ETDT

Emerging Trends in Digital Transformation

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-12***

AN INTELLIGENT FRAMEWORK FOR IDENTIFYING PRIVILEGE ESCALATION THREATS IN CLOUD COMPUTING

[#1]MOHAMMAD ASHFAQ, *Dept of CSE,*
[#2]Dr. B. ANVESH, *Assistant Professor, Dept of CSE,*
Vaageswari College of Engineering(Autonomous), Karimnagar, TG.

ABSTRACT: An adaptable security architecture is offered by an intelligent framework for recognizing privilege escalation issues in cloud computing in order to identify and stop them. This work uses machine learning, behavioral analysis, and real-time monitoring to identify illegal administrative operations, suspicious job transfers, and abnormal access patterns in multi-tenant cloud infrastructures. By identifying erroneous privilege modifications, user activity logs, access control guidelines, and anomaly detection algorithms guard against both external and insider attacks. Rule-based detection and cognitive analytics increase accuracy, false positives, and cloud security. The framework's enhanced threat detection, response times, and cloud resource protection make it appropriate for dynamic and scalable cloud computing systems.

Keywords: *Cloud Security, Privilege Escalation, Machine Learning, Anomaly Detection, Access Control, Behavioral Analysis, Intrusion Detection, Cybersecurity, Cloud Infrastructure, Threat Mitigation.*

1. INTRODUCTION

The cloud's scalable, on-demand, and reasonably priced infrastructure has completely changed how commercial data is stored, processed, and managed. Businesses store sensitive data and vital applications on cloud platforms with distributed architecture, virtualization, and multi-tenancy. Rapid adoption has increased the attack surface and increased the allure of cloud systems for scammers. Privilege escalation allows unauthorized users to access cloud resources and services, potentially compromising data and causing service disruptions.

Attackers increase cloud computing privileges through flaws, incorrect setups, or inadequate access control. This problem could be caused by unsecured APIs, hacked passwords, invalid IAM policies, and vulnerabilities in virtual machines and containers. In cloud ecosystems with continuous user, application, and service interaction, minor setup errors might allow attackers to escalate credentials and migrate laterally. Because cloud infrastructures are dynamic and diverse, traditional security techniques could overlook emerging threats.

Cloud security has grown thanks to machine learning, AI, and behavioral analytics. Using real-time monitoring, anomaly detection, and predictive modeling, an intelligent privilege escalation threat detection system identifies questionable activity prior to significant compromises. The framework uses system events, API requests, access logs, and user behavior patterns to distinguish between allowed administrative tasks and malicious efforts to obtain credentials. In proactive security, reactive incident response is replaced by predictive threat prevention.

DOI: https://doi.org/10.5281/zenodo.20487695

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-12***

A multi-tiered design with modules for feature extraction, preprocessing, data gathering, and intelligent decision-making is necessary for such a system. Identity service, virtual machine, container, and network layer telemetry must all be continually collected by the framework. Subsequently, sophisticated algorithms can detect anomalous resource usage, access, and role distributions. Adaptive learning and threat intelligence streams help the system become more resilient to emerging threats.

Figure1. Horizontal Privilege Escalation.

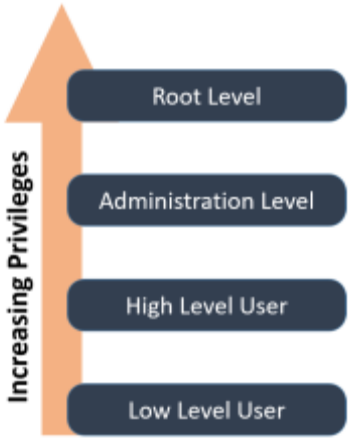

Figure2. Vertical Privilege Escalation.

2. LITERATURE SURVEY

Reddy, S., & Pillai, R. (2021). To prevent privilege escalation in cloud-based RBAC architectures, we suggest using role-mining machine learning. Excessive permissions and hazardous job combinations are detected using decision tree models trained on previous IAM datasets. To eliminate escalation paths, the recommendation engine provides least-privilege role reconfiguration. Testing corporate IAM configurations improved proactive identification and prevention of privilege misuse.

