International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2 (2026)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 2, 2026
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Privilege Escalation Attack Detection and Mitigation in Cloud Using Machine Learning

Smt. P. Anitha[1], Molabanti Jagadeesh Babu [2], Dabbakuti Venkata Tirupathi Raju [3], Pittu Baji [4], Thella Jessy Abhishek [5], Machani Sai Kiran[6], Devarakonda Bhargav Sai Teja [7]

[1] Assistant Professor, St. Ann's College of Engineering & Technology, Chirala, Andhra Pradesh- 523157

[2-7] UG Student, St. Ann's College of Engineering & Technology, Chirala, Andhra Pradesh- 523157

ABSTRACT: The rapid increase in attack sophistication along with the expansion of smart connected devices has created serious cybersecurity concerns, especially in cloud environments. Although cloud computing offers major advantages to organizations, its centralized nature makes deploying distributed security systems difficult, and the continuous flow of sensitive information increases the chances of both accidental and intentional data breaches. Malicious insiders pose an even greater risk because they already possess legitimate privileges and can misuse them to cause extensive harm. This work introduces a machine-learning-based system designed to detect insider threats and classify suspicious behaviors related to privilege escalation. The framework analyzes cloud log activities to identify irregular patterns that may indicate security issues. Ensemble learning is used to improve prediction accuracy by combining multiple models. While earlier research has examined network anomalies, many methods do not effectively detect privilege-escalation attacks.To address this gap, a customized subset of the CERT insider threat dataset is used, and four ML models Random Forest, AdaBoost, XG Boost, and Light GBM are evaluated. Among these, Light GBM achieves the good accuracy, whereas While Light GBM offers the best overall performance, certain algorithms excel at detecting specific insider behaviors.

Key words: *Insider Threat Detection, Privilege Escalation, Ensemble Learning, LightGBM, CloudSecurity.*

1. INTRODUCTION

Cloud computing has revolutionized data storage and processing by offering scalable, on-demand services. However, this centralization introduces security challenges, particularly concerning unauthorized data access and insider threats. Insider threats, originating from within the organization, pose significant risks as they involve individuals misusing their authorized access to harm systems or steal data. These threats are especially concerning in applications like online social networks (OSNs), business platforms, and e-commerce systems, where sensitive user information and financial data are prevalent. Detecting insider threats is challenging because these individuals have legitimate access to the company's systems and data, making traditional security tools like firewalls often ineffective against such threats.

To address latency and bandwidth issues associated with cloud computing, paradigms like fog and edge computing have emerged. Fog computing extends cloud services to the network's edge, processing data closer to its source, while edge computing involves data processing directly on devices. While these models enhance performance, they also introduce unique security vulnerabilities. Many attacks affecting fog and edge computing are inherited from cloud computing; however, current cloud security solutions may not be effective in these environments due to their unique properties. Therefore, robust security measures, such as strong encryption, intrusion detection and prevention systems, and continuous monitoring, are essential to protect against unauthorized access and data breaches in these distributed architectures.

In data access scenarios within OSNs, business platforms, and e-commerce applications, escalation attacks can occur during routine operations. For instance, employees or contractors with legitimate access might intentionally steal sensitive customer data or inadvertently expose the system to external threats through negligence. Insider threats are a serious danger for e-commerce businesses, as disgruntled employees or ex-employees may attempt to steal company data or proprietary information, hoping to sell it to rival businesses. Mitigating these threats requires implementing strict access controls, conducting regular security training, and employing advanced intrusion detection systems.[5] Effective mitigation involves enforcing least privilege access, implementing strong authentication,

continuous monitoring, and rapid incident response mechanisms.

2. LITERATURE SURVEY

.**[1] S, A., D, S., & G, P. (2024)** The authors proposed a malicious insider threat detection system for cloud environments using advanced sampling-based anomaly detection techniques. Their approach improves detection accuracy by handling imbalanced datasets through variation of sampling methods. They focused on identifying unusual user behavior patterns that indicate insider attacks. The model enhances security monitoring by reducing false positives and improving response time. Their work highlights the importance of adaptive anomaly detection in cloud security.**[2] Nascimento et al. (2025)** This study focused on evaluating the availability of SDN-ICN services in multi-access edge computing environments. The authors developed a reliability assessment model to analyze system performance under failures and cyber threats. They discussed how software-defined networking and information-centric networking can improve service resilience. Their work contributes to ensuring continuous service availability in distributed edge networks. The study emphasizes fault tolerance and system robustness.

