International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 04 April-2026 | Impact Factor: 3.5

# Privilege Escalation Attack Detection and Mitigation in Cloud Using Machine Learning

**Dr. A.V.H. Sai Prasad**
Associate Professor,
Dept of CSE(DS) , CMR Technical Campus
Hyderabad, Telangana,
India
avsaiprasad.ds@cmrtc.ac.in

**Ms. N. Soujanya**
Assistant Professor,
Dept of CSE(DS), CMR Technical Campus Hyderabad,
Telangana, India
noundlasoujanya516@gmail.com

**G. Sruthi**
UG Student, Dept of CSE(DS),
CMR Technical Campus
Hyderabad, Telangana,
India
sruthiguvva25@gmail.com

**B. Maneesh Preetham**
UG Student, Dept of CSE(DS),
CMR Technical Campus
Hyderabad, Telangana, India
kkbehara1976@gmail.com

**T. Druva Sri**
UG Student, Dept of CSE(DS),
CMR Technical Campus
Hyderabad, Telangana, India
dhruvasree2830@gmail.com

**S. Sriman**
UG Student, Dept of CSE(DS),
CMR Technical Campus
Hyderabad, Telangana, India
shreemansamudrala@gmail.com

**How to Cite this Article**:
Vardhan1, T. A., Venkateshwarlu2, S. C. & Soujanya, N., Sruthi, G., Preetham, B. M., Sri, T. D. & Sriman, S. (2026). Privilege Escalation Attack Detection and Mitigation in Cloud Using Machine Learning. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.284



https://doi.org/10.55041/ijcope.v2i4.284

**ABSTRACT—** Because of the recent exponential rise in attack frequency and sophistication, the proliferation of smart things has created significant cyber security challenges. Even though the tremendous changes cloud computing has brought to the business world, its centralization makes it challenging to use distributed services like security systems. Valuable data breaches might occur due to the high volume of data that moves between businesses and cloud service suppliers, both accidental and malicious. Unlike outsiders, insiders possess privileged and proper access to information and resources. In this work, a machine learning-based system for insider threat detection and classification is proposed and developed a systematic approach to identify various anomalous occurrences that may point to anomalies and security problems associated with privilege escalation. By combining many models, ensemble learning enhances machine learning outcomes and enables greater prediction performance. Multiple studies have been presented regarding detecting irregularities and vulnerabilities in network systems to find security flaws or threats involving privilege escalation. But these studies lack the proper identification of the attacks. This study proposes and evaluates ensembles of Machine learning (ML) techniques in this context. This paper implements machine learning algorithms for the classification of insider attacks. A customized dataset from multiple files of the CERT dataset is used. Four machine learning algorithms, i.e., Random Forest (RF), Adaptive boosting(AdaBoost), Extreme Gradient Boosting(XGBoost), and Light Gradient Boosting Machine(LightGBM), are applied to that dataset and analyzed results. Overall, LightGBM performed best.

However, some other algorithms, such as RF or AdaBoost, may perform better on some internal attacks (Behavioral Biometrics attacks) or other internal attacks. Therefore, there is room for incorporating more than one machine learning algorithm to obtain a stronger classification in multiple internal attacks. Among the proposed algorithms, the LightGBM algorithm provides the highest accuracy of 97%; the other accuracy values are RF at 86%, AdaBoost at 88%, and XGBoost at 88.27%.

## INTRODUCTION

Cloud computing is a new way of thinking about how to facilitate and provide services through the Internet. The current financial crisis, as well as the expanding computing demands, have necessitated significant changes to the current Cloud Model in terms of data storage, processing, and display. Cloud computing prevents people from spending a lot on equipment maintenance and purchases by utilizing cloud infrastructure. Cloud storage providers adopt fundamental security measures for their systems and the data they handle, including encryption, access control, and authentication. Depending on the accessibility, speed, and frequency of data access, the cloud has an almost infinite capacity for storing any type of data in different cloud data storage structures. Sensitive data breaches might occur due to the volume of data that moves between businesses and cloud service providers, both inadvertent and malicious. The characteristics that make online services easy to use for workers and IT systems also make it harder for businesses to prevent unwanted access. To achieve vertical access control, the attacker may need to take various actions to overcome or override security restrictions. Vertical privileges controls are finer-grained versions of security models that implement business objectives like separation of roles and least privilege, as shown in Figure 2. An attacker, for example, takes control of an ordinary registered user on a network and tries to acquire administrative or root access. Anomaly activity on organizational systems or user accounts can be detected using behavioral analytics, which might signal intrusion or privilege escalation.

