Machine Learning Based Anomaly Detection System for Malicious e-Mail Activity in Defence Networks

Lt Col Yuvraj Singh
Defence Institute of Advanced Technology (DIAT) , Pune

Abstract:

Defence communication networks are prime targets for sophisticated e-mail–based cyberattacks, including spear-phishing, credential harvesting, covert data exfiltration & malware delivery through embedded attachments or links. Traditional signature-based and rule-based spam filters are inadequate in these environments, as modern adversaries continuously modify content, employ multilayer obfuscation, and mimic legitimate communication patterns to evade detection. This paper proposes a ML driven anomaly detection system designed specifically for malicious e-mail activity in defence networks, where resilience, low false-positive rates, privacy & operational reliability are critical.

The aim of this paper is to propose a comprehensive ML-based anomaly detection system tailored for malicious e-mail activity in defence networks, integrating the latest trends identified in the literature. Drive results towards improved robustness under adversarial perturbations and distribution shifts, which commonly occur in dynamic defence communication environments.This work contributes a comprehensive, scalable, and defence-ready ML anomaly detection framework capable of strengthening e-mail security in mission-critical networks. Spam filtering operates within an evolutionary scenario where spammers continuously employ adversarial techniques specifically tailored to minimize detection. Overall, this paper advances a scalable, multimodal, adversary-resilient, and defence-ready anomaly detection framework that aligns with the latest trajectory of e-mail security research. By integrating innovations such as GNN-based structure modelling, LLM-driven multi-agent reasoning, adversarial robustness & federated collaboration, this paper provides a next-generation foundation for strengthening email security in high-security defence networks.

Keywords:

e-mail, cyberattacks, ML driven, GNN, LLM, detection system.