International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09i02.016 ISSN: 2581-4621

Enhancing Cloud Security with Machine Learning: Detection and Mitigation of Privilege Escalation Attacks

[1]Shaik Saleha Shireen, [2]Bushra Tahseen
[1]*M. Tech Student, Dept. Of. CSE, Dr. K.V. Subba Reddy Institute of Technology, Kurnool.*
[2]*Associate Professor, Dept. Of. CSE, Dr. K.V. Subba Reddy Institute of Technology, Kurnool.*

Abstract
Cloud security is a critical concern as cyber threats, particularly privilege escalation attacks, continue to rise. This paper presents a machine learning-based approach for detecting and mitigating privilege escalation attacks in cloud environments. The proposed system utilizes classification algorithms, including LightGBM, AdaBoost, XGBoost, and Random Forest, to identify malicious activities. The study demonstrates how these models improve threat detection accuracy and response efficiency. Experimental results show that LightGBM outperforms other models in detecting privilege escalation attacks with high precision.
Keywords: Privilege escalation, machine learning, random forest, adaboost, XGBoost, LightGBM, classification.

Introduction

Cloud computing has transformed the way businesses and individuals store, process, and manage data. Organizations increasingly rely on cloud-based services

due to their scalability, efficiency, and cost-effectiveness. However, security concerns remain a critical issue in cloud environments. One of the most severe threats is privilege escalation attacks, where an attacker gains unauthorized access to higher-level privileges, allowing them to perform malicious actions such as:

- Accessing sensitive data
- Modifying system configurations
- Installing malicious software
- Compromising other users' accounts

Understanding Privilege Escalation Attacks

Privilege escalation attacks occur when an attacker exploits vulnerabilities in the system to obtain unauthorized access to higher permissions. These attacks are classified into two types: **Vertical Privilege Escalation** – When an attacker gains higher access rights than they are authorized to.
Horizontal Privilege Escalation – When an attacker accesses another user's account with the same privilege level but without permission.
Such attacks often go undetected in traditional security systems, making machine learning (ML) a powerful tool for detecting and mitigating them.

Existing system

Recent studies have focused on detecting and identifying insider threats involving privileged access misuse. Researchers have tested various machine learning and deep learning techniques to tackle this issue, including SVM, Naïve Bayes, CNN, Linear Regression, PCA, and KNN. However, as attack methods keep evolving, there is a growing need for faster and more efficient algorithms. To stay ahead of these threats, a smart and reliable strategy is essential for detecting, classifying, and preventing insider attacks. Traditional machine learning methods for attack detection have several limitations. They cannot automatically design features, often have a low detection rate, and struggle to identify small variations of known attacks, including insider threats. Additionally, existing systems often generate a high number of false positives, where normal user activities are mistakenly flagged as attacks, leading to unnecessary disruptions.

Proposed system

In most cases, using an ensemble of models improves insider threat detection and classification compared to individual models. Combining multiple models helps reduce noise in the results, leading to greater consistency and robustness. Ensemble models are also capable of capturing both linear and non-linear patterns in the data by integrating different approaches. The proposed methodology uses well-known supervised machine learning algorithms such as RandomForest, AdaBoost, XGBoost, and LightGBM. These models analyze datasets to detect and classify insider threats. The implementation process includes several steps, such as dataset preprocessing, model training, testing, detection, and classification, ensuring a more reliable and accurate threat detection system.

Methodology

This study focuses on detecting privilege escalation attacks in cloud environments using machine learning techniques. The methodology follows a structured approach, involving dataset collection, data preprocessing, feature selection, machine learning model application, and model evaluation. The goal is to develop a highly accurate and efficient model for identifying insider threats.

1. Dataset Collection: The dataset used in this research is derived from multiple files of the CERT Insider Threat Dataset, specifically focusing on email-related information. This dataset includes user behaviors, system interactions, and email communication patterns to detect privilege escalation attempts.

