International Journal of Scientific Research and Engineering Development-– Volume 8 Issue 4, July-Aug 2025
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Proactive Detection of Privilege Escalation Attacks in Cloud Platforms

Komarapu Bhanuprasanna*, Dr. V. Uma Rani**, Dr. Sunitha Vanamala***
*(Post Graduate Student, M.C.A Department of Information Technology, Jawaharlal Nehru Technological University, Hyderabad, Email: bhanuprasannakomarapu@gmail.com)
** (Professor & Head of DIT, Department of Information Technology, Jawaharlal Nehru Technological University Hyderabad Email: umarani@jntuh.ac.in)
***(Lecturer, Department of Computer Science, TSWRDCW, Warangal East, Warangal, Telangana, India Email: sunithavanamala@gmail.com)

----------**********----------

Abstract:

With the rapid growth in both the frequency and complexity of cyber-attacks, the widespread adoption of smart devices has introduced serious security concerns. Although cloud computing has significantly transformed the business landscape, its centralized architecture poses challenges for implementing distributed services, especially in areas like security management. Among these risks, insider threats are particularly critical, as insiders have legitimate access to sensitive systems and data, giving them the potential to cause substantial harm compared to external attackers.

This project focuses on detecting privilege escalation attacks in cloud platforms using machine learning. A detection pipeline is implemented to analyze user activities and classify them as either normal or malicious. For validation, the KDD Cup '99 intrusion dataset from Kaggle, which contains diverse attack scenarios, is utilized. Multiple classifiers including SVM, Random Forest, MLP, AdaBoost, Decision Tree, GNB, Gradient Boosting, and Logistic Regression are trained and evaluated. Experimental results indicate that MLP and SVM achieve the best performance with a weighted F1-score of approximately 0.93, while GNB performs the least effectively. The system is integrated with a Flask application that enforces access control by automatically blocking or granting key delivery based on the predictions.

Keywords — Cloud Computing, Insider Threats, Privilege Escalation, Machine Learning, Intrusion Detection, Support Vector Machine, Classification

----------**********----------

I. INTRODUCTION

Cloud computing has significantly transformed how organizations store, manage, and process data, offering greater scalability and efficiency. However, this technological shift also introduces new cyber security concerns, particularly insider threats. These threats, posed by individuals with authorized access to internal systems, can cause severe damage by compromising data confidentiality and system integrity. Traditional security mechanisms often fall short in identifying such threats due to their complex and evolving nature, making it essential to explore more advanced and adaptive security solutions. This study focuses on the detection and mitigation of insider threats in cloud environments using advanced techniques such as machine learning and behavioural analytics. By integrating cyber security principles with modern data-driven approaches, the research aims to provide a comprehensive understanding of insider threat dynamics and develop proactive strategies for identifying and neutralizing such risks. This interdisciplinary approach supports the creation of more resilient and secure cloud infrastructures, enhancing the overall defence posture against internal security breaches

A. LITERATURE REVIEW

S. Nagendrudu et al. [1] explored the use of machine learning for detecting insider threats in cloud environments. Their work highlighted the limitations of single-model approaches and proposed that integrating multiple classifiers could strengthen anomaly detection. However, the study did not provide robust attack categorization, leaving scope for more refined detection mechanisms.

A. Veera Yugandhar Reddy et al. [2] advanced this direction by applying ensemble learning techniques, including Random Forest, AdaBoost, XGBoost, and LightGBM, on a customized CERT dataset. Their results demonstrated that LightGBM achieved the

highest accuracy (97%), though other models like Random Forest and AdaBoost were more effective for certain insider behaviors. This underscores the importance of adaptive, multi-model frameworks for handling diverse insider threats.

Similarly, Muhammad Mehmood et al. [3] emphasized ensemble-based detection for privilege escalation attacks. Their study also validated the superior performance of LightGBM (97% accuracy) over other classifiers on the CERT dataset, but noted that algorithms such as Random Forest and AdaBoost performed better in specialized scenarios like behavioral biometrics–based threats. This suggests that combining models can significantly improve detection performance compared to using a single classifier.

B. EXISTING SYSTEM:

Current systems emphasize the necessity of securing cloud platforms due to the wide range of applications operating simultaneously on shared infrastructure. Ensuring both security and reliability in such a dynamic environment is complex. One notable approach includes the use of Trend Micro Locality Sensitive Hashing (TLSH), a clustering-based malware detection technique. This method relies on Cuckoo Sandbox, which performs dynamic analysis by executing files in an isolated environment to observe their behaviour.

