X’Zaveion Owens

CYSE 201S

Professor Yalpi

February 16th,2025

AI IN CYBERSECURITY

Introduction

Artificial Intelligence (AI) technology creates vast revolutionary changes through its broad industrial applications according to this article. This review primarily explains the increased placement of AI in better cybersecurity resolutions. The examination demonstrates how AI technologies aid operators to detect sophisticated cyberthreats better while delivering exact and efficient blocking capabilities against these threats according to Haan (2023).

Conceptual Framework

This research mainly majors on Choi's Cyber Routine Activities Theory (RAT) to enlighten scholars and people in general on how cybercrime operates. The purpose of this research is to create a complete understanding of online criminal elements through an assessment of motivated offenders alongside potential targets and insufficient prevention methods meant to block these attacks.

Core Concepts

People who pursue cybercrime activities make up the category of motivated offenders. A target becomes suitable when it presents itself as an attackable entity. The system suffers from the absence of adequate protective controls which prevent successful attacks.

Cybercriminals use AI.

AI has two distinct functions since it serves cybersecurity purposes through effective applications yet cyber attackers use this power to fabricate phishing attacks and engineer complex malware for destructive intentions. The researchers focus their examination on technologies which include ChatGPT.

Methodology

The research combines quantitative forum data analysis with expert interview results for studying AI-based cybercrime patterns and their consequences.

Findings

The research shows how dark web forums together with their light web counterparts adopt the increasing utilization of AI-powered tools including Worm GPT along with ChatGPT. Worm GPT possesses the ability to produce intricate malware which acquires security defense knowledge during its existence before successfully avoiding detection systems for prolonged durations. The artificial intelligence system ChatGPT develops deceptive email messages and social engineering techniques which result in people revealing their personal information.

Cybercrime: Experts view

Better cyber hygiene along with ethical framework development for handling AI risks has driven experts to alter their views on AI technology according to qualitative interviews. Quantitative data merged with qualitative research proves the importance of tight regulation and immediate cyber cleaning procedures for the modern cybercrime world.

Recommendations

The report identifies two critical components that organizations need to implement to bolster their online safety measures through AI fellows and wide public understanding campaigns.

Conclusion

Immediate action should be taken mandatorily to address cybersecurity issues which continues to grow complex during fast technological advancement that now includes state of the art cybercrime powered by Artificial Intelligence. Cybercrime experts must put into place rules and policies aligning with AI's capabilities and they must also analyze the technological side of these coercions to build hands-on defense systems.

Citations

Haan, K. (2023, December 11). 24 top AI statistics and Trends in 2024. Forbes. Retrieved from https://www.forbes.com/advisor/business/ai-statistics

Shetty, S., Choi, K. C Park, I. (2024). Investigating the Intersection of AI and Cybercrime: Risks, Trends, and Countermeasures. International Journal of Cybersecurity Intelligence C Cybercrime, 7(2),