AI in Cyber Defense: Opportunities, Challenges, and Emerging Pathways

Nitu Singh,Sasmita Lenka
Dept. of Computer Science and Engineering, GIFT Autonomous, Bhubaneshwar, 752054, India
Email: nitu@gift.edu.in

Abstract:

In today's interconnected world, cybersecurity is a crucial issue. With the rising number of digital assaults and information breaks, associations are attempting to shield their significant information from likely dangers. The application of Artificial Intelligence (AI) has emerged as a promising approach to improving cybersecurity. AI is being used by businesses to improve their cybersecurity posture as cyberattacks become increasingly sophisticated and frequent. As a proactive cyber defense, AI can assist businesses in real-time cyber threat detection, Prevention, and response. In this paper, we discuss the current state of AI-based cybersecurity and highlight both opportunities and obstacles. In addition, we identify areas requiring additional research and discuss the future of AI in cybersecurity.

Keywords: Artificial Intelligence, Cybersecurity, Deep Learning, Machine Learning.

1. INTRODUCTION

Cybersecurity is defined as the ability to protect digital data, networks, and computer systems from unauthorised access, theft, damage, and other malicious activities. Figure 1 shows the components of cybersecurity. The majority of online protection strategies employ firewalls, antivirus programmes, interruption discovery frameworks, and access control systems. However, these techniques have some drawbacks, such as the fact that they are unable to identify unknown threats. It has a high rate of false positives and takes a long time to respond. Yet, sophisticated attackers can easily evade these methods' due to their reliance on predefined rules and signatures.

2. APPLICATIONS OF AI IN CYBERSECURITY

Anomaly detection, threat intelligence, and intrusion detection are just a few of the cybersecurity applications that AI can be used for. Machine learning algorithms are used in anomaly detection to find unusual behavior in networks or systems. AI is used in threat intelligence to analyse data and forecast potential cyberattacks. Frameworks for intrusion identification use man-made intelligence calculations to identify unapproved admittance to frameworks or organisations.

3. BENEFITS OF AI IN CYBERSECURITY

There are numerous advantages to using AI for cybersecurity. First, the ability of AI algorithms to detect and respond to threats in real time speeds up the detection and response process to cyberattacks. Second, AI can quickly analyse a lot of data, making it easier for cybersecurity teams to find potential threats and vulnerabilities. Thirdly, cybersecurity professionals can concentrate on more difficult tasks because AI can automate routine tasks.

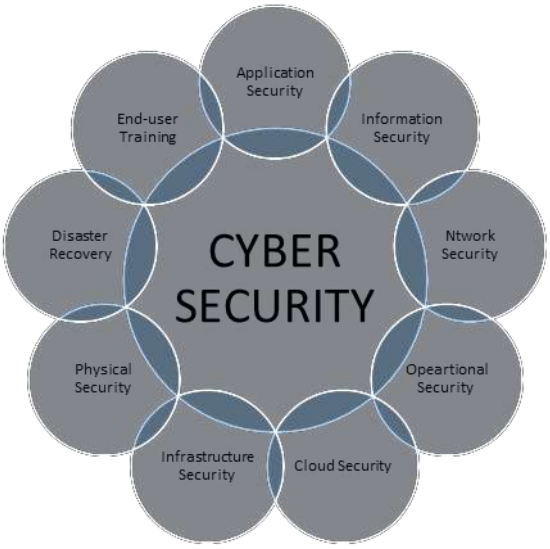

Figure 1: Components of Cybersecurity

4. OPPORTUNITIES OF AI IN CYBERSECURITY

There are a number of benefits to incorporating AI into cybersecurity. AI can speed up the identification and mitigation of cyberattacks by assisting businesses in real- time cyber threat detection and response. AI is capable of spotting advanced and unknown threats that conventional signature-based detection systems might miss. AI is able to look at a lot of data to find patterns and trends, revealing potential cyber threats. AI has the ability to automate routine tasks like patching and updating, allowing security personnel to concentrate on more difficult endeavours.