2. Data Preprocessing: Dataset preprocessing is a crucial step in preparing raw data for effective machine learning model training. Since raw data often contains inconsistencies and redundant features, preprocessing ensures that the dataset is clean, structured, and optimized for machine learning. In this project, email-based data is preprocessed to enhance the accuracy of privilege escalation attack detection

Steps in Data Preprocessing

1. Data Aggregation: Logs from CERT Insider Threat dataset are merged to provide a holistic view of insider threats. Helps in identifying patterns across multiple data points.

2. Data Cleaning: Missing values, duplicate entries, and inconsistent data formats are removed. Ensures data integrity and reliability before feeding it into the machine learning models.

3. Data Normalization: Converts numerical attributes to a standardized scale to improve model performance. Example: Login frequency values may range from 1 to 1000, which must be normalized to avoid model bias.

4.FeatureEngineering&Transformation: Creates new relevant features based on existing data to improve threat detection accuracy. Example: Combining login timestamps to detect abnormal login patterns. Through these preprocessing steps, the dataset becomes structured, noise-free, and ready for machine learning applications

3. Feature Selection: Feature selection is crucial for improving the efficiency and accuracy of machine learning models. It helps in removing redundant data while retaining the most informative attributes. Objective of Feature Selection are to reduce computational complexity, improve model interpretability, enhance detection accuracy by focusing on relevant attack indicators. Here’s how each feature plays a role:

1. ID:Aunique identifier for each email.

2. Subject of Email: Helps analyze keywords that might indicate phishing or malicious intent

3. Email Message: The main content of the email, which is crucial for detecting suspicious behavior.

4. Date of Email Received: Useful for identifying attack patterns over time.

5. Labels: Indicates whether an email is classified as spam (potential attack) or normal behavior. These extracted features will be used for training your machine learning model to detect privilege escalation threats effectively. By eliminating irrelevant features, the model is optimized for faster training while maintaining high detection accuracy**.**

4. Data Labeling and Splitting:

Data labeling and splitting are critical steps in training a machine learning model for privilege escalation attack detection. This step ensures that the model learns to distinguish between normal user activities and malicious actions, enabling effective classification of security events. Properly labeled and partitioned data helps the model generalize well to new attack patterns in real-world cloud environments.

Data Labeling Process: Each data instance is assigned a binary label to indicate whether it represents normal behavior or a privilege escalation attack:

□ **Label 0 → Normal User Behavior:** Routine login activities from familiar IP addresses. Authorized privilege escalations by administrators. Expected system access patterns based on job roles.

□ **Label 1 → Privilege Escalation Attack:**

Unauthorized users gaining higher privileges without approval. Sudden administrative access granted to previously low-privilege accounts. Suspicious login attempts from unfamiliar or blacklisted IP addresses. Unusual command executions that modify security configurations. By labeling data accurately, the machine learning model can distinguish legitimate user actions from malicious privilege escalation attempts.

Data Splitting Process: Once labeled, the dataset is split into training and testing subsets to evaluate model performance. The dataset is divided as follows:

1. Training Set (80%): Used to train the machine learning model .It Contains both normal and attack data in a balanced ratio. The model learns patterns, correlations, and attack signatures from this dataset.

2. Testing Set (20%): Used to evaluate model accuracy and performance. It Includes unseen normal and attack cases to assess how well the model generalizes. The model is tested on real world attack scenarios without prior exposure to measure its ability to detect new threats.

5. Machine Learning Model Application To detect privilege escalation attacks, four supervised learning models are applied. Ensemble Learning Approaches

1. Bagging (Bootstrap Aggregating): Used in Random Forest to reduce variance and improve stability.

2. Boosting (Sequential Learning Enhancement): Applied in AdaBoost, XGBoost, and LightGBM to focus on misclassified instances and improve accuracy. Machine Learning Algorithms Used

1. Random Forest (Bagging Approach): Uses multiple decision trees to enhance classification accuracy. Reduces overfitting and handles imbalanced data well.

2. AdaBoost (Boosting Approach): Combines weak learners sequentially to focus on misclassified data points. Increases detection accuracy, especially for rare privilege escalation events.

