

# Effective Strategies for Security Privileged Access in Cloud Environment

<sup>1</sup>Mr. N. Harini, <sup>2</sup>Saripalli Dhanusha, <sup>3</sup>Gorakala Kavya, <sup>4</sup>Challa Bhuvaneshwari, <sup>5</sup>Kotta Usha, <sup>1</sup>Assistant Professor, <sup>1,2,3,4,5</sup> Department of Computer Science and Engineering, Vignana's Institute of Engineering for Women, Visakhapatnam, Andhra Pradesh, India

## ABSTRACT

As organizations rely more on remote work capabilities and larger cloud systems, their vulnerability to cyberattacks increases. Privilege escalation attacks are a prevalent and complex threat, and any network can become a target. Organizations need multiple defense strategies when any asset can become an entry point for intruders. This research addresses the pressing challenge of privilege escalation attacks in cloud computing, proposing an advanced detection and mitigation framework employing machine learning techniques, including AdaBoost, Random Forest, XGBoost, and LightGBM. Leveraging ensemble learning, the framework combines the strengths of these classifiers to enhance the accuracy and adaptability of detecting diverse privilege escalation patterns within cloud environments. The training dataset encompasses a comprehensive set of features, including system logs, user behavior analytics, and network traffic data, enabling the models to learn both normal and malicious behaviors associated with privilege escalation. The ensemble approach ensures a robust and dynamic defense mechanism, well-suited for the evolving nature of security threats in cloud infrastructures. This project emphasizes the proactive mitigation of privilege escalation attacks by integrating real-time response mechanisms based on ML model predictions. The proposed solution contributes to the advancement of cloud security by not only enhancing detection accuracy but also providing a responsive and adaptive approach to counteracting privilege escalation attempts.

**Keywords:** Privilege Escalation, Adaboost, LightGBM, Random Forest, XGBoost, Ensemble Learning

## INTRODUCTION

The escalating frequency and complexity of cyberattacks in tandem with the widespread adoption of smart technologies have presented significant cybersecurity challenges. While cloud computing has revolutionized business operations, its centralized nature poses hurdles in deploying distributed security systems effectively. This centralized model increases the risk of data breaches due to the substantial volume of data exchanged between businesses and cloud service providers, both inadvertently and maliciously. Insider threats emerge as a critical concern as malicious insiders possess elevated access levels, presenting opportunities for substantial damage. In response, this work proposes a machine learning-based system tailored for insider threat detection and classification, focusing on identifying anomalous behaviors indicative of privilege escalation-related security issues. Ensemble learning techniques are explored to improve prediction accuracy, utilizing a customized dataset derived from the CERT dataset. Through the application and analysis of four machine learning algorithms (Random Forest, Adaboost, XGBoost, and LightGBM), with LightGBM showcasing the highest accuracy at 97%, this study underscores the efficacy of employing multiple algorithms to strengthen classification capabilities, especially concerning diverse internal attack vectors.

## LITERATURE SURVEY

Le et al. [9] discussed that insider threats are among the most expensive and difficult-to-detect forms of assault since insiders have access to a company's networked systems and are familiar with its structure and security processes. A unique set of challenges face insider malware detection, such as extremely unbalanced data, limited ground truth, and behavioral drifts and shifts. Machine learning is used to analyze data at several levels of detail under realistic situations to identify harmful behaviors, especially malicious insider attacks. Random Forest beats the other ML methods, achieving good detection performance and F1-score with low false positive rates in most situations. The proposed work achieved an accuracy of 85% and a false positive rate of only 0.78%.

Janjua et al. [10] discussed that preventing malicious insiders from acting maliciously in an organization's system is a significant cybersecurity challenge. The paper's main goal is to use several Machine Learning approaches to classify email from the TWOS dataset. The following supervised learning techniques that have been used on the dataset are Adaboost, Naïve Bayes (NB), Logistic Regression (LR), KNN, Linear Regression (LR), and Support Vector Machine (SVM). Experiments reveal that AdaBoost has the best classification accuracy for harmful and non-malicious emails, with a 98% accuracy rate. Although the model was trained on the original dataset, the data is limited. The model's results may be improved if the dataset is bigger.

