

Cyber crime range from individual citizen criminal behavior (hacking) to collective behavior, Malware, phishing, denial-of-service attacks, social engineering assaults, and man-in-the-middle attacks are examples of cyber attacks or threats. Cybersecurity entails lowering the danger of cyber-attacks. Management should address cyber threats proactively. Firewalls and other cybersecurity technology are commonly accessible. All essential parties, including government, business, infrastructure owners, and users, share responsibility for cybersecurity. Governments and multinational organizations have an important role in cybersecurity. The Department of Homeland Security (DHS) places a high value on cyberspace security. The DHS has a specific component called the National Cyber Security component that is in charge of risk management programs and cybersecurity regulations. The purpose of the Federal Communications Commission in cybersecurity is to improve the security of important computer networks and networked infrastructure. The Computer Fraud and Abuse Act (CFAA) continues to be the most pertinent applicable statute representing the United States' proactive cybersecurity endeavor.

2. OVERVIEW ON AI

All essential parties, including government, business, infrastructure owners, and users, share responsibility for cybersecurity. Governments and multinational organizations have an important role in cybersecurity. The Department of Homeland Security (DHS) places a high value on cyberspace security. The DHS has a specific component called the National Cyber Security component that is in charge of risk management programs and cybersecurity regulations. The Computer Fraud and Abuse Act (CFAA) continues to be the most pertinent applicable statute representing the United States' proactive cybersecurity endeavor.

AI systems are becoming increasingly adept at data analysis. One major aspect of AI technology is that it can be integrated into existing technologies. AI has improved numerous fields, including chemistry and medicine, where AI-aided computers begin regular diagnostics. The following computer-based tools or technologies have been utilized to meet AI's goals:

- Statistical and semantic NLP are the two core NLP approaches. Healthcare is the major industry that use NLP methods [8].
- Robots are computer-based, programmable robots with physical manipulators and sensors. The employment of intelligent robots in healthcare enhances patient satisfaction, diagnostic accuracy, and hospital operational performance. Medical robots can help in assisted living, social engagement, and surgery, among other things. Robotic guidance is becoming more common in spine surgery.
- Fuzzy logic: Making decisions based on a range of values as opposed to point estimations based on shaky or insufficient facts. In order to deal with knowledge uncertainty, imprecise logic is a type of logic that mimics human thought using incomplete or inaccurate data. The fuzzy model is not impacted by impressions or changes to the parameters.
- Machine Learning: Algorithms that can predict, understand, and "learn" on their own, without the use of pre-programmed instructions. By using analytical data algorithms, machine learning (ML) collects characteristics from incoming data and evaluates prediction models.
- A subset of machine learning known as "Deep Learning" handles different aspects of a challenging problem at each layer in a deep hierarchy of levels. It attempts to boost the capacity of supervised and unsupervised learning algorithms for handling challenging real-world scenarios by introducing several processing layers.
- Data mining is the practice of locating fresh information and occult patterns in vast databases. Some of the computing methods used in data mining include statistics, regression models, neural networks, fuzzy sets, and evolutionary models. Every AI technology offers a unique set of advantages. Instead of using only one of these models, it is recommended to combine them. AI technologies are significantly changing the retail industry and the shopping experience for customers.

3. APPLICATIONS OF AI IN CYBERSECURITY

- There are several inter-disciplinary linkages between AI and cybersecurity. Cybercrime is being detected and combated using. They might be used to teach security experts about the digital world and how to spot irregularities. The application of artificial intelligence may be utilized to extend the capabilities of current cyber security systems. Four domains, including automated defense, cognitive security, adversarial training, and parallel and dynamic monitoring, may all be improved by businesses using AI.
- Cyber security systems are divided into two categories: expert (driven by analysts) and automated (driven by machines). An excellent illustration in Artificial intelligence may significantly aid an organization's cyber security as networks expand in size and complexity. An ideal cyber-defense approach aims to completely safeguard users while maintaining all features. Automated artificial intelligence technology can be connected to ongoing cyber security operations. Among them are the following:
    - Developing more precise biometric login methods
    - Predictive analytics can be used to identify threats and malicious activity.
    - Natural language processing can improve learning and analysis.
    - Human analysis is improved, from malicious attack detection to endpoint protection.
    - Routine security tasks can be automated. There are no zero-day vulnerabilities.