[3] Aleke & Trigui (2025) The authors examined legal and ethical challenges in digital forensics, especially in the context of AI-driven investigations. They discussed issues like data privacy, evidence admissibility, and cross-border legal complexities. The study highlights the risks of bias and lack of transparency in AI-based forensic tools. They also proposed guidelines to ensure ethical compliance and accountability. Their work bridges the gap between technology advancement and legal frameworks. **[4] Rana (2025)** This research introduced the use of data mining techniques combined with the K-means clustering algorithm for enterprise risk auditing. The author demonstrated how clustering can identify hidden patterns and anomalies in financial and operational data. The approach improves decision-making in risk management processes. It also helps organizations detect fraud and irregularities effectively. The study shows the practical application of machine learning in business risk analysis. **[5] Madarie et al. (2025)** The authors explored cybersecurity experts' perspectives on how data thieves operate in digital environments. They analyzed attacker behavior using Routine Activity Theory and suggested refinements to improve its applicability. The study provides

insights into common attack strategies and vulnerabilities exploited by cybercriminals. Their findings help in designing better preventive security measures. The research emphasizes understanding human behavior in cybersecurity defense.

[6] Safeer (2024) This work discussed the application of reinforcement learning techniques in cybersecurity systems. The author highlighted how RL can be used for adaptive threat detection and automated response mechanisms. The study reviewed different RL models and their effectiveness in dynamic cyber environments. It also addressed challenges like training complexity and real-time implementation. The research shows the potential of intelligent, self-learning security systems.

3 SYSTEM ARCHITECTURE

The system architecture begins with cloud network dataset collection and test data input, followed by dataset preprocessing. The processed data undergoes train-test splitting before being fed into the LightGBM classifier. The model classifies traffic into normal, insider attacker, or external attacker categories, with final performance evaluation metrics generated for validation.

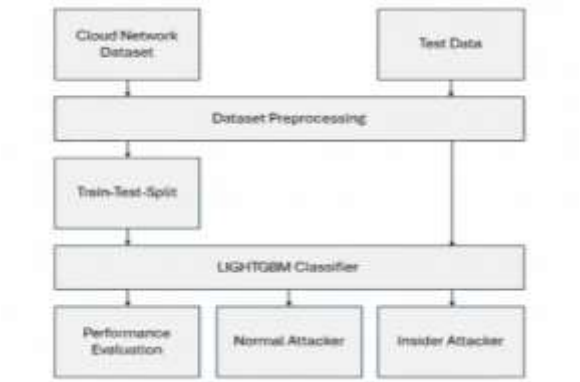

Fig1: **System Architecture**

3.1 METHODOLOGY

The proposed Escalation Attack Detection system adopts a machine learning–based framework to identify privilege escalation and insider threats in cloud and enterprise environments. The methodology consists of data collection, preprocessing, feature engineering, model training, and performance evaluation.

Initially, system logs, user activity records, access control data, and network behavior features are collected from the cloud network dataset. The dataset contains both normal user activities and escalation attack instances. This ensures that the model learns the distinction between legitimate privilege usage and abnormal privilege escalation behavior.

In the preprocessing stage, missing values are handled, duplicate records are removed, and categorical attributes are encoded into numerical format. Feature normalization is

applied using Min-Max scaling to ensure uniform distribution of values:

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}}$$

where $X$is the original feature value, and X_{min}, X_{max}represent minimum and maximum feature values.

The dataset is then divided into training and testing sets using a train–test split approach. Relevant features are selected to reduce dimensionality and computational complexity. The processed data is fed into the LightGBM classifier, which is based on gradient boosting. The boosting objective function is defined as:

$$F(x) = \sum_{m=1}^{M} \gamma_m \, h_m(x)$$

where $h_m(x)$represents the weak learner (decision tree), $\gamma_m$is the learning weight, and $M$is the number of boosting iterations.

For classification, the model predicts whether a user belongs to Normal, Insider Attacker, or Escalation Attacker class. The probability of class prediction is computed using the softmax function:

$$P(y_i) = \frac{e^{z_i}}{\sum_{j=1}^{k} e^{z_j}}$$

where $z_i$is the model output score and $k$is the number of classes.

Finally, performance is evaluated using Accuracy, Precision, Recall, F1-score, and Confusion Matrix analysis to measure detection efficiency and false alarm reduction. This methodology ensures accurate, scalable, and real-time escalation attack detection.

4. DESIGN AND CONSTRUCTION

The design of the proposed Escalation Attack Detection system follows a modular and scalable architecture suitable for cloud and enterprise environments. The system is structured into data acquisition, preprocessing, model training, classification, and evaluation modules. Each module operates independently while maintaining seamless integration for efficient attack detection.

In the construction phase, the system first incorporates a cloud network dataset containing user activity logs, access control records, system calls, and network traffic features. A preprocessing engine is designed to clean the dataset by removing missing values, eliminating

redundant attributes, and encoding categorical variables. Feature normalization is integrated to ensure consistent data

distribution and improve model convergence.

The processed dataset is then divided into training and testing subsets using a train–test split mechanism. A feature selection component is constructed to extract significant attributes related to privilege misuse and abnormal access behavior, reducing dimensionality and computational cost.