5. CHALLENGES OF AI IN CYBERSECURITY

In spite of the advantages of AI in cybersecurity, there are a number of obstacles that must be overcome. First, AI algorithms' inability to be explained makes it difficult to comprehend how they make decisions. This can make it hard for people to use it, especially in regulated industries where explain ability is required by law. Also, the precision of AI - based identification frameworks can be impacted by one-sided information or antagonistic assaults. Thirdly, AI algorithms' complexity can make them susceptible to cyberattacks like model poisoning and evasion.

It is important to make sure that AI systems themselves are secure because AI algorithms can be attacked. AI algorithms may generate either false positives or false negatives. This can result in the incorrect identification of threats or the inability to identify actual threats. The application of AI in cybersecurity raises ethical questions, particularly in relation to privacy and the possibility that AI might be used maliciously.

6. REAL-TIME EXAMPLES

Machine learning can quickly scan large amounts of data and analyze it using statistics. Modern organizations generate huge amounts of data, so it’s no wonder technology is such a useful tool.

Security Screening

Security screening done by migration officials and customs can distinguish individuals who are lying about their expectations. However, errors can occur during the screening process. Also, because people get tired and easily get distracted, human-based screening can make mistakes.

A system known as AVATAR was developed by the Department of Homeland Security in the United States for the purpose of screening individuals' facial expressions and body language. Big Data and AI are used by AVATAR to detect subtle variations in body language and facial expressions that could lead to suspicion.

A screen with a virtual face that asks questions is included in the system. It screens changes in their responses as well as contrasts in their voice tone. The data that has been collected is compared to things that might mean that someone is lying. If a passenger is deemed suspicious, they are flagged for additional inspection. The framework has a screen with a virtual face that clarifies pressing issues. It screens changes in their responses as well as contrasts in their voice tone. The data that has been collected is compared to things that might mean that someone is lying. If a passenger is deemed suspicious, they are flagged for additional inspection.

1) Security and Crime Prevention

Since 1995, the New York City police department has been using the artificial intelligence system known as CompStat. CompStat is an early form of artificial intelligence that uses a variety of software tools and incorporates philosophy and organizational management. The framework was the principal device utilized for "prescient policing", and many police headquarters across the U.S. have been utilizing CompStat to explore wrongdoings from that point forward. AI and game theory are being used to predict terrorist threats by AI-based crime analysis tools like Armorway, which is based in California. Additionally, Armorway is utilized by the Coast Guard for port security in New York, Boston, and Los Angeles.

7. FUTURE DIRECTIONS OF AI IN CYBERSECURITY

Future research ought to concentrate on developing explainable AI algorithms that can provide insights into how they arrive at their decisions in order to address the difficulties posed by AI in cybersecurity. Through the use of diverse and objective training data and the creation of defenses against adversarial attacks, AI-based detection systems ought to also be given the opportunity to advance in terms of accuracy and robustness. AI blended with other cybersecurity technologies like IoT security and blockchain can further improve organizational security.

There is still a lot of research to be done on how AI can be used in cybersecurity. The development of AI algorithms that are more robust and secure, the improvement of AI systems' accuracy, and the resolution of ethical issues associated with the application of AI in cybersecurity should be the primary focuses of subsequent research.

8. CONCLUSION

AI-based cybersecurity presents substantial opportunities for businesses to improve their security posture. However, further research and development are required to address the AI-related cybersecurity issues. AI has the potential to play a crucial role in protecting businesses from the growing threat of cyberattacks by addressing these issues. The impact of artificial intelligence on our lives continues to grow as technology integrates into everyday life. In terms of cybersecurity, the most significant benefits center around faster analysis and threat mitigation.

REFERENCE

1. G.NIKHITA REDDY, G.J.UGANDER REDDY, “A STUDY OF CYBER SECURITY CHALLENGES AND ITS EMERGNING TRENDS ON LATEST TECHNOLOGIES”, International Journal of Engineering and Technology - UK ISSN: 2049-3444, Volume 4 No.1 January 2014. Available at https://arxiv.org/abs/1402.1842.
2. K. M Rajasekharaiah[1], Chhaya S Dule[2] and E Sudarshan[3], “Cyber Security Challenges and its Emerging Trends on Latest Technologies”, IOP Conference Series: Materials Science and