There are many advantages to integrating artificial intelligence in cyber security. AI-based cyber security solutions are designed to work around the clock to protect you.

- Cognitive security blends the strengths of artificial intelligence and human intellect. Cognitive computing (CC), a more advanced sort of artificial intelligence, makes use of several types of AI. It refers to hardware and/or software that simulates the operation of the human brain. Artificial intelligence (AI) has been defined as technology that can do jobs that would ordinarily need human intelligence. Cognitive computing aims to go past the limitations of traditional programmable (von Neumann) computers. Watson for cyber security, IBM's first cognitive system, established its ability to answer tough questions as efficiently as the world's human champions in a Jeopardy exhibition match.

- Adversarial Training: This phrase refers to the creation and deployment of artificial intelligence for harmful intentions. To investigate AI vulnerabilities, cybersecurity engineers are developing pre-emptive adversarial attack models. An adversarial learning assault on the algorithms might force them to misbehave or divulge knowledge about their inner workings.

  • Monitoring in parallel and dynamically: The learning capacities of the intended systems necessitate some sort of ongoing monitoring throughout deployment. Monitoring is required to guarantee that any deviation between a system's intended and actual behavior is detected and addressed appropriately.

4. BENEFITS

Some of the most complex challenges, such as cybersecurity, are perfectly suited to artificial intelligence. It is a game-changing technology that has transformed our lives. It will be embedded in our houses, automobiles, and electronics, making everything "smarter" and more efficient. AI can distinguish between malware and legitimate software. New AI capabilities have the potential to make the world a safer, more just, and ecologically friendly place. AI-based solutions, due to their adaptability and flexibility, can assist us in overcoming the shortcomings of traditional cyber security systems.

5. CHALLENGES

There are restrictions that prohibit AI from becoming a widely used tool. Cost, extensive resources, and training are some of the drawbacks of AI in cyber security. AI in cybersecurity necessitates more resources and funds than standard non-AI cyber security solutions, and it may be impractical in some cases. Absolute security is difficult to achieve in the field of cybersecurity.

6. CONCLUSION

Artificial intelligence has grown in popularity and investment within the cyber security field. Google, IBM, Juniper Networks, Apple, Amazon, and Balbix were among the early AI adopters. As cyber assaults become more common, artificial intelligence is assisting security operations analysts in staying ahead of threats. AI automated systems will soon become an essential component of cyber security solutions, but they will also be utilized to do harm by hackers. The future of AI-enabled cyber security looks bright. More information about artificial intelligence in cyber security may be found in the books and periodicals listed below:

REFERENCES

[1] Ahmad, I., Abdullah, A. B., & Alghamdi, A. S. (2009). Application of artificial neural network in the detection of DOS attacks. SIN'09 - Proceedings of the 2nd International Conference on Security–234. https://doi.org/10.1145/1626195.1626252.

[2] Protect yourself from the Conficker computer worm.(2009).Microsoft. http://www.microsoft.com/protect/computer/viruses/worms/conficker.mspx.

[3] Sadiku, M. N. O., Fagbohungbe, O. I., & Musa, S. M. (2020). Artificial Intelligence in Cyber Security. International Journal of Engineering Research and Advanced Technology, 06(05), 01–07. https://doi.org/10.31695/ijerat.2020.3612.

[4] Rajani, P., Adike, S., & Abhishek, S. G. K. (2020). ARTIFICIAL INTELLIGENCE : THE NEW AGE. 8(2), 1398–1403.

[5] Mohammed Imran Shaik, K Anbazhagan, Digital Forensics-The Potential Evidence, Journal of Innovations in Information Technology , http://innovation-journals.org/JIIT/IT1-1/IT%20V1-I1-9.pdf

[6] Dr. Sandeep Singh Rawat Mohammed Imran Sk, Web Application Security Vulnerabilities, International Conference on Paradigms in Engineering & Technology, ISBN:978-93-5258-110-8, Pages 628-632

[7] Journal of Computer Security

[8] International Journal of Artificial Intelligence & Applications

[9] International Journal of Computer and Internet Security