WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Privilege Escalation Attack Detection Mitigation in Cloud Using Machine Learning

[1]Nikhil, [2]Sai Abhiram, [3]Revanth Reddy , [4]Mr. Praveen S R

[1]Student, [2]Student, [3]Student, [4]Professor,
Department of Computer Science and Engineering, R. L. Jalappa Institute of Technology, Doddaballapur, Bengaluru, India

ABSTRACT

The proliferation of smart gadgets has led to an exponential increase in cyberattacks, which has made cybersecurity more difficult. Because of its centralized architecture and the volume of data that is shared between businesses and cloud providers, cloud computing poses hazards even as it is revolutionizing corporate processes. With legal access, malicious insiders are a serious risk since they can cause a great deal of harm by abusing their powers. In order to detect privilege escalation assaults, this paper suggests a machine learning-based insider threat detection system. To increase prediction accuracy, the system integrates several models through ensemble learning.A CERT insider threat dataset was used to test four machine learning algorithms: Random Forest (RF), AdaBoost, XGBoost, and LightGBM. With a 97% accuracy rate, LightGBM outperformed RF, AdaBoost, and XGBoost, which had respective accuracy rates of 86%, 88%, and 88.27%. LightGBM was the best overall, but in some assault scenarios, RF and AdaBoost fared better, indicating that combining algorithms is necessary for stronger, more reliable classification.

I. INTRODUCTION

This study examines machine learning algorithms—Random Forest, AdaBoost, XGBoost, and LightGBM—for detecting insider attacks. A customized dataset was used to train and evaluate these models, with LightGBM achieving the highest accuracy.The research highlights the need for intelligent algorithms to enhance security.It proposes a user-centered approach, focusing on realistic attack scenarios, preprocessing, model evaluation, and detailed reporting, making it a valuable contribution to insider attack detection. Cloud computing offers scalable services, but it also faces security risks, particularly from insider threats exploiting privilege escalation, which gives attackers greater access to sensitive data.

II. OBJECTIVES

- Develop a machine learning-based system to detect and classify privilege escalation attacks by insiders in cloud environments.
- Utilize advanced ML techniques to identify anomalies in user behavior and potential insider threats.

-Apply and evaluate four ML algorithms Random Forest, AdaBoost, XGBoost, and LightGBM—on a customized CERT dataset.

-Achieve higher detection accuracy and improve classification performance for insider attack scenarios.

-Enhance cloud security by mitigating insider threats through efficient and effective ML algorithms

III. EXISTING SYSTEM

Traditional rule-based techniques or isolated machine learning models are the mainstays of current solutions for identifying privilege escalation assaults in cloud environments. They frequently have trouble with unbalanced datasets, are unable to recognize small insider threats, and are not flexible enough to handle a variety of attack scenarios, such as vertical or horizontal privilege escalation. These restrictions expose businesses to complex attacks that take advantage of privileged access, underscoring the need for stronger cloud security detection systems.

IV. PROPOSED SYSTEM

The proposed system combines ensemble machine learning models—Random Forest, AdaBoost, XGBoost, and LightGBM—to detect privilege escalation attacks in cloud environments. It uses a customized CERT dataset to identify insider threats. The approach involves data preprocessing, feature selection, and classification for improved accuracy and fewer false positives. LightGBM achieves the highest accuracy of 97%, enabling detection of horizontal and vertical privilege escalations with a scalable and adaptable framework.

V. LITERATURE SURVEY

Cloud computing has revolutionized data storage and access, yet it also brings new security risks, especially from insider threats. Among these, privilege escalation attacks—where authorized insiders exploit their access to gain higher privileges—pose significant challenges. Such attacks are difficult to detect because insiders understand system operations and can behave subtly.

To tackle this problem, researchers have applied various machine learning (ML) techniques:

Random Forest (RF): Widely studied for its strong detection ability, RF provides high accuracy with a low rate of false alarms.

AdaBoost: This boosting method improves detection by combining multiple weak classifiers to create a more accurate model.

XGBoost and LightGBM: These advanced ensemble methods are effective at handling imbalanced datasets and offer faster training speeds.

Prior work by Kumar et al. utilized clustering along with feature selection techniques like Principal Component Analysis (PCA) and Random Forest to enhance malware detection, highlighting the critical role of data preprocessing. Similarly, Le and Zincir-Heywood demonstrated that supervised models such as Artificial Neural Networks (ANN) and Random Forest applied on detailed data could achieve strong detection results.

