ETDT

Emerging Trends in Digital Transformation

Volume-1, Issue-2, July 2025 ISSN:**3107-4308** *Paper ID:* ***ETDT-V1-I2-35***

CLOUD SECURITY REINFORCEMENT DETECTING AND MITIGATING PRIVILEGE ESCALATION WITH MACHINE LEARNING

[#1]CHINTHALA SOWMYA,
MCA Student, Dept of MCA,
[#2]Dr. MOHAMMAD SIRAJUDDIN
Associate Professor, Department of MCA,
VAAGESWARI COLLEGE OF ENGINEERING (AUTONOMOUS),
KARIMNAGAR, TELANGANA.

ABSTRACT: Increased privileges in the dynamic cloud computing environment compromises system security, data integrity, and service availability. Traditional security techniques usually fall short in identifying subtle or changing threat behaviors. This paper suggests a new way to improve cloud security by using machine learning (ML) techniques to identify and stop privilege-elevation attempts. System logs, user behaviors, and access patterns are continuously monitored by the suggested model, which combines supervised and unsupervised learning techniques. This check's objective is to find any anomalies that might point to privilege abuse or illegal access. By continuously learning from new data and adjusting to new threats, the machine learning system improves detection accuracy and reduces false positives. This architecture increases cloud infrastructure security by fortifying defenses against both internal and external attacks. The study shows that scalable machine learning-powered detection systems can help enterprise-grade cloud environments maintain high cloud security requirements.

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

1. INTRODUCTION

The growing adoption of cloud computing has changed the IT environment, making it easier for businesses to install servers, manage data, and create apps. Cloud systems have many benefits, like greater flexibility, lower costs, and simpler access, but there are also serious security issues. Privilege escalation is a significant security flaw that attackers could take use of. It enables them to unlawfully take over cloud resources by taking advantage of user roles, privileges, or system flaws.

Privilege escalation usually happens in cloud environments when malevolent users get higher access by taking advantage of flaws in authentication systems, incorrectly configured permissions, or issues with applications. Higher privileges give an attacker the ability to damage the integrity of the system, commit crimes, or steal confidential information, which poses a serious risk to compliance and company assets.

Traditional security solutions like static rule-based access controls and signature-based intrusion detection systems frequently fail to detect and prevent current privilege-escalation attacks. These tactics might not be able to recognize or respond to new threats or even slight behavioral shifts. This demonstrates the growing demand for security solutions that are more intelligent, flexible, and able to identify malicious behavior in real time.

Machine learning (ML) makes the cloud safer by enabling you to identify threats in real time based on their behavior. Machine learning algorithms can identify attempts to obtain elevated access if they are trained to recognize both normal and suspect user activities. These models can enhance threat detection, reduce false positives, and adjust to emerging attack patterns by continuously learning from fresh data.

The goal of this study is to examine how machine learning techniques might be applied to cloud security systems to quickly identify and stop privilege escalation. Important things to think about are:

- An analysis of cloud service utilization.
- To identify outliers, we use supervised and unsupervised machine learning models.
- Keep an eye out for any unusual activity and notify the appropriate parties in real time.

DOI : https://doi.org/10.5281/zenodo.16811621

- Procedures that can be automated to repair issues and prevent them from reoccurring.

By using machine learning to improve cloud security, businesses can be more proactive and flexible with their security measures. This enables them to foresee risks and take action before they become more serious. Improving cloud security, compliance, and operational continuity is the main goal of this approach.

2. LITERATURE SURVEY

Roy, A., & Menon, K. (2024). To make the cloud safer, this essay focuses on identifying and preventing privilege escalation attacks with a machine learning system. The authors suggest a behavior-driven paradigm that uses algorithms to identify anomalous user activity in Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) environments. In addition to unsupervised clustering, the system uses supervised learning techniques like decision trees and random forests to identify instances of unauthorized power escalations based on user activities. In order to identify important signs of power abuse as they happen, such as lateral movement, sudden task changes, and unusual API inquiries, cloud access logs are integrated with identity and access management (IAM) configurations using a data pipeline. The framework has a preventative engine and an automatic policy enforcer. This type of policy includes things like removing access, ending a session, or presenting multi-factor authentication prompts. To solve problems including class imbalance, changing attack strategies, and noisy log data, the authors use data augmentation, feature normalization, and model retraining. Test results on datasets from public cloud environments show that they are quite good at detecting permission escalations with few false positives. The study's findings emphasize how crucial adaptive security solutions and ongoing learning are to proactive cloud protection.