## I. PROBLEM DEFINITION

Cloud computing environments store large amounts of sensitive data and provide services to many users simultaneously. However, these systems are vulnerable to insider attacks and privilege escalation threats. Traditional security systems mainly focus on external threats and often fail to detect malicious activities performed by authorized users. Insider attackers can exploit system vulnerabilities and gain unauthorized privileges. Once they gain elevated access, they can steal confidential information, modify system data, or disrupt services. Therefore, there is a need for an intelligent system that can monitor user behavior, analyze system logs, and detect suspicious activities automatically. The problem addressed in this project is the detection and mitigation of privilege escalation attacks in cloud environments using machine learning techniques.

## 1.2 PROJECT FEATURES

This study proposes and evaluates ensembles of Machine learning (ML) techniques in this context. This paper implements machine learning algorithms for the classification of insider attacks. A customized dataset from multiple files of the CERT dataset is used. Four machine learning algorithms, i.e., Random Forest (RF), Adaboost, XGBoost, and LightGBM, are applied to that dataset and analyzed results. Overall, LightGBM performed best. However, some other algorithms, such as RF or AdaBoost, may perform better on some internal attacks (Behavioral Biometrics attacks) or other internal attacks. Therefore, there is room for incorporating more than one machine learning algorithm to obtain a stronger classification in multiple internal attacks. Among the proposed algorithms, the LightGBM algorithm provides the highest accuracy of 97%; the other accuracy values are RF at 86%, AdaBoost at 88%, and XGBoost at 88.27%.

### Related Work

Many researchers have proposed machine learning approaches for detecting cyber attacks and insider threats. One research study proposed a phishing email detection system using machine learning algorithms such as Support Vector Machine (SVM), Naïve Bayes, and Long Short Term Memory (LSTM). The system analyzed email content and classified messages as phishing or legitimate. Another study focused on

detecting insider threats by analyzing user behavior patterns in enterprise networks. The researchers used anomaly detection techniques to identify suspicious user activities. Some researchers have developed machine learning frameworks that analyze system logs and user access records to detect abnormal patterns that indicate malicious activities. Although these methods provide good detection accuracy, there is still a need for improved systems that can efficiently analyze large datasets and detect privilege escalation attacks in cloud environments.

## II. METHODOLOGY

The proposed system follows a structured approach to detect and mitigate privilege escalation attacks in cloud environments using machine learning techniques.

### 1. Data Collection

The system uses the **CERT Insider Threat Dataset**, which contains user activity logs such as login details, file access records, and system events. This dataset helps in identifying normal and malicious user behavior.

### 2. Data Preprocessing

The collected dataset is preprocessed to improve data quality. The steps include:

Handling missing values

Data cleaning

Feature selection

Normalization

After preprocessing, the dataset is split into:

**Training data (80%)**

**Testing data (20%)**

### 3. Model Training

Multiple machine learning algorithms are applied to train the system, including:

Random Forest

AdaBoost

XGBoost

LightGBM

CatBoost

Each model is trained using the training dataset to learn patterns of normal and malicious activities.

### 4. Model Evaluation

The performance of each algorithm is evaluated using different metrics such as:

Accuracy

Precision

Recall

F1-score

Confusion matrix is also used to analyze correct and incorrect predictions.

### 5. Result Comparison

All models are compared using graphical visualization techniques. This helps in identifying the best-performing algorithm for detecting privilege escalation attacks.

### 6. Attack Prediction

The best-performing model (LightGBM/CatBoost) is used to predict attacks on new or unseen data. The system classifies activities into: Normal behavior, Suspicious/Malicious behavior

### 7. Output Generation

Finally, the system provides: Prediction results , Graphical analysis , Performance comparison . This helps administrators take necessary actions to improve cloud security..

## III. PROPOSED SYSTEM

In propose paper to detect such insider attacks author of this paper employing ensemble machine learning algorithms such as Random Forest, LIGHTGBM, XGBOOST and ADABOOST. Among all algorithms LIGHTGBM is giving better accuracy and each algorithm performance is evaluated in terms of confusion matrix, accuracy, precision, recall and FSCORE

In propose paper author has used all traditional Ensemble algorithms so as extension we have utilized CATBOOST algorithm which is one of the advance ensemble algorithm and can give better accuracy.

## IV. IMPLEMENTATION DETAILS

The implementation phase is less creative than system design. It is primarily concerned with user training, and file conversion. The system may be requiring extensive user training. The initial parameters of the system should be modifies as a result of a programming. A simple operating procedure is provided so that the user can understand the different functions clearly and quickly. The different reports can be obtained either on the inkjet or dot matrix printer, which is available at the disposal of the user. The proposed system is very easy to implement. In general implementation is used to mean the process of converting a new or revised system design into an operational one.

