

O USO DA INTELIGÊNCIA ARTIFICIAL NA DETECÇÃO DE AMEAÇAS CIBERNÉTICAS

Uma revisão bibliográfica

THE USE OF ARTIFICIAL INTELLIGENCE IN CYBER THREAT DETECTION

A Literature Review

Luciana Pinto Lima

Faculdades Integradas do Tapajós, FIT

E-mail: luuh_lymma@outlook.com

ORCID: 0009-0005-3001-4766

RESUMO

O avanço das tecnologias digitais tem ampliado significativamente a conectividade e a dependência de sistemas computacionais em diferentes setores da sociedade. Paralelamente, observa-se o crescimento de ameaças cibernéticas cada vez mais sofisticadas, tornando a segurança da informação um desafio para organizações e usuários. Nesse contexto, a Inteligência Artificial (IA) tem sido empregada como ferramenta de apoio na detecção e prevenção de ataques cibernéticos. O presente trabalho tem como objetivo analisar, por meio de revisão bibliográfica, as contribuições da IA para a identificação de ameaças em ambientes digitais. A pesquisa foi desenvolvida a partir da análise de livros e artigos científicos relacionados à segurança cibernética, aprendizado de máquina e detecção de anomalias. Os estudos consultados indicam que técnicas de aprendizado de máquina, redes neurais e detecção de anomalias contribuem para a identificação de comportamentos suspeitos, monitoramento de tráfego de rede e reconhecimento de padrões associados a ataques digitais. Observou-se que a aplicação da IA favorece a detecção de phishing, ransomware, invasões de rede e ataques de força bruta, permitindo respostas mais rápidas diante de incidentes. Apesar dos avanços, desafios relacionados à qualidade dos dados, interpretabilidade dos algoritmos e necessidade de atualização constante dos modelos ainda limitam sua aplicação. Conclui-se que a Inteligência Artificial representa uma importante aliada da segurança cibernética, contribuindo para o fortalecimento dos mecanismos de proteção digital.

Palavras-chave: Inteligência Artificial, Segurança Cibernética, Aprendizado de Máquina, Detecção de Ameaças.

ABSTRACT

The advancement of digital technologies has significantly increased connectivity and dependence on computer systems across different sectors of society. At the same time, cyber threats have become increasingly sophisticated, making information security a major challenge for organizations and users. In this context, Artificial Intelligence (AI) has been employed as a supporting tool for the detection and prevention of cyberattacks. This study aims to analyze, through a bibliographic review, the contributions of AI to threat identification in digital environments. The research was developed based on the analysis of books and scientific articles related to cybersecurity, machine learning, and anomaly detection. The studies reviewed indicate that machine learning techniques, neural networks, and anomaly detection methods contribute to the identification of suspicious behaviors, network traffic monitoring, and recognition of patterns associated with digital attacks. It was observed that the application of AI supports the detection of phishing, ransomware, network intrusions, and brute-force attacks, enabling faster responses to security incidents. Despite these advances, challenges related to data quality, algorithm interpretability, and the need for continuous model updates still limit its application. It is concluded that Artificial Intelligence represents an important ally in cybersecurity, contributing to the strengthening of digital protection mechanisms.

Keywords: Artificial Intelligence, Cybersecurity, Machine Learning, Threat Detection.

REFERÊNCIAS

CHANDOLA, V.; BANERJEE, A.; KUMAR, V. Anomaly Detection: A Survey. **ACM Computing Surveys**, v. 41, n. 3, Article 15, 2009.

JAIN, A. K.; GUPTA, B. B. Towards Detection of Phishing Websites on Client-Side Using Machine Learning Based Approach. **Telecommunication Systems**, v. 68, n. 4, p. 687–700, 2018.

SGANDURRA, D. *et al.* **Automated Dynamic Analysis of Ransomware: Benefits, Limitations and Use for Detection**. arXiv preprint arXiv:1609.03020, 2016.

SOMMER, R.; PAXSON, V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. *In: IEEE Symposium on Security and Privacy*. Washington, DC: IEEE, 2010. p. 305–316.

THIRIMANNE, S. P. *et al.* Deep Neural Network Based Real-Time Intrusion Detection System. **SN Computer Science**, v. 3, Article 145, 2022.