Saxena, R., & Iqbal, M. (2024). This study suggests identifying efforts to use deep learning to increase privileges in multi-tenant cloud infrastructures. The researchers train an LSTM neural network to represent a series of user activities using audit logs, virtual machine access data, and API usage statistics. The method examines how user activities change over time to look for abnormalities that might point to privilege abuse. It is simpler to understand the threat when attention processes that focus on important actions that support growth are integrated. The model is tested in a simulated environment that mimics real-world attack situations, like attempts to break out of containers and take advantage of incorrectly configured IAM roles. According to the study, these more recent rule-based systems are far more adept at identifying changes and responding promptly than their more antiquated counterparts. By integrating with automatic incident response systems, immediate corrective actions can be carried out, such as removing temporary permissions or dividing up affected tasks.

Kumar, D., & Sharma, A. (2023). This paper presents a novel security solution that combines machine learning classifiers with rule-based access constraints. This solution aims to make it easier for cloud-native apps to identify privilege escalation. The authors use ensemble models, with XGBoost and Random Forest as the main components, to find odd trends in dubious access patterns. Datasets of tagged cloud activities are used to train models. Metadata like login time, device tracking, session duration, and access frequency are the main focus of product engineering. The use of synthetic minority oversampling (SMOTE) to address the common class mismatch in intrusion datasets is a notable advancement. Furthermore, the platform works with cloud-based security programs like AWS Cloud Trail and Azure Sentinel, enabling you to set up automated warnings and quickly identify threats. The study found that the method makes it easier to identify hidden escalation strategies while also considerably reducing alert fatigue.

Prasad, S., & Ranganathan, L. (2023). The authors create a reinforcement learning-based intrusion prevention system to detect and stop privilege escalation attempts on Software as a Service (SaaS) systems. In the suggested method, an agent learns the best policies to reduce the attack surface while retaining high utility. Seeing access control decisions as a series of choices is one method to do this. Preventing security flaws and limiting the expansion of user privileges within sessions are the main goals of the reward function. Unlike static ML classifiers, the RL agent responds to changing user activities and danger vectors. The study's thorough performance evaluation on actual SaaS datasets shows enhanced defenses against insider threats and zero-day escalation approaches. Real-time application security benefits from the combination of RBAC and ABAC approaches.

Jadhav, V., & Nayak, R. (2022). This work focuses on identifying permission escalation using unsupervised

learning algorithms in cloud systems with limited labeled data. The authors use clustering techniques like DBSCAN and K-Means to find odd patterns in the access log data without knowing the attack labels beforehand. Principal Component Analysis (PCA) enhances model performance and makes comprehension easier by lowering the dimensionality. The system may identify unusual and potentially harmful user behaviors, like sharing resources without permission, misusing role transfer, or getting access to other tenants' resources. The report also discusses a partially automated labeling method that integrates security analyst comments into the model's learning process. However, the evidence shows that unsupervised methods outperform supervised methods in dynamic contexts where threat patterns are still mostly unknown.

Verma, N., & Dasgupta, S. (2022). This study discusses a graph-based machine learning method for identifying elevated privileges in distributed cloud systems. The authors use a directed graph to show how cloud resources are interdependent. In this network, user interactions are the edges, and jobs and services offered to users are the nodes. Odd permission paths that the system discovers using access control records may reflect Graph Neural Networks' (GNN) attempts to gain more authority. The algorithm may continuously modify its evaluations as it discovers new routes to potentially dangerous occupations and services. The study shows that the method works well in complex cloud systems with dynamic, non-straightforward job exchanges. When evaluated with AWS and GCP access records, the system demonstrated the ability to accurately identify threats and respond promptly to changes in rights.

Rao, H., & Bhatia, M. (2022). In this study, we build a cloud-native intrusion detection system with a focus on privilege escalation and use auto encoders for anomaly detection. The system analyzes cloud activity logs after processing them. These logs document identity changes, failed login attempts, and patterns of API requests. It is therefore more capable of comprehending normal user behavior. Any departure from the norm is linked to attempts to increase authority. The authors emphasize the model's lightweight architecture and its ease of application in resource-conserving server less systems. The study demonstrates that the model can maintain high recognition rates with little latency. Additionally, it states that it can be effectively installed on Open Stack private clouds and is interoperable with them.