The core construction includes the LightGBM classifier module. LightGBM is selected due to its gradient boosting framework, fast training speed, and ability to handle large-scale structured data efficiently. The classifier is trained to distinguish between Normal Users, Insider Attackers, and Escalation Attackers. Decision trees are iteratively built and optimized to minimize classification error.

5 RESULTS AND DISCUSSION

The proposed Escalation Attack Detection system was evaluated using a structured cloud/network dataset containing normal user behavior, insider attacks, and privilege escalation attack instances. The LightGBM classifier demonstrated strong classification capability in distinguishing between legitimate and malicious activities.

Fig 2: Upload Mobile Sense Data Interface

After uploading, dataset details are displayed. A graph shows the number of normal users and insider attack records. The system analyzes 494 records with 830 features derived from CERT logs to detect privilege escalation attacks. The dataset includes Normal and Insider Attack classes. Experimental results using Random Forest, AdaBoost, XGBoost, and LightGBM show effective classification, with LightGBM achieving superior accuracy and efficient real-time cloud threat detection.

Fig 3: Light GBM Confusion matrix

Light GBM model gives the best accuracy for attack detection. Results and confusion matrix are shown on screen .

The LightGBM model achieved 96.96% accuracy, 97.58% precision, 96.25% recall,

and 96.81% F1-score. The confusion matrix shows most Insider Attacks correctly detected (37), with minimal misclassification. Some Normal instances were misclassified, but overall results demonstrate strong detection capability and effective privilege escalation attack identification in cloud environments.

Fig 4: Predicted results

System predicts whether given test data is normal or insider attack. Final prediction result is displayed to the user.The predicted output shows real-time classification of test instances using the trained LightGBM model. For the given feature inputs, the system successfully identifies one instance as an Insider Attack and another as Normal. This demonstrates the model's ability to analyze high-dimensional behavioral features and accurately detect privilege escalation activities in cloud environments.

6. CONCLUSION

Privilege Escalation Attack Detection and Mitigation in Cloud Using Machine Learning" successfully demonstrates the potential of machine learning techniques in enhancing cloud security. The research addresses one of the critical challenges in cloud computing: escalation attacks and privilege escalation, which often lead to severe data breaches and financial losses. By leveraging advanced algorithms such as AdaBoost and, the system efficiently detects malicious activities while minimizing false positives and false negatives.

Another significant achievement of the research lies in its ability to process and analyze real-time data for attack prediction. By preprocessing datasets and implementing scalable algorithms, the system provides an end-to-end solution that not only detects threats but also assists organizations in taking proactive measures to mitigate risks. The graphical representations and confusion matrices further make the system user-friendly and practical for stakeholders, including IT administrators and cybersecurity teams.

Future Scope

The research lays the groundwork for several future enhancements that can further improve the detection and mitigation of privilege escalation attacks in cloud environments. One of the most promising directions is the integration of deep learning

techniques, such as Recurrent Neural Networks (RNNs) or Long Short-Term Memory (LSTM) networks, to capture sequential patterns in user activity logs. These models can analyze temporal dependencies, making them suitable for detecting sophisticated attack patterns.

Another avenue for future research is the incorporation of anomaly detection techniques. While the current system relies on labeled datasets for supervised learning, anomaly detection can identify previously unseen or zero-day attacks.

REFERENCES

[1] S, A., D, S., & G, P. (2024). Malicious insider threat detection using variation of sampling methods for anomaly detection in cloud environment. In Computers and Electrical Engineering (Vol. 105, p. 108519). Elsevier BV.

[2] Nascimento, E., Lins, L., Tavares, E., Pereira, P., Dantas, J., Kosta, S., & Maciel, P. (2025). Availability assessment of SDN-ICN service for multi-access edge computing. In The Journal of Supercomputing (Vol. 81, Issue 2). Springer Science and Business Media LLC.

[3] Aleke, Ngozi Tracy, and Mohamed Trigui. "Legal and Ethical Challenges in Digital Forensics Investigations." In Digital Forensics in the Age of AI, pp. 147-176. IGI Global Scientific Publishing, 2025.

[4] Rana, Sharif Uddin Ahmed. "Application of Data Mining Combined with K-means Clustering Algorithm in Enterprises' Risk Audit." In The Economics of Talent Management and Human Capital, pp. 29-54. IGI Global, 2025.

[5] Madarie, R., Weulen Kranenbarg, M., & de Poot, C. (2025). Cybersecurity Expert Perspectives on Data Thieves' Actions in Digital Environments: Potential Refinements for Routine Activity Theory. In Deviant Behavior (pp. 1–19). Informa UK Limited.

[6] Safeer, E. (2024). Reinforcement Learning Approaches in Cyber Security. In Advances in Information Security, Privacy, and Ethics (pp. 53–76). IGI Global.