VI. SYSTEM ARCHITECTURE

1. Data Collection gathers system, email, and external device logs.

2. Data Preprocessing involves aggregation, normalization, and feature extraction.

3. Detection and Classification are performed using supervised ML algorithms like Random Forest, XGBoost, AdaBoost, and LightGBM.

Random Forest:-For reliable categorization, Random Forest constructs several decision trees and aggregates their results.

XGBoos:-Gradient boosting with regularization is used by XGBoost to increase speed and accuracy.

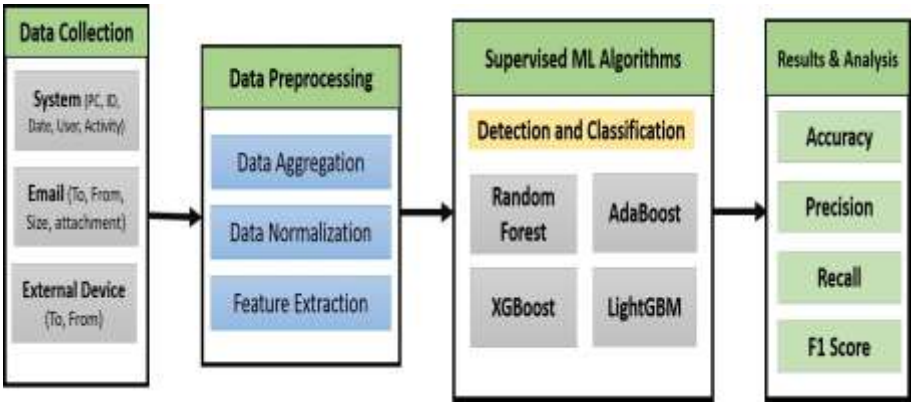
AdaBoost:-By concentrating on previously incorrectly classified data points, AdaBoost improves model performance.

LightGBM:-Achieves rapid and scalable gradient boosting through the use of histogram-based learning.

4.The model learns patterns indicating suspicious behavior.

5.The algorithms classify whether activity is normal or an attack.

6.Results & Analysis evaluate performance using accuracy, precision,recall and F1score



VII. RESULTS

1.The web-based system detects privilege escalation attacks using machine learning models.

2.Users input transaction data through a secure login interface for analysis.

3.The system evaluates the input and flags it as either safe or a potential insider threat.

4.It provides immediate feedback, enhancing real-time threat response capabilities.

VIII. CONCLUSION

The implementation of machine learning algorithms—Random Forest, AdaBoost, XGBoost,andLightGBM—enables accurate detection and mitigation of privilege escalation attacks in cloud environments. This approach ensures quicker identification of anomalies, strengthens data protection, and supports real-time decision-making. The intelligent model reduces human oversight and enhances security reliability in dynamic cloud infrastructures.

IX. REFERENCES

[1] U. A. Butt, R. Amin, H. Aldabbas, S. Mohan, B. Alouffi, and A. Ahmadian, ‘‘Cloud-based email phishing attack using machine and deep learning algorithm,’’ *Complex Intell. Syst.*, pp. 1–28, Jun. 2022.

[2] D. C. Le and A. N. Zincir-Heywood, ‘‘Machine learning based insider threat modelling and detection,’’ in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manag. (IM)*, Apr. 2019, pp. 1–6.

[3] P. Oberoi, ‘‘Survey of various security attacks in clouds based environ- ments,’’ *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 9, pp. 405–410, Sep. 2017.

[4] A. Ajmal, S. Ibrar, and R. Amin, ‘‘Cloud computing platform: Performance analysis of prominent cryptographic algorithms,’’ *Concurrency Comput., Pract. Exper.*, vol. 34, no. 15, p. e6938, Jul. 2022.

[5] U. A. Butt, R. Amin, M. Mehmood, H. Aldabbas, M. T. Alharbi, andN. Albaqami, ‘‘Cloud security threats and solutions: A survey,’’ *Wireless Pers. Commun.*, vol. 128, no. 1, pp. 387–413, Jan. 2023.

[6] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. Bilal, ‘‘Smart home security: Challenges, issues and solutions at different IoT layers,’’ *J. Supercomput.*, vol. 77, no. 12, pp. 14053–14089, Dec. 2021.