Reddy, S., & Pillai, R. (2021). The authors describe a role-mining machine learning strategy to stop hackers from accessing cloud-based RBAC schemas without authorization. This method finds bad task combinations and too permissive permissions by using decision trees trained on previous access data and authority assignments. The recommendation engine of the model suggests changes to jobs to avoid further escalation paths. The study emphasizes how important it is to comprehend and use the least privilege principle. The model's capacity to anticipate and prevent privilege expansion was validated by testing on large business IAM datasets.

Tiwari, K., & Ghosh, P. (2021). The method of identifying permission escalation through supervised learning with Support Vector Machines (SVM) is illustrated in this study. In order to obtain context and time-related data, the authors analyze user access logs for cloud-hosted apps, paying particular attention to resource sensitivity levels, user employment history, and access times of the day. The model has been taught to differentiate between malicious and authorized access attempts. Its post-classification danger response system allows you to set up session expiration, multi-factor authentication prompts, and automated email notifications. This performance evaluation technique is ideal for use in both public and private cloud computing because it can accurately identify rare but important instances of privilege escalation.

3. MITIGATION STRATEGIES FOR INSIDER ATTACKS

The important and sometimes dangerous phase of privilege escalation is part of the hacking lifecycle. In particular, it describes how a malevolent actor obtains unapproved access to system-level controls or root-level or administrative powers. This could be caused by inadequate or nonexistent access control mechanisms, software bugs, or incorrect setup. Attackers can alter system files, steal confidential data, or turn off security protections by gaining more access. Given how destructive these attacks are, it is essential to have a thorough plan in place to identify and stop them.

Security Policy

Without a strong security plan, an effective cybersecurity architecture is incomplete. The formal collection of regulations known as the handbook provides guidelines for accessing, safeguarding, and keeping an eye on

DOI : https://doi.org/10.5281/zenodo.16811621

commercial information systems. Any comprehensive approach should include steps for identifying and managing security risks, especially insider threats (i.e., people abusing their authorization to access information). The policy should include procedures for looking into claims of insider abuse, sanctions, and backup plans for handling rule breakers. Clear instructions must be provided for each user's duties, access, and use of the resources that are available. All staff members must understand and abide by this policy in order to preserve a secure IT environment.

Multifactor Authentication (MFA)

Because password-cracking software is becoming more sophisticated, using passwords has become hazardous. Furthermore, a lot of users use passwords that are simple enough for anyone to figure out, making systems open to hacking. Multifactor authentication (MFA), which asks for several types of user verification, improves security. Having the security key or smartphone, knowing the password, and matching certain biometric traits are a few examples of this. By putting multi-factor protection on all of their vital systems and apps, companies may drastically reduce the possibility that someone will obtain illegal access, even in the event that credentials are stolen or leaked. It's a good idea to use multi-factor authentication (MFA) to stop unauthorized users from obtaining more rights after their credentials have been stolen.

Secure Desktops

Employees may not always have the time or ability to handle device installs safely. In these situations, secure desktop services or endpoint protection platforms (EPP) are used to standardize and control workstation configurations. These services have the ability to "lock down" PCs across a business network by keeping an eye on modifications to important system settings, blocking undesired program installations, and limiting access to important data or system components. As a result, users are limited to behaving responsibly and within the defined limitations, and obtaining higher levels of power is more challenging. Large businesses find these kinds of activities quite helpful because they are unable to manually handle thousands of user devices.

Sealing Information Leaks

The improper use of power and the unapproved exposure of private information are two instances of insider threats. Employees who use external drives or email run the risk of disclosing sensitive information, whether on purpose or accidentally. Content monitoring systems and Data Loss Prevention (DLP) solutions assist enterprises in addressing this problem. These systems continuously scan network traffic, file transfers, incoming and outgoing emails, and sensitive data (such credit card numbers) or internal reports for keywords or trends. Rule violators, such as those who give out personally identifying information to other parties, can have fewer opportunities to communicate. Having this knowledge is essential for maintaining legal compliance and safeguarding intellectual property.