Le and Zincir-Heywood [2] discussed that insider threat actions could be taken intentionally or accidentally, like information system sabotage or irresponsible working with cloud resources. One of the difficulties in researching insider threats is that a malicious insider has access to the organization's network systems and is familiar with its security processes. To assist cybersecurity experts in detecting harmful insider activity on unseen data, ANN, RF, and LR machine learning techniques are taught on finite ground truth. User-session data looks to be the greatest choice for data granularity since it enables a system with a significant malicious insider detection rate and quick response times. They used machine learning techniques such as RF and ANN, which performed well in this work. Because RF provides excellent precision, it can be used when manpower for examining alerts is restricted.

## EXISTING METHOD

Before the development of our project's , the prevailing systems for detecting and mitigating Privileged Escalation attacks in cloud environments typically comprised several approaches. Anomaly Detection systems were commonly used, employing algorithms to spot unusual patterns in system logs, user activities, and network traffic that might signal potential privilege escalation attempts. However, these systems often faced challenges such as high false positive rates and the need for meticulous tuning to remain effective. Rule-based Models were another prevalent strategy, relying on predefined conditions or thresholds to identify suspicious activities related to privilege escalation. Although straightforward to implement, they often lacked the adaptability needed to detect complex or evolving attack patterns. Unsupervised Learning techniques, including clustering and autoencoders, were utilized to uncover patterns or anomalies in data without labeled examples. While useful for detecting unknown threats, these models sometimes struggled with interpretability and required human validation. Ensemble Methods, such as AdaBoost, Random Forests, XGBoost, and LightGBM, were also employed to improve detection accuracy and robustness by combining predictions from diverse classifiers. Despite their effectiveness, deploying ensemble models could demand substantial computational resources and expertise.

## PROPOSED METHOD

The system's advanced detection framework employs machine learning algorithms to effectively identify privilege escalation patterns in cloud environments. Integrating powerful techniques such as AdaBoost, Random Forest, XGBoost, LightGBM, and a Voting Classifier significantly enhances accuracy and adaptability across a wide range of privilege escalation behaviors. Through ensemble learning, the system synergistically combines the strengths of these classifiers, improving overall detection performance and system robustness by aggregating predictions and ensuring reliable detection

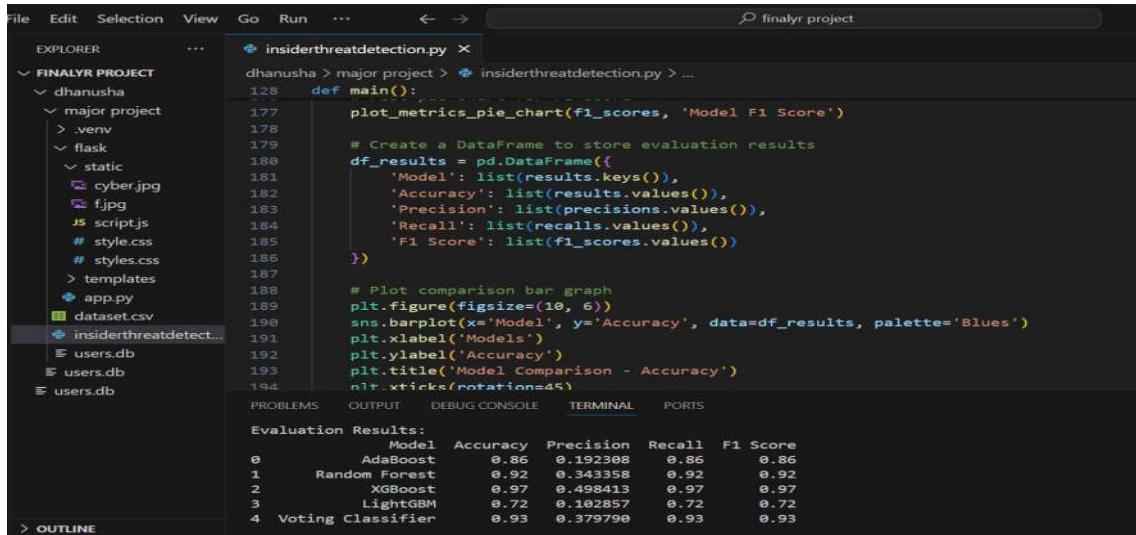
outcomes. This capability is further reinforced by a rich training dataset encompassing system logs, user behavior analytics, and network traffic data, enabling the machine learning models to discern between normal and malicious behaviors associated with privilege escalation. Moreover, the system emphasizes proactive mitigation by integrating real-time response mechanisms based on machine learning predictions, enabling swift and adaptive countermeasures against privilege escalation attempts and minimizing potential security breaches. Its dynamic defense mechanism continuously refines detection algorithms based on real-time data, ensuring effective adaptation to the evolving threat landscape within cloud infrastructures. These combined features make it a robust and effective solution for addressing complex security challenges in cloud computing environments.