3. XGBoost(Boosting Approach): An optimized boosting algorithm designed for speed and scalability. Handles large datasets efficiently while reducing false positives.

4. LightGBM (Boosting Approach): A gradient boosting model specialized for large-scale data processing. Faster training time with higher accuracy than traditional boosting methods. By leveraging ensemble learning techniques, the detection system becomes more robust against sophisticated insider threats.

6. ModelEvaluation & Performance Metrics :

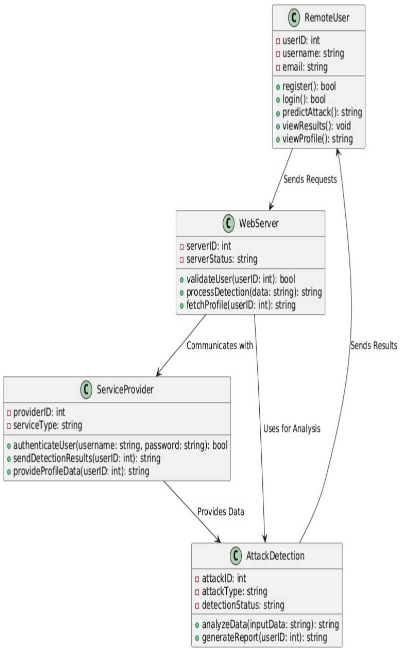
After training, each machine learning model is evaluated based on multiple performance metrics to determine its effectiveness in detecting privilege escalation attacks. Performance Metrics Used

- Accuracy → Measures the percentage of correctly classified instances.

- Precision → Determines the proportion of correctly identified threats out of total flagged cases
- . Recall (Sensitivity) → Identifies the percentage of actual attacks detected by the model.
- F1-Score → Balances precision and recall for an overall assessment of model performance.

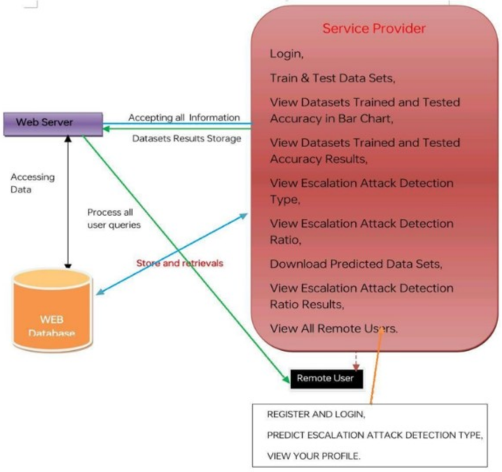
UML Diagrams

1. Class diagram



The RemoteUser class represents an end user interacting with the system, with attributes like userID, username, and email. It includes methods for registering, logging in, predicting attacks, and viewing results or profile data while communicating with the WebServer. The WebServer acts as a bridge between users and other components, managing authentication, processing attack detection, and fetching user profiles. It works closely with the ServiceProvider, which handles user authentication and profile management, verifying credentials, sending detection results, and providing profile data. The AttackDetection class processes attack-related data, analyzes threats, and generates reports, sending them to the WebServer for further processing**.**

Architecture:


Service Provider
Login,
Train & Test Data Sets,
View Datasets Trained and Tested Accuracy in Bar Chart,
View Datasets Trained and Tested Accuracy Results,
View Escalation Attack Detection Type,
View Escalation Attack Detection Ratio,
Download Predicted Data Sets,
View Escalation Attack Detection Ratio Results,
View All Remote Users.
Web Server
Accepting all Information
Datasets Results Storage
Accessing Data
Process all user queries
Store and retrievals
WEB Database
Remote User
REGISTER AND LOGIN,
PREDICT ESCALATION ATTACK DETECTION TYPE,
VIEW YOUR PROFILE.