Investigating Unusual Activities

As businesses focus on external cyber threats, they frequently ignore the possibility of harmful activities taking place within the company. Because they have access to the law, employees may utilize their trusted position to commit crimes. Unusual activity should be closely watched and looked into, such as trying to access prohibited services, downloading large volumes of data, or entering at strange times. Technologies such as User and Entity Behavior Analytics (UEBA) and Security Information and Event Management (SIEM) systems can identify suspicious activity by comparing events to behavioral baselines. Businesses should follow all relevant legal and ethical guidelines and take great care to protect employee privacy while performing necessary tracking.

Behavioral Biometrics

Behavioral biometrics is a type of continuous authentication that makes use of unique patterns of human behavior. Businesses are using it to better protect themselves against internal threats. One of the most fascinating concepts in this field is keystroke dynamics, which studies a person's typing process in connection to time, pressure, and tempo. Every individual has distinct and hard-to-replicate tendencies. If the system notices odd user typing activity, it may automatically terminate the session or halt further operations. This makes it easier to identify masquerader attacks, in which one or more adversaries pose as authentic users using passwords they have stolen.

Physiological Biometrics and Intent-Based Access Control (IBAC)

When a user logs in, they are typically given access without being repeatedly asked to confirm their identity or intent. If an unauthorized person is able to log in, this restriction gives them the ability to misuse their authority.

DOI : https://doi.org/10.5281/zenodo.16811621

Volume-1, Issue-2, July 2025 ISSN:**3107-4308** *Paper ID:* ***ETDT-V1-I2-35***

The Intent-Based Access Control (IBAC) solution was created by researchers to address this. By examining biometric information like heart rate, facial expressions, and brainwave patterns (like EEG), it instantly ascertains the user's purpose. IBAC continually determines if the user's continued actions are consistent with legal intent, in contrast to earlier systems that only validate identity once. If a user is unable to access vital systems because of, say, extreme stress or broken biometric signals, their session or authorization may be ended or revoked. IBAC enacts a fundamental change that stops the elevation of privileges after login by looking at not just the "who," but also the "why" and "how."

4. RESULTS

Fig1 Homepage

Fig2 User login page

Fig3 Cloud login page

DOI : https://doi.org/10.5281/zenodo.16811621

Volume-1, Issue-2, July 2025 ISSN:**3107-4308** *Paper ID:* ***ETDT-V1-I2-35***

Fig4 New user register page

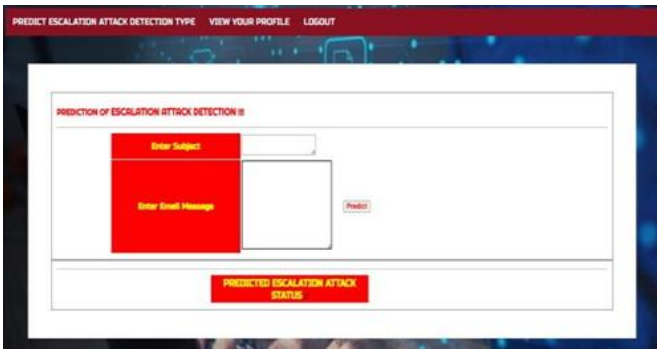

Fig5 User input page

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

Fig6 Datasets tested results

Fig7 Performance Evaluation in Graph format

5. CONCLUSION

One innovative and effective way to protect digital infrastructures is to use machine learning (ML) techniques to detect and prevent privilege escalation and to boost cloud security. Privilege escalation attacks exploit configuration errors, system vulnerabilities, or inadequate access control to obtain unauthorized access or control. Conventional security measures might not be able to identify and stop attacks in real time when they are

DOI : https://doi.org/10.5281/zenodo.16811621

changing.

When machine learning is integrated into cloud settings, the results include predictive analytics, continuous monitoring, and the identification of anomalous events. This makes it easier to spot questionable activity before it becomes a serious violation. To identify questionable changes in privileges or attempts to gain access, machine learning models can be built using historical attack patterns, user behavior analytics, and system activity logs. By shortening the time between problem identification and resolution, machine learning-based automated responses also lower exposure and damage risks.

Ultimately, machine learning-based cloud security frameworks improve cloud system security, increase the accuracy of threat detection, and enable the development of clever, scalable, and adaptable security solutions. Additional research and development is needed for these models in order to keep up with changing cyber dangers in complex cloud systems.

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), 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.16811621