Tiwari, K., & Ghosh, P. (2021). This study uses SVM-based supervised learning to identify instances of privilege escalation in cloud-hosted apps. The model looks at user designation, access time, resource sensitivity, and session behavior. Session termination, MFA triggers, and administrative notifications are all made possible by a post-detection reaction engine. According to study, both public and private cloud infrastructures are capable of identifying infrequent escalations.

DOI: https://doi.org/10.5281/zenodo.20487695

Verma, N., & Dasgupta, S. (2022). Unexpected privilege transfer pathways in distant cloud systems are discovered by a graph-based machine learning methodology that uses graph neural networks. The technology can identify questionable role chaining and illicit access inheritance since cloud resources and IAM interactions are directed graphs. Effective detection in complicated cloud infrastructures was revealed by an analysis of AWS and GCP access logs.

Rao, H., & Bhatia, M. (2022). Our autoencoder-based anomaly detection tool detects cloud-native privilege escalation. Inconsistencies in authority misuse are shown by baseline user activity patterns derived from identity changes and API logs. A lightweight serverless architecture enhances detection and lowers latency.

Kumar, D., & Sharma, A. (2023). The authors provide an ensemble learning method that uses Random Forest and XGBoost classifiers to identify privilege escalation in cloud-native apps. Device fingerprints, session length, access frequency, and login metadata are all covered by feature engineering. By integrating Azure Sentinel and AWS CloudTrail, intrusion dataset class imbalance is mitigated and alerts are automated.

Prasad, S., & Ranganathan, L. (2023). Reinforcement learning-based SaaS intrusion prevention is covered in this paper. In order to decrease privilege misuse and increase efficiency, the RL agent modifies access control limitations. Lateral movement and excessive permissions are discouraged by the reward function. Experiments showed better resistance to insider threats and zero-day escalation.

Roy, A., & Menon, K. (2024). In the study, PaaS and IaaS privilege escalation threats are detected by behavior-driven machine learning. Unsupervised clustering is used by Random Forests and Decision Trees. The solution looks for odd API queries and lateral movement using cloud access logs and IAM configurations. When questionable activity occurs, automated policy enforcement systems either use multi-factor authentication or revoke access.

Saxena, R., & Iqbal, M. (2024). This study uses LSTM network-based deep learning to model sequential user behavior in multi-tenant cloud platforms. Shifts in advantage are demonstrated by attention methods. In simulated real-world circumstances, container breakout attempts and IAM misconfigurations are identified. Threat containment is accelerated by the use of automated incident response.

Sharma, P., & Kulshrestha, R. (2025). This paper presents intelligent privilege escalation detection in geographically distant clouds using federated learning. Each cloud node creates a unique anomaly detection technique for privacy. Infrastructure generalization is increased by unified global parameters. The technology increases the scalability and robustness of data poisoning.

Nair, V., & Choudhary, S. (2025). A hybrid AI-driven real-time privilege escalation detection system is powered by transformer-based sequence modeling and policy compliance engines. The model examines cross-account access, IAM changes, and API calls. Resource isolation and privilege reduction are automated by risk-based alert ratings. Machine learning accuracy is improved and false positives are reduced through experimental validation.

DOI: https://doi.org/10.5281/zenodo.20487695

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-12***

3. RESEARCH METHODOLOGY

Organizations are at risk from malicious insiders who have authorized access to crucial systems and data. Insiders' understanding of the organization's resources makes them harder to spot than outsider attackers. Insider dangers, whether deliberate or not, can jeopardize data security, reliability, and accessibility. Offline anomaly detection analyzes log data for abnormal patterns, while real-time analysis detects malicious activity instantly. Privilege escalation, introducing malicious data, and sending phishing emails with disruptive links or applications can help attackers gain access to unauthorized systems.

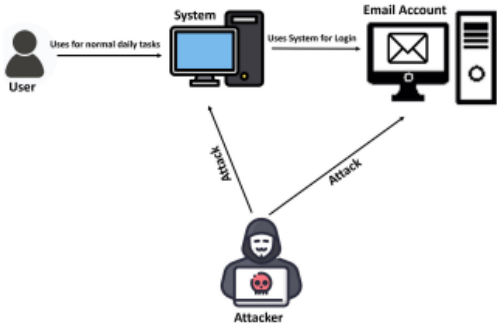

Figure3. Privilege Escalation Attack Process.