Another focus in existing research is the challenge of detecting insider threats, which are among the most damaging and hardest to identify. The detection of insider-related malware is further complicated by issues such as imbalanced datasets, minimal labelled data (ground truth), and the evolving nature of user behaviour over time.

C. PROPOSED SYSTEM:

The proposed system introduces a user-oriented machine learning framework designed to detect insider threats in cloud environments by simulating real-world conditions. Unlike traditional approaches that rely on idealized training scenarios, this system adopts a realistic methodology by encompassing data collection, preprocessing, and analysis through machine learning techniques. It strengthens cloud security by inspecting network packet content before storage or transfer, ensuring that each packet is thoroughly analysed and classified as safe or malicious. Based on these classifications, the system enforces intelligent access control, allowing only safe data to be transmitted or stored, while blocking malicious packets. This proactive and adaptive approach enables the detection of privilege escalation and insider threats more effectively, thereby reducing the risk of data breaches and improving the resilience of cloud infrastructures

I. METHADOLOGY

The proposed architecture for proactive detection of privilege escalation attacks in cloud platforms integrates multiple machine learning models with a feature-driven detection engine. This hybrid framework ensures accurate and adaptive classification of network packets as safe or malicious, even in dynamic and high-dimensional cloud environments. The architecture consists of data collection from network traffic, preprocessing and feature extraction modules, and a model integration layer comprising algorithms such as SVM, Random Forest, MLP, AdaBoost, Decision Tree, GNB, Gradient Boosting, and Logistic Regression. The results, along with evaluation metrics, are delivered through a Flask-based user interface, enabling real-time monitoring and enhanced cloud security.

A. SYTEM WORKFLOW

- **File Upload** : Owner upload encrypted log and packet data
- **Examine** : Analyze the data through ML analysis
- **Detection** : Predict and classify the potential cyberattacks
- **Access Control** : Block decrypted keys if thread found
- **Key Delivery** : Send key to authorized users when file is safe

B. OBJECTIVES:

- To develop an intelligent and automated framework for detecting privilege escalation attacks in cloud environments using machine learning techniques.
- To model and analyze user activity patterns for differentiating between normal and malicious behaviours, overcoming the limitations of traditional rule-based mechanisms.
- To implement and evaluate multiple machine learning classifiers such as SVM, Random Forest, MLP, AdaBoost, Decision Tree, GNB, Gradient Boosting, and Logistic Regression.
- To train and test the models on the KDD Cup ’99 intrusion dataset, which contains diverse attack scenarios.
- To compare model performance using evaluation metrics like Accuracy, Precision, Recall, and F1-Score, ensuring reliability and robustness.
- To enforce automated access control policies that grant or block user requests based on prediction outcomes.
- To ensure instant containment of malicious activities, minimizing the risk of data breaches and system compromise.
- To enhance cloud security resilience by providing a proactive, adaptive, and scalable solution.