- **User Registration & Login** – Users register and log in through a web interface. The system authenticates credentials and grants access to security functionalities, including attack detection results and risk monitoring.
- **Dataset Processing & Model Training** – The Service Provider trains machine learning models (LightGBM, AdaBoost, XGBoost, Random Forest) using stored datasets. These models analyze historical attack patterns and generate predictions. Accuracy is evaluated and visualized in bar charts for performance assessment.
- **Attack Detection & Prediction** – The trained models analyze real-time user activities, identifying suspicious behavior linked to privilege escalation. The Web Server processes user requests, and the models predict whether an action is normal or an attack. If an escalation attempt is detected, the system flags the activity and calculates an attack detection ratio.
- **Data Storage & Retrieval** – Detection results, trained datasets, and user profiles are securely stored in a web database. When users request attack detection results, the Web Server retrieves and presents the information through the Service Provider’s interface while ensuring secure access.
- **Visualization & Reporting** – The system provides real-time insights, including attack detection results, risk assessments, and model performance reports. Security professionals and remote users can view and download these reports for further analysis.
- **Continuous Learning & Improvement** – The system periodically updates training datasets with new attack patterns, retraining machine learning models to enhance accuracy. This continuous learning process reduces false positives and improves security efficiency over time.

FUTURE ENHANCEMENTS Integration with SIEM Systems: Integrating the privilege escalation attack detection system with Security Information and Event Management (SIEM) solutions enhances security monitoring and response capabilities by providing a centralized platform for analyzing security threats. SIEM tools, such as Splunk, IBM QRadar, and Microsoft Sentinel, collect and process security logs from various sources, including user activity and cloud services, to detect suspicious behavior in real time. This integration allows for faster detection and automated response to potential attacks, such as blocking unauthorized access or enforcing additional authentication steps. Additionally, SIEM systems help in correlating security events, enabling security teams to identify patterns of malicious activity across multiple systems. By maintaining a detailed record of security incidents, SIEM integration also supports forensic analysis and future threat prevention. Overall, this enhancement ensures a proactive security approach, improving the accuracy, efficiency, and effectiveness of threat detection and mitigation in cloud environments

CONCLUSION:

This project successfully presents a machine learning-driven approach for detecting and mitigating privilege escalation attacks in cloud environments, specifically through email-based data analysis. By leveraging advanced machine learning algorithms such as LightGBM, XGBoost, AdaBoost, and Random Forest, the system effectively classifies user activities as normal or suspicious. Among these, LightGBM demonstrated the highest accuracy, precision, recall, and F1 score, making it the most reliable model for detecting insider threats.The implementation of automated detection and response mechanisms ensures that unauthorized privilege escalations are quickly identified, helping organizations prevent security breaches before they cause significant damage. Additionally, the use of real-time monitoring enhances overall cloud security by continuously analyzing user behavior and taking proactive measures against potential threats. This research underscores the importance of machine learning, behavioral analysis, and automation in strengthening cloud security frameworks. As cloud adoption continues to grow, incorporating intelligent security solutions like this will play a crucial role in safeguarding sensitive data, minimizing risks, and ensuring compliance with cybersecurity standards.

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] Mehmood, H. Aldabbas, M. T. Alharbi and N. Albaqami, "Cloud security threats and solutions: A survey", Wireless Pers. Commun., vol. 128, no. 1, pp. 387-413, Jan. 2023.

[3] 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.

[4] S. Zou, H. Sun, G. Xu and R. Quan, "Ensemble strategy for insider threat detection from user activity logs", Comput. Mater. Continua, vol. 65, no. 2, pp. 1321-1334, 2020.

[5] . D. C. Le, N. Zincir-Heywood and M. I. Heywood, "Analysing data granularity levels for insider threat detection using machine learning", IEEE Trans. Netw. Service Manag., vol. 17, no. 1, pp. 30-44, Mar. 2020.

[6] Privilege Escalation Attack Detection and Mitigation in Cloud Using Machine Learning MUHAMMAD MEHMOOD1 , RASHID AMIN 1,2 , MUHANA MAGBOUL ALI MUSLAM 3 (Member, IEEE), JIANG XIE 4 , (Fellow, IEEE), AND HAMZA ABBAS 17 May 2023