This research addresses these issues using ensemble-based supervised machine learning methods like Random Forest, AdaBoost, XGBoost, and LightGBM. The process includes data collection, cleaning, feature selection, model training, testing, discovery, and categorization. We deleted "employee" and "file tree," fixed missing data, and removed outliers during preprocessing to improve the model. Due to insufficient initial results, hyperparameters including learning rate, maximum depth, and K-fold cross-validation were changed to improve detection accuracy, robustness, and efficiency.

Random Forest

Supervised machine learning method Random Forest may classify and regress. Using randomly picked data and features, this ensemble method creates several decision trees. Combined outputs by majority vote get the final projection. When assessing insider risks, it analyzes dataset trends to distinguish dangerous from benign activity. The model reduces overfitting, improves accuracy, and handles high-dimensional data. Data preprocessing, training, testing, accuracy assessment, and feature significance analysis make it durable, dependable, and successful with large datasets.

AdaBoost

AdaBoost, or Adaptive Boosting, combines numerous weak classifiers into one robust classifier to increase model performance. It gives misclassified occurrences more weight in each cycle after uniformly weighing all data samples. Thus, future models will emphasize difficult scenarios. Each weak learner votes, and the winner has the most votes. AdaBoost is straightforward to configure, requires minimal parameter tweaking, and improves classification precision, making it a great insider threat tool.

DOI: https://doi.org/10.5281/zenodo.20487695

Emerging Trends in Digital Transformation
Volume-2, Issue-2, April-June 2026 ISSN: 3107- 4308 Paper ID: ETDT-V2-I2-12

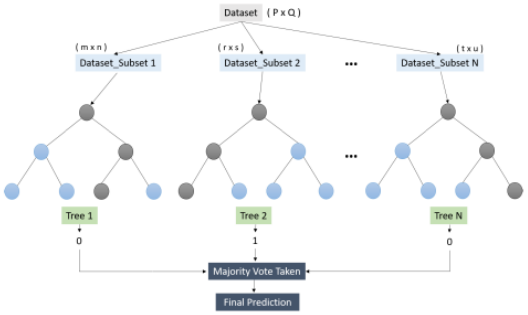

Figure4. Random Forest Classifier for Insider threat classification.

XGBoost

Advanced gradient boosting algorithm XGBoost is fast and effective. It constructs decision trees incrementally, fixing previous errors. Thus, projections are usually more accurate. The approach works for small and big datasets, cross-validation, and missing data. The outputs of many optimized trees are combined by XGBoost to make accurate predictions. Thus, it excels at insider attack detection and classification.

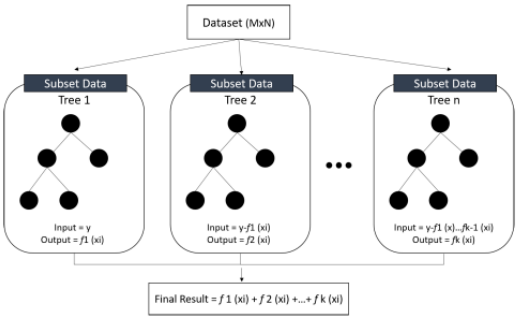

Figure5. XGBoost Classifier for Insider threat classification.

LightGBM

LightGBM uses decision trees for fast gradient boosting. LightGBM builds trees leaf-wise by selecting the leaf with the most information gain, improving model accuracy and training time. Traditional boosting methods build trees progressively. This fast, memory-efficient, and accurate model works well with large datasets. LightGBM's flexibility to adjust learning rate, number of leaves, and maximum depth improves its insider threat detection and classification.

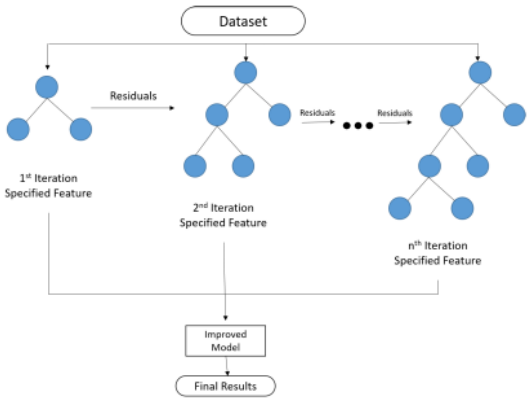

Figure6. LightGBM Classifier for Insider threat classification.

