The Impact of Artificial Intelligence

Yafei Wang

CyberSecurity Service Provider Internship Program, ICS 296 & 396, Fall 2023

Advisors: Dr. Curtis Arnold, Chief Scientist – Cyber, & Dr. Robert Adamove, Sr. Associate, (Core4ce)

Problem Statement:

New technologies such as cloud computing and the Internet of Things are exacerbating the gap between cyber threats and traditional cybersecurity, creating an urgent need for innovative solutions that focus on the potential of artificial intelligence to effectively address these evolving challenges.

Purpose:

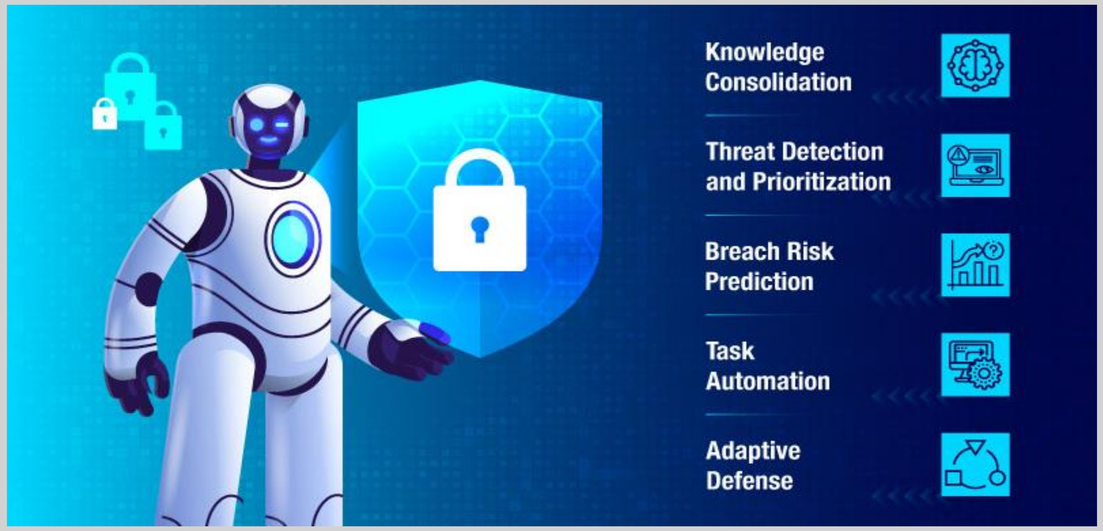
The study aims to collect and synthesize existing research, focusing on the evolving cybersecurity landscape. It seeks innovative solutions to protect digital assets and data, particularly through the application of artificial intelligence in cybersecurity.Understand the increasingly complex cybersecurity threats and the shortcomings of traditional security measures, and gain insights into the potential of artificial intelligence to solve and prevent cybersecurity incidents, thereby advancing knowledge in the field and suggesting directions for future innovation.

Approach:

Using multiple academic databases like ACM Digital Library, IEEE Xplore, and Google Scholar, chosen for their relevance to computer science, artificial intelligence, and cybersecurity. The search includes a carefully developed list of keywords and phrases such as cybersecurity, artificial intelligence, network security, and machine learning. Techniques like Boolean operators, phrase searches, and truncation are used for accurate search results. Filters in databases are strategically applied to refine results, focusing on the most relevant and credible sources. Additionally, gray literature, including reports and white papers, is considered for valuable insights.

Discussion & Conclusion:

Artificial intelligence plays an irreplaceable role in enhancing network security by moving from passive to proactive security measures, providing dynamic network protection.Ethical considerations and the collaboration between humans and artificial intelligence remain key points that need consideration.



Regardless of the Intern's methodology, knowledge does not derive from unverifiable generalities. Analysis occurs against the intern's research data and allows for the establishment of a conclusion or evidence that supports a shift or confirmation of beliefs, values, and understanding. Simple point is, you cannot make statements of generalities or opinion without the literature (which you cite) supporting or justifying your statements.

Path Forward:

Future research should enhance machine learning algorithms for anomaly detection and employ artificial intelligence for behavioral analysis of cyber attackers, aiming to improve network security. This includes systematic testing and creating frameworks to anticipate attacker actions.Evaluating AI on different platforms to understand whether they have the potential for cross-platform application.

References:

Cormier, A., & Ng, C. (2020, March 4). Integrating cybersecurity in hazard and risk analyses. Journal of Loss Prevention in the Process Industries.