Cybersecurity Intrusion Detection Systems: A Comprehensive Survey on Combating Evolving Threats through Adversarial Attack Strategies

Ayoub Akennaf, Mounia Mikram

School of Information Science, Rabat, Morocco

Abstract:

Cyber dangers have become more common in recent years, making it even more important to have strong intrusion detection systems (IDS) that can find and stop hostile attempts. The goal of this paper is to repeat and expand on the results of the state of the art of Intrusion Detection Systems and Adversarial Attacks, which looked into how machine learning-based IDS can be hacked in different ways. We test how well different machine learning models work when they are attacked using well-known methods such as the fast gradient sign method, the Carlini and Wagner attacks, and projected gradient descent. Our study uses a wide range of experiments to check how well these attacks work and how strong the models are. In addition, we look into new ways to protect IDS against adversarial changes, such as adversarial training and feature reduction techniques. These will help IDS find threats more quickly. The goal of our repeat study is to add to the current conversation in the fields of hostile machine learning and cybersecurity by giving more information about the arms race between adversarial attacks and defense strategies. In the end, this study aims to give valuable direction that can help in developing IDS that are stronger and better able to protect against new cyber dangers.

Keywords:

Cybersecurity, fraud detection, cyber threats, Internet of Things, cloud computing.