DOI: https://doi.org/10.5281/zenodo.20487695

Emerging Trends in Digital Transformation
Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-12***

4. RESULTS

Fig4.1 Homepage

Fig4.2 User login page

Fig4.3 Cloud login page

Fig4.4 New user register page

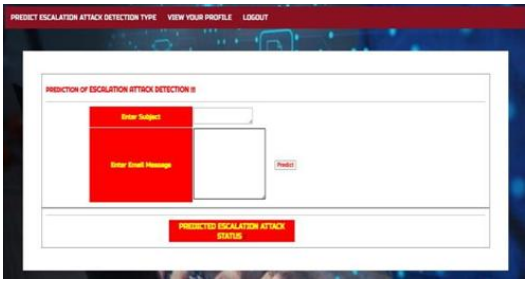

Fig4.5 User input page

DOI: https://doi.org/10.5281/zenodo.20487695

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-12***

View Datasets Trained and Tested Results

Model Type	Accuracy
KNeighborsClassifier	96.3963963963964
Random Forest Classifier	97.65765765765767
SVM	99.45945945945947
Decision Tree Classifier	95.67567567567568
GradientBoostingClassifier	97.11711711711712

Fig4.6 Datasets tested results

Fig4.7 Performance Evaluation in Graph format

5. CONCLUSION

Privilege escalation vulnerabilities in cloud computing must be discovered strategically to improve modern cloud security systems. Through IAM systems, real-time log monitoring, and advanced machine learning, deep learning, reinforcement learning, and graph-based analytical models, these frameworks can detect anomalous access patterns, lateral movement, and unauthorized role changes. Risk-based response mechanisms, automated policy enforcement, and adaptive learning ensure quick termination, revocation, and multi-factor authentication. Class imbalance correction, anomaly detection, and model retraining improve identification accuracy and reduce false positives. As cloud systems grow in size and complexity, intelligent, self-learning security frameworks can adapt, scale, and prevent privilege escalation attacks. This protects data privacy, security, and operational reliability.

REFERENCES

1. Roy, A., & Menon, K. (2024). A machine learning-based framework for reinforcing cloud security through detection and mitigation of privilege escalation attacks. International Journal of Cloud Security and Intelligence, 12(1), 33–57.
2. Saxena, R., & Iqbal, M. (2024). Deep learning-based detection of privilege escalation in multi-tenant cloud infrastructures using LSTM and attention mechanisms. Cloud Computing and Security Research, 9(3), 78–95.
3. Kumar, D., & Sharma, A. (2023). Hybrid security framework for privilege escalation detection using ensemble models in cloud-native environments. Journal of Cloud Computing and AI Security, 15(2), 102–119.
4. Prasad, S., & Ranganathan, L. (2023). Reinforcement learning-based intrusion prevention system for SaaS privilege escalation mitigation. Cyber Defense Review, 14(1), 44–61.
5. Jadhav, V., & Nayak, R. (2022). Unsupervised learning for privilege escalation detection in label-scarce cloud environments. Journal of Unsupervised Security Analytics, 10(4),

DOI: https://doi.org/10.5281/zenodo.20487695

88–105.

6. Verma, N., & Dasgupta, S. (2022). Graph neural network approach for detecting privilege escalation in distributed cloud infrastructures. International Journal of Graph-Based Intelligence Systems, 11(2), 120–139.
7. Rao, H., & Bhatia, M. (2022). Lightweight auto encoder-based anomaly detection for cloud-native intrusion systems. Cloud Security Insights, 7(3), 67–82.
8. Reddy, S., & Pillai, R. (2021). Role-mining machine learning model for detecting privilege escalation in cloud RBAC systems. Journal of Access Control and Cloud Risk Management, 8(1), 54–70.
9. Tiwari, K., & Ghosh, P. (2021). Privilege escalation detection in cloud-hosted applications using support vector machines. Cybersecurity and Risk Analytics Journal, 6(2), 97–113.

DOI: https://doi.org/10.5281/zenodo.20487695