Enhancing Network Security through AI-Powered Automated Incident Response Systems

Bhargava Reddy Maddireddy, Bharat Reddy Maddireddy

ABSTRACT

In the rapidly evolving landscape of cybersecurity, the detection and mitigation of network security incidents have become paramount concerns for organizations worldwide. Traditional incident response approaches often rely on manual intervention and reactive measures, which are no longer sufficient to address the sophisticated and rapidly evolving nature of cyber threats.

To enhance network security and mitigate the risks posed by cyberattacks, there is a growing imperative to leverage advanced technologies such as artificial intelligence (AI) to develop automated incident response systems.

This paper presents a comprehensive exploration of AI-powered automated incident response systems and their role in enhancing network security. By integrating AI algorithms, machine learning techniques, and real-time threat intelligence, these systems offer the capability to detect, analyze, and respond to security incidents in a timely and proactive manner. Through automated decision-making and orchestration, AI-powered systems can effectively identify and mitigate security breaches, minimize response times, and reduce the impact of cyberattacks on organizations' networks and operations.

The key components of AI-powered automated incident response systems include advanced threat detection mechanisms, adaptive response strategies, and intelligent decision-making capabilities.

AI-powered systems can adapt their response strategies to mitigate emerging and previously unseen cyber threats effectively. Through a review of existing literature and case studies, this paper examines the implementation, benefits, and challenges of AI-powered automated incident response systems in real-world network security environments.

The findings highlight the potential of these systems to enhance threat detection accuracy, improve incident response efficiency, and strengthen overall network security posture. Moreover, the paper discusses ethical considerations, regulatory implications, and future research directions in the field of AI-driven network security, underscoring the need for responsible and transparent deployment of automated incident response systems to safeguard digital assets and protect against cyber threats in an increasingly interconnected world.

Systemization Of Knowledge (Sok)- Cross Impact Of Transfer Learning In Cybersecurity: Offensive ,Defensivean Threat Intelligence Perspectives

Sofiy Makara, Ali Dehghantanhaa, Fattane Zarrinkalamb, Gautam Srivastavac andAbbas Yazdinejada

ABSTRACT

Recent literature highlights a significant cross-impact between transfer learning and cybersecurity. Many studies have been conducted on using transfer learning to enhance security, leading to various applications in different cybersecurity tasks. However, previous research has focused on specific areas of cybersecurity. This paper presents a comprehensive survey of transfer learning applications in cybersecurity by covering a wide range of domains, identifying current trends, and shedding light on under-explored areas.

The survey highlights the significance of transfer learning in addressing critical issues in cybersecurity, such as improving detection accuracy, reducing training time, handling data imbalance, and enhancing privacy preservation. Additional insights are provided on the common problems solved using transfer learning, such as the lack of labeled data, different data distributions, and privacy concerns.

The paper identifies future research directions and challenges that require community attention, including the need for privacy-preserving models, automatic tools for knowledge transfer, metrics for measuring domain relatedness, and enhanced privacy preservation mechanisms. The insights and roadmap presented in this paper will guide researchers in further advancing transfer learning in cybersecurity, fostering the development of robust and efficient cybersecurity systems to counter emerging threats and protect sensitive information.

To the best of our knowledge, this paper is the first of its kind to present a comprehensive taxonomy of all areas of cybersecurity that benefit from transfer learning and propose a detailed future roadmap to shape the possible research direction in this area.