## **THE DESIGN STRUCTURE OF THE COMPARATORS**

The design structure of the comparators in our project involves a systematic integration of diverse machine learning algorithms to form a cohesive ensemble learning framework for privilege escalation attack detection. Each comparator, including Random Forest, XGBoost, LightGBM, AdaBoost, and the Voting Classifier, contributes distinct strengths to the overall system. Random Forest, known for its robustness to overfitting and ability to handle large datasets, forms a fundamental component ensuring reliable base predictions. XGBoost, a gradient boosting algorithm, excels in capturing complex relationships and boosting model performance through iterative learning. LightGBM, optimized for speed and efficiency, enhances scalability while maintaining accuracy, crucial for real-time processing in cloud environments. AdaBoost's focus on weak learners and ensemble aggregation strengthens model diversity and resilience against varied attack scenarios. The Voting Classifier combines predictions from multiple models using majority voting, leveraging the collective intelligence of individual classifiers for enhanced accuracy and generalization. This structured integration of comparators ensures a balanced approach, leveraging the unique capabilities of each algorithm to achieve robust and adaptable privilege escalation attack detection within cloud computing contexts.

## **RESULT ANALYSIS**

The incorporation of machine learning algorithms such as Random Forest, XGBoost, LightGBM, AdaBoost, and a Voting Classifier into the Privilege Escalation Attack Detection System represents a robust and versatile approach to cybersecurity. By leveraging ensemble learning techniques and a diverse set of classifiers, the system demonstrates a high degree of accuracy and adaptability in detecting privilege escalation attacks within cloud environments. The integration of user authentication functionalities, including signup and login interfaces, adds a layer of security and ensures that only authorized users can access the prediction system. Upon inputting email content, the system's predictive capabilities swiftly determine the presence of privilege escalation threats, empowering organizations with timely insights to preemptively respond and fortify their security postures. This holistic approach not only enhances detection accuracy but also contributes to a proactive defense strategy crucial for safeguarding sensitive information and maintaining the integrity of cloud infrastructures.



```
def main():
    plot_metrics_pie_chart(f1_scores, 'Model F1 Score')

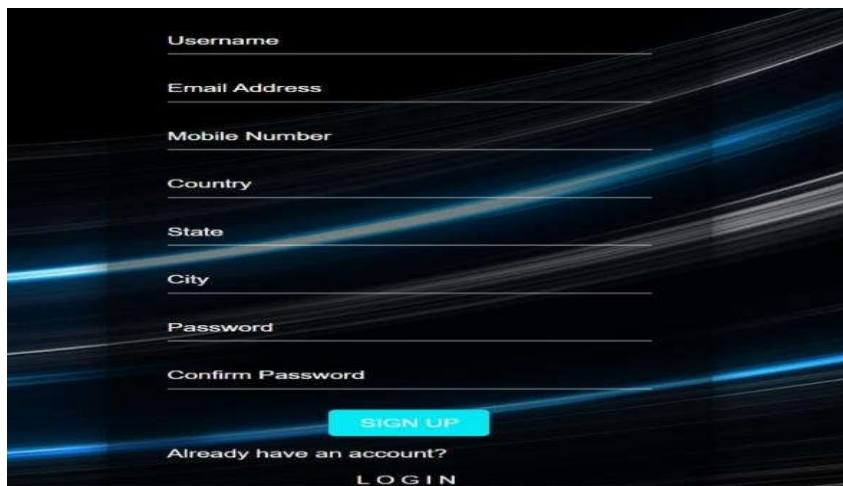
    # Create a DataFrame to store evaluation results
    df_results = pd.DataFrame({
        'Model': list(results.keys()),
        'Accuracy': list(results.values()),
        'Precision': list(precisions.values()),
        'Recall': list(recalls.values()),
        'F1 Score': list(f1_scores.values())
    })

    # Plot comparison bar graph
    plt.figure(figsize=(10, 6))
    sns.barplot(x='Model', y='Accuracy', data=df_results, palette='Blues')
    plt.xlabel('Models')
    plt.ylabel('Accuracy')
    plt.title('Model Comparison - Accuracy')
    plt.xticks(rotation=45)
```