### 4.1 ALGORITHMS USED

#### 4.1.1 RANDOM FOREST

Random Forest is a supervised machine learning algorithm that is widely used for classification and regression problems. It works by creating multiple decision trees during the training process and combining their results to produce a more accurate and stable prediction. Each tree is built using a random subset of the dataset and features, which helps reduce overfitting and improves model performance. In this project, the Random Forest algorithm is used to analyze user activity patterns and classify them as normal behavior or malicious insider activity. Due to its ability to handle large datasets and high-dimensional features, Random Forest is effective in detecting privilege escalation attacks in cloud environments.

#### 4.1.2 ADAPTIVE BOOSTING

AdaBoost, also known as Adaptive Boosting, is an ensemble learning technique that improves the performance of weak classifiers by combining them into a strong classifier. The algorithm works by training multiple models sequentially, where each new model focuses more on the data instances that were misclassified by the previous models. By adjusting the weights of incorrectly classified samples, AdaBoost gradually improves the accuracy of the final model. In this project, AdaBoost is used to enhance the detection of insider threats by giving more importance to difficult-to-classify user activity patterns. This helps in improving the overall classification accuracy and reliability of the system.

#### 4.1.3 EXTREME GRADIENT BOOSTING

XGBoost (Extreme Gradient Boosting) is an advanced machine learning algorithm that is known for its high performance and efficiency. It is based on gradient boosting techniques and uses an optimized implementation that improves speed and accuracy. XGBoost builds multiple decision trees sequentially, where each new tree tries to correct the errors made by the previous trees. The algorithm also includes regularization techniques that help prevent overfitting and improve model generalization. In this project, XGBoost is used to detect abnormal user behaviors in the cloud environment by analyzing large amounts of user activity data and identifying patterns that indicate possible insider threats.

#### 4.1.4 LIGHT GRADIENT BOOSTING MACHINE

LightGBM (Light Gradient Boosting Machine) is a fast and efficient gradient boosting algorithm developed to handle large-scale data and high-dimensional features. It uses a leaf-wise tree growth strategy, which allows the model to achieve higher accuracy while reducing training time. LightGBM is

especially useful for big datasets because it consumes less memory and provides faster processing compared to traditional boosting algorithms. In this project, LightGBM is used to analyze complex user activity logs and detect malicious behavior in cloud systems. Its ability to process large datasets efficiently makes it suitable for detecting insider threats and privilege escalation attacks.

### 4.1.5 CATEGORICAL BOOSTING

CatBoost (Categorical Boosting) is a powerful gradient boosting algorithm developed by Yandex. It is designed to handle categorical features efficiently and reduce prediction errors. CatBoost automatically processes categorical data without requiring extensive preprocessing, which simplifies the training process and improves model accuracy. The algorithm also reduces overfitting by using ordered boosting techniques. In this project, CatBoost is used to improve the detection of insider threats by accurately classifying user activities based on patterns in the dataset. Because of its strong performance and ability to handle complex datasets, CatBoost achieved the highest accuracy among the algorithms used in the project.

## V. EXPERIMENTAL RESULTS AND DISCUSSION

The following screenshots showcase the results of our project, highlighting key features and functionalities. These visual representations provide a clear overview of how the system performs under various conditions, demonstrating its effectiveness and user interface. The screenshots serve as a visual aid to support the project's technical and operational achievements.

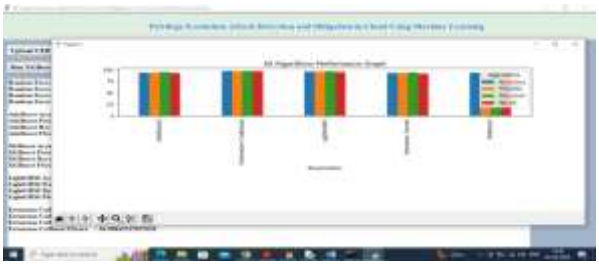
**System Interface – Home Page:**

To run project double, click on run.bat file to get below screen

**Fig. 1.Accuracy Page.**

In above screen LIGHTGBM got 95% accuracy and now run CATBOOST algorithm to get below output

**Fig. 2. Final Output Page**



In above graph x-axis represents algorithms names and y-axis represents accuracy and other metrics in different color bars and in all algorithms extension got high performance. Now Click on “Predict Attack from Test Data”

## VI. CONCLUSION

This project successfully implemented a machine learning based system for detecting privilege escalation attacks in cloud environments. The system analyzed user behavior data and used multiple machine learning algorithms to classify activities as normal or malicious. These algorithms are Random Forest, AdaBoost, XGBoost, and LightGBM. Using these supervised machine learning algorithms, this paper demonstrated the effective experimental results

having higher accuracy in the classification report. Among the proposed algorithms, the LightGBM algorithm provides the highest accuracy of 97%; the other accuracy values are RF with 86%, AdaBoost with 88%, and XGBoost with 88.27%. In the future, the proposed models may increase their performance by expanding the dataset in size and diversity in terms of its features and the new trends of insider attackers to perform the attack.

