RESEARCH PAPER

TITLE : CYBERSECURITY & ARTIFICIAL INTELLIGENCE

SUBMITTED BY : KHADER BASHA DASTAGEER

COUNTRY : SINGAPORE

Synopsis :

Considering the breadth of AI-centric applications, this paper is narrowing its focus on the vulnerability, opportunity, and growth of AI in Cyber Security domain. The definition and motive of cyber security varies among diverse organizations and standards around the world. Incorporating cybersecurity is not to only secure the perimeters, but rather to identify the value of the assets under threat, localize the threat, and then prioritize the actions to build a defence-in-depth framework that ensures continuity of service.

EMERGING of AI IN CYBERSECURITY:

The paper focused on the border security perspective of the spectrum of threats ranging from internal to transnational attacks, and the interconnected nature of military, government, and civilian information systems, the emphasis on improved measures to cope with the constantly evolving technology is crucial for maintaining the relevance and effectiveness.

Probabilistic ontologies can improve this process by providing a framework for understanding the likelihood of certain events or behaviours, which is crucial for detecting potential security breaches or attacks. AI technologies become much more proactive and efficient, the adversarial AI started to evade detection or generate sophisticated attacks.

PROSPECTS AND PROGRESSIONS

AI techniques across various applications holds tremendous potential for addressing numerous socio-economic and environmental challenges. AI has made remarkable notes in im-proving cybersecurity applications through its contributions to threat detection, response, and prevention. Anomaly Detection the pattern recognition of the attack vectors through these models helps the security personnel to make efficient decisions in a timely manner.

Cloud Security and Encryption is a framework enables a digital twin system with a virtual representation of Industrial IoT-based big data management and combines reinforcement tech-niques and federated learning to strengthen cloud security.

Incident Reaction & Mitigation the detection and security monitoring techniques assist in identifying the adverse events, the subsequent actions require the analysis of the encountered threat and responding to the vulnerability.

Threat Intelligence & Deception Technology considered more proactive methods, modern security management systems of-ten allows vulnerable spots within specific parts of the infrastructure or tracking mechanisms within the system to capture the behaviour or data flow from cybercriminals.

The ability of AI in such an environment with a large volume of unstructured data improves the accuracy of threat detection, reduces manual interventions, and exemplifies the prospect of AI in preventing sophisticated cyber-attacks.

CONFRONTS IN FULFILLING AI

Knowledge about those threat and vulnerabilities are also essential to maintain the adaptive and proactive defence mechanism to fight against the notorious portion of AI application to raise security concerns.

THREATS AND VULNERABILITIES

The legitimate purpose of AI in such a way is often diverted by cybercriminals to gain personal benefits. Advanced phishing attacks, automated hacking, sophisticated fraud, and manipulations are prime examples of AI targeted attacks with the help of AI.AI technology to reshape the cyber security methods to tackle modern, complex, and sophisticated attacks, the following limitations need to be addressed properly, and more research is indeed essential for improvements.

Potential Misuse of Artificial Intelligence

The increasing accessibility of AI tools and techniques means that the barrier to entry for cybercriminals is lowering, leading to more advanced and targeted cyber-attacks.AI can be ex-piloted to create sophisticated malware that adapts to security defences, automate large-scale phishing campaigns.

FUTURE DIRECTIONS

The future of cybersecurity lies in the ability to anticipate, adapt, and respond to these challenges effectively. Artificial Intelligence (XAI) plays a crucial role in the future direction of AI in cybersecurity. It addresses the challenge of the" black box" nature of deep learning models, aiming to make AI's decision-making transparent and under-standable.

CONCLUSION

The strength of AI can be maintained by the evolving cyber-attacks if the evolution of AI can be run at the same rate as the attacks. The possibility of integrating other technologies into the AI-integrated security applications, the threat actors can be defended effectively, or at least the impact can be minimized. AI in cybersecurity is transforming the workforce, steering it towards more intellectually demanding roles in this situation.

----END----