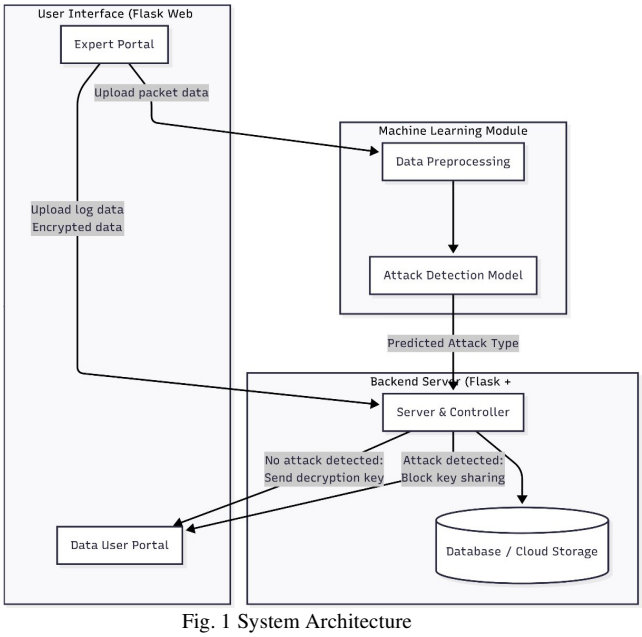

Fig. 1 System Architecture

C. RESULTS

Fig. 2 Home Page

Fig. 3 Owner Register Page

Fig. 4 Owner Login Page

Fig. 5 File Upload Page

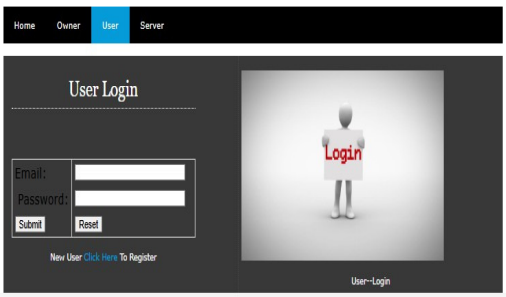

Fig. 6 User Login Page

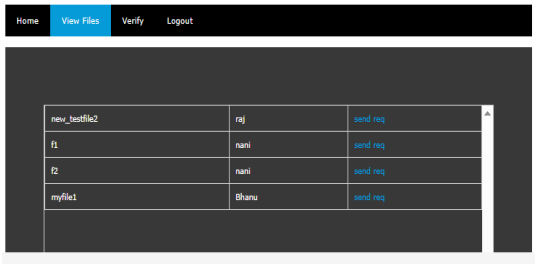

Fig. 7 User Files View Page

Fig. 8 Server Login Page

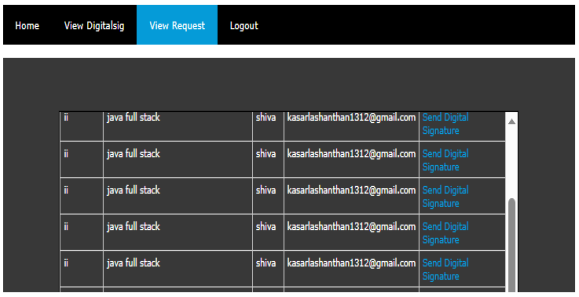

Fig. 9 Server Requested View Page

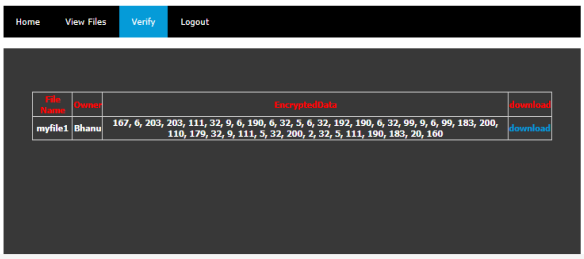

Fig. 10 User Requested File Granted

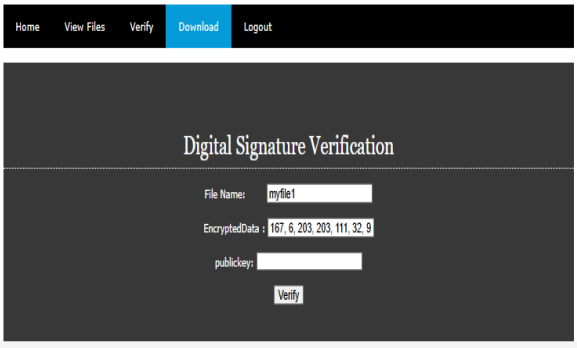

Fig. 11 Granted Files Downloaded Page

III CONCLUSION

The proposed machine learning–based detection system effectively identifies malicious behavior and integrates seamlessly into a cloud security framework. Among the models tested on the KDD dataset, MLP and SVM achieved ~0.93 weighted F1- score, while GNB was the least effective. These results demonstrate that advanced ML models can significantly improve intrusion and privilege-escalation detection in cloud environments.

Looking forward, performance of these models can be further enhanced by expanding the dataset in size, diversity, and relevance to evolving attack patterns. Incorporating recent behavioral trends and broader features will enable more robust threat identification. As organizations increasingly rely on machine learning for security decisions, improving model accuracy becomes critical for reducing risk and ensuring operational integrity. This research highlights a promising direction for building intelligent, data-driven defense systems against insider threats across various sectors.

REFERENCES

[1] 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.
[2] 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.
and A. Ahmadian, "Cloud-based email phishing attack using machine and deep learning algorithm", Complex Intell. Syst., pp. 1–28, Jun. 2022.
learning for anomaly detection: A review", ACM Comput. Surv., vol. 54, no. 2, pp. 1–38, Mar. 2021.
[5] X. Sun, Y. Wang, and Z. Shi, "Insider threat detection using an unsupervised learning method: COPOD", Proc. Int. Conf. Commun., Inf. Syst. Comput. Eng. (CISCE), pp. 749–754, May 2021.

