Are GPT-Powered AI Systems Superior to Traditional Cybersecurity Tools: Applications and Challenges

International Journal of Safety and Security Engineering • Article • *Open Access* • 2025 •
DOI: 10.18280/ijsse.150912

Abdelmaboud, Abdelzahir [a]; Salih, Sayeed [b]; Hashim, Aisha H. A. [b];
Almohamedh, Refan Mohamed [c]; Tajelsier, Hayfaa [d]; +1 author

[a] Humanities Research Center, Sultan Qaboos University, Muscat, 123, Oman

Abstract

Generative Pre-trained Transformer (GPT) models are revolutionizing cybersecurity by enhancing threat detection, risk evaluation, phishing defense, and automatic vulnerability analysis. This study delves into the various applications of GPT Technologies in security operations, emphasizing their competence in processing security information of large volume, anomaly detections, and providing real-time insights. Case studies cite quantifiable benefits: Anomaly detection by AI reached a high of 80% accuracy, malware and phishing classification 75–95% accuracy, and Microsoft Copilot reduced phishing attacks by 45% in commercial settings. VirusTotal and Cylance AI improved malware categorization accuracy by 38%, reducing false positives by 35%. Incident response effectiveness was improved by as high as 40% in reported deployments. However, GPT models are also exposed to adversarial exploitation, gaps in explanation, integration issues, and dependence on previous data.

This paper lists countermeasures, such as prompt engineering, fine-tuning, domain-specific training, and hybrid AI-human decision systems. Findings further highlight the significance of continuous updates, interdisciplinary collaboration with adherence to ethical frameworks to reap the full benefits of GPT-powered cybersecurity. So, take into consideration integrating these models into present security ecosystems. This way, organizations may strengthen their defenses, improve risk management, and make resilience against cyber threats.

Author keywords

cybersecurity; data privacy; generative AI; natural language processing; phishing prevention; risk management; threat detection

Funding details

Details about financial support for research, including funding sources and grant numbers as provided in academic publications.

Funding sponsor	Funding number	Acronym
Prince Sattam bin Abdulaziz University See opportunities by PSAU	PSAU/2025/R/1446	PSAU
Prince Sattam bin Abdulaziz University See opportunities by PSAU		PSAU

Funding text

This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2025/R/1446).

Corresponding authors

Corresponding author S. Salih

Affiliation Department of Electrical and Computer Engineering, Faculty of Engineering, International Islamic University Malaysia, Kuala Lumpur, 53100, Malaysia

Email address salih.sayd@gmail.com

Abstract

Author keywords

Funding details

Corresponding authors