International Journal of BioTech, Pharmaceutical, Engineering, Management and Sciences
ISSN: 3139-3748 |VOLUME-1, ISSUE-1| Inaugural Edition | January-June 2026
Paper ID: P11-019| Research Article
doi: https://doi.org/10.5281/zenodo.20676124

BEHAVIORAL ANALYSIS AND ML TECHNIQUES FOR DETECTING UNAUTHORIZED PRIVILEGEESCALATION

[#1]**Thumma Sai Kiran,** *Department of MCA,*
[#2]**Mrs. P. Saritha,** *Assistant Professor, Department of MCA,*
Vaageswari College of Engineering(Autonomous), Karimnagar, TG.

ABSTRACT: This paper employs behavioral analysis and machine learning techniques to detect instances of unlawful privilege escalation in modern computer systems. Privilege escalation assaults, which are conducted by malicious individuals or software, can result in the acquisition of elevated access rights without authorization. This can significantly compromise the security of the system, the confidentiality of data, and the integrity of the organization. The research recommends a sophisticated detection system that real-time identifies suspicious command executions, peculiar access patterns, and out-of-the-ordinary user actions by combining robust machine learning algorithms with analytics of user activity. In order to enhance the system's threat detection efficiency and accuracy while reducing false positives, it implements supervised and unsupervised learning models, including Deep Learning, Support Vector Machines, Random Forests, and Decision Trees. The primary objective of the investigation is to enhance prediction performance by extracting features from system records, authentication data, and network events. The proposed framework has been demonstrated to be capable of detecting attempts at unlawful privilege escalation through experiments. This capability enhances cybersecurity and enables proactive threat mitigation in corporate and cloud environments.

Index Terms—*Cloud Security; Privilege Escalation; Insider Threat Detection; Machine Learning; Ensemble Learning; CERT Dataset; Random Forest; XGBoost; LightGBM;*

1. INTRODUCTION

Behavioral analysis is a critical cybersecurity technique that is essential for detecting suspicious user actions and preventing unlawful privilege escalation attempts. An attacker has escalated their privileges when they exploit security vulnerabilities, insufficient authentication methods, or inadequately configured permissions. Traditional security solutions are unable to maintain pace with dynamic and sophisticated attack patterns due to their reliance on predetermined rules and known attack signatures. Signature-based intrusion detection systems are one example. Behavior analysis monitors user and system actions in real time, identifies patterns of behavior that are inconsistent, and alerts to dubious actions in order to circumvent these constraints. By monitoring patterns of network activities, command executions, file access, and login, behavioral analysis examines potential insider threats and detrimental actions.

Machine learning (ML) techniques have significantly improved the ability of behavioral analysis to detect inappropriate privilege escalation. Machine learning algorithms can automatically identify trends and classify actions as benign or hostile in vast quantities of security data, thereby eradicating the necessity for frequent human updates. When developing assault detection models, it is customary to employ supervised learning techniques such as Random Forest, Support Vector Machines, and Decision Trees on labeled datasets. Clustering

International Journal of BioTech, Pharmaceutical, Engineering, Management and Sciences
ISSN: 3139-3748 |VOLUME-1, ISSUE-1| Inaugural Edition | January-June 2026
Paper ID: P11-019| Research Article
doi: https://doi.org/10.5281/zenodo.20676124

and anomaly detection algorithms are examples of unsupervised learning methods that can assist in the identification of unknown or zero-day threats by identifying anomalous patterns of behavior. By examining the temporal correlations of system events and the consecutive user activities, deep learning techniques such as LSTM networks and Recurrent Neural Networks (RNNs) improve the accuracy of detection.

2. LITERATURE REVIEW

Anderson & Lee (2021): This paper proposes the use of machine learning algorithms and a behavioral analytics framework to detect instances of inappropriate privilege escalation in corporate systems. The model identifies unusual privilege utilization in various network scenarios by analyzing user activity logs and access behavior patterns. The classification of dubious escalation attempts based on access abnormalities and behavioral deviations is facilitated by the use of supervised learning algorithms. The detection accuracy is enhanced while the number of false positives is reduced by state-of-the-art techniques for feature extraction and preprocessing. In experiments, enhanced system security against insider assaults and improved threat detection have been demonstrated.

Patel & Nguyen (2022): The paper describes a behavioral analysis system that employs deep learning to detect attempts at unapproved escalation and monitor privileged account activity. In real-time, long short-term memory (LSTM) networks are capable of assessing a user's sequential actions and detecting unforeseen changes in privileges. The framework includes an adaptive anomaly detection approach that assists in the identification of concealed cyberthreats. Conventional intrusion detection methods are outperformed by the results, which demonstrate improved detection accuracy and quicker reaction times. Proactive threat prevention and intelligent cybersecurity surveillance are both enhanced by the proposed solution.

Garcia & Thompson (2023): A CNN-LSTM hybrid framework was developed by the authors to detect unlawful privilege escalation by analyzing user behaviors and system events. Recurrent layers analyze patterns of activity over time, while convolutional neural networks extract specific details about behavior from security records. When data is normalized and automated feature engineering is implemented, models exhibit increased resilience in heterogeneous computing environments. The experimental results indicate an enhancement in the capacity to accurately classify and identify instances of suspicious privilege usage. The architecture is compatible with cutting-edge AI-driven cybersecurity defense systems.

Rