Chapter 4
Email-Based Privilege Escalation Attack Detection in Cloud Environments Using Machine Learning

B. Sreedevi
https://orcid.org/0000-0003-1225-4238
SASTRA University, India

S. Barathi
https://orcid.org/0000-0002-9471-9491
Srinivasa Ramanujan Centre, India

ABSTRACT

Cloud computing offers scalable data access and operational efficiency but introduces serious security challenges—most notably, privilege escalation attacks where insiders gain unauthorized administrative control. This project presents a machine learning-based system to detect such attacks through email analysis. Email content is transformed into numerical features using vectorization techniques. Several classifiers including Random Forest, KNN, SVM, XGBoost, and LightGBM are trained on a labeled dataset to differentiate between safe and malicious emails. An ensemble

DOI: 10.4018/979-8-3373-5992-2.ch004

voting classifier ensures higher accuracy and reduces false positives. The system performs real-time detection and generates alerts for suspicious activities, thereby enhancing cloud security against internal threats.

1. INTRODUCTION

This work addresses the challenge of detecting insider threats and privilege escalation in cloud computing by leveraging machine learning (ML), particularly ensemble models such as Random Forest, AdaBoost, and LightGBM (a gradient boosting framework). LightGBM achieved a high detection accuracy of 97% using a customised CERT (Computer Emergency Response Team) dataset. Its strengths lie in its focus on insider threats, use of a realistic dataset, and comparative analysis of multiple ML models. However, limitations include a lack of real-time detection, restricted dataset generalisation, the absence of deep learning and explainability techniques, and a narrow focus on insider threats only. The proposed extension enhances the base methodology by incorporating real-time detection, combining LightGBM with anomaly detection methods such as Isolation Forest (an unsupervised anomaly detection algorithm), applying advanced feature engineering from system behaviour and logs, introducing role-based anomaly detection, and integrating visual dashboards for improved threat monitoring and response. (Homoliak et al., 2019; Butt et al., 2023).

2. LITERATURE SURVEY

The study titled "Detection of Insider Threats using Machine Learning on the CERT Dataset" explored various supervised machine learning (ML) models to detect insider activities, including privilege escalation. Techniques such as Random Forest, Decision Trees, and Support Vector Machine (SVM) were applied to user activity data, including email usage, access logs, and device logs. While detection rates were high, the study reported challenges in real-time deployment and maintaining accuracy across varied user behaviour profiles. Research on ensemble learning for