## VII. FUTURE SCOPE

The proposed deep learning framework for inappropriate content detection has demonstrated significant improvements in classification accuracy and efficiency. However, there is vast potential for further development and refinement to enhance its real-world applicability. Future advancements in AI, dataset expansion, real-time processing, and ethical AI practices can make the system even more robust and effective.

These are some future aspects: Expansion of Inappropriate Content Categories, Real- Time Content Moderation, Integration with Video-Sharing, Improvement in Explainability and Transparency, Cross-Language and Cross-Cultural Adaptation, Privacy and Ethical Considerations, Continuous Learning and Model Adaptation, Hybrid AI-Human Moderation System.

## VIII.ACKNOWLEDGMENT

We take this opportunity to express our gratitude to the people who have been instrumental in the successful completion of this project, we take this opportunity to express our profound gratitude and deep regard to our guide **Dr. A.V.H Sai Prasad**, Designation for his/her exemplary guidance, monitoring and constant encouragement throughout the project work. The blessing, help and guidance given by him/her shall carry us a long way in the journey of life on which we are about to embark.

We also take this opportunity to express a deep sense of gratitude to the Project Review Committee (PRC) coordinators **N. Soujanya, Shafana Bakshi,**
for their cordial support, valuable information and guidance, which helped us in completing this task through various stages.

We are also thankful to **Dr. K. Murali**, Head, Department of Computer Science and Engineering (Data Science) for providing encouragement and support for completing this project successfully.

We are deeply grateful to **Dr. A. Raji Reddy**, Director, for his cooperation throughout the course of this project. Additionally, we extend our profound gratitude to **Sri. Ch. Gopal Reddy**, Chairman, **Smt. C. Vasantha Latha**, Secretary and
**Sri. C. Abhinav Reddy**, Vice-Chairman, for fostering an excellent infrastructure and a conducive learning environment that greatly contributed to our progress.

The guidance and support received from all the members of CMR Technical Campus who contributed to the completion of the project. We are grateful for their constant support and help.

Finally, we would like to take this opportunity to thank our family for their constant encouragement, without which this assignment would not be completed. We sincerely acknowledge and thank all those who gave support directly and indirectly in the completion of this project.

## IX. REFERENCES

[1] Securing Cloud Environments: A Machine Learning Approach To Privilege Escalation Detection - https://www.ijcnis.org/index.php/ijcnis/article/view/8432/2509?utm_source=chatgpt.com&__cf_chl_tk=9VUAGo3b4M5vCZoo9Q_O8I_F.TYXU0hWfSUH4eHimfE-1774639584-1.0.1.1-QmhOTErei7zfzyAI20LNS1dkXEiy.3gNvm9ugwK0Z3U

[2] Practical Machine Learning for Cloud Intrusion Detection: Challenges and the Way Forward - https://arxiv.org/abs/1709.07095

[3] Machine Learning-Based Insider Threat Detection - https://ieeexplore.ieee.org/document/8737460

[4] Detection and Mitigation of Privilege Escalation Attacks Using ML - https://ijetms.in/Vol-9-issue-2/Vol-9-Issue-2-16.pdf?utm_source=chatgpt.com

[5] ML-Based Intrusion Detection System for Cloud Security - https://www.ijcrt.org/papers/IJCRT24A4367.pdf?utm_source=chatgpt.com

[6] Machine Learning-Driven Privilege Escalation Detection Framework - https://easychair.org/publications/preprint/JHg8/open?utm_source=chatgpt.com

[7] Automating Privilege Escalation with Deep Reinforcement Learning - https://arxiv.org/abs/2110.01362

[8] Machine Learning for Cloud-Based Privilege Escalation Detection - https://turcomat.org/index.php/turkbilmat/article/view/14787

[9] Privilege Escalation Attack Detection and Mitigation in Cloud Using Machine Learning - https://www.researchgate.net/publication/370616797_Privilege_Escalation_Attack_Detection_and_Mitigation_in_Cloud_using_Machine_Learning

## X. GITHUB REPOSITORY LINK

https://github.com/sruthi619/IOMP-A4