Terminal Output:

	Model	Accuracy	Precision	Recall	F1 Score
0	AdaBoost	0.86	0.192308	0.86	0.86
1	Random Forest	0.92	0.343358	0.92	0.92
2	XGBoost	0.97	0.498413	0.97	0.97
3	LightGBM	0.72	0.102857	0.72	0.72
4	Voting Classifier	0.93	0.379790	0.93	0.93

Figure 1. Displaying the evaluation results



Username

Email Address

Mobile Number

Country

State

City

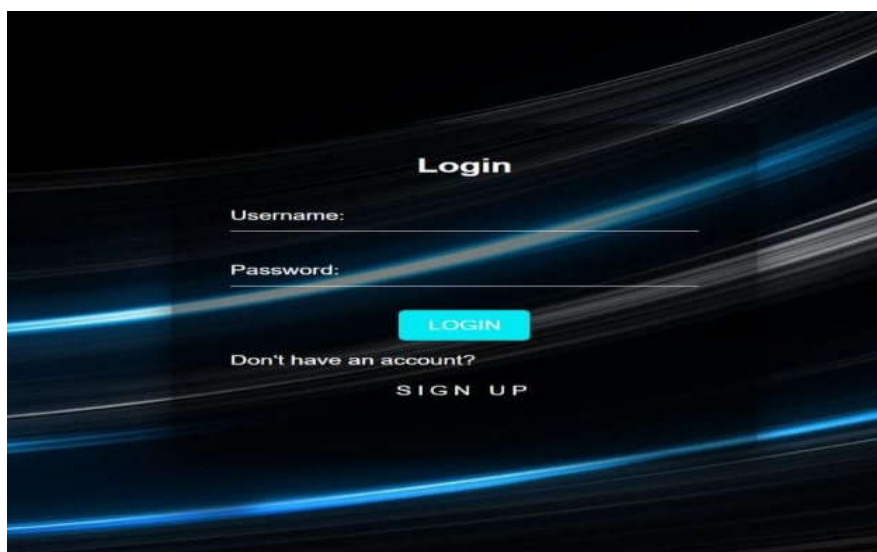
Password

Confirm Password

**SIGN UP**

Already have an account?  
**LOGIN**

Figure 2. Signup page



**Login**

Username:

Password:

**LOGIN**

Don't have an account?  
**SIGN UP**

Figure 3. Login page



Figure 4. Displaying Interface



Figure 5. Bar diagrams



Figure 6. Line charts



Figure 6. Pie Charts

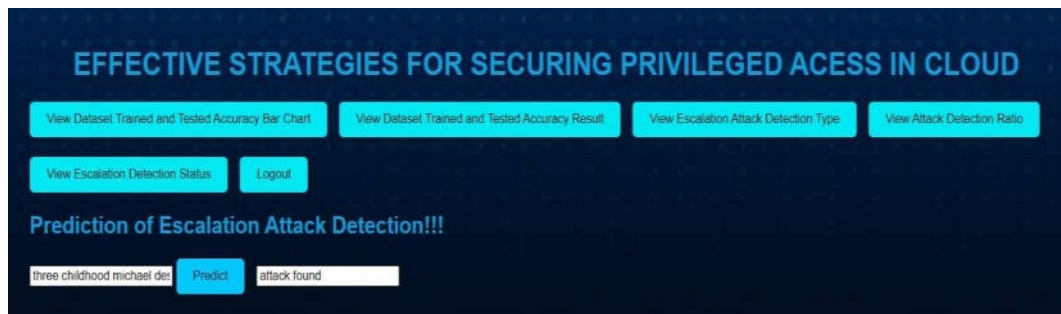


Figure 7. Privilage escalation attack found result

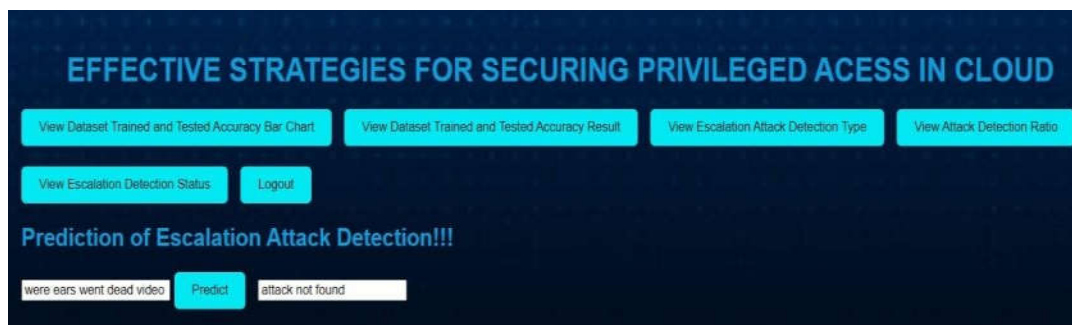


Figure 8. Privilage escalation attack not found result

## CONCLUSION

This project represents a comprehensive approach to addressing the escalating threat of privilege escalation attacks in cloud computing environments. By employing advanced machine learning algorithms such as Random Forest, XGBoost, LightGBM, AdaBoost, and a Voting Classifier, we have created a robust framework capable of accurately detecting diverse privilege escalation patterns within cloud infrastructures. The integration of user authentication features in the interface ensures secure access, allowing users to input email content for analysis regarding the presence of privilege escalation attacks. The ensemble learning techniques employed have shown promising results in terms of accuracy, precision, recall, and F1 scores, showcasing the effectiveness of our detection and mitigation strategies. Furthermore, the real-time response mechanisms based on machine learning predictions provide proactive defense measures, contributing significantly to overall cybersecurity resilience. Moving forward, continuous refinement of the models and interface based on feedback and emerging threats will enhance the framework's capabilities in safeguarding cloud systems from evolving security challenges. This project underscores the importance of leveraging advanced technologies and proactive measures in mitigating cybersecurity risks in modern cloud environments.

## 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 environments," *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, and N. 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.
- [7] 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.
- [8] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, "On the effectiveness of machine and deep learning for cyber security," in *Proc. 10th Int. Conf. Cyber Conflict (CyCon)*, May 2018, pp. 371–390.
- [9] D. C. Le, N. Zincir-Heywood, and M. I. Heywood, "Analyzing data granularity levels for insider threat detection using machine learning," *IEEE Trans. Netw. Service Manag.*, vol. 17, no. 1, pp. 30–44, Mar. 2020.
- [10] F. Janjua, A. Masood, H. Abbas, and I. Rashid, "Handling insider threat through supervised machine learning techniques," *Proc. Comput. Sci.*, vol. 177, pp. 64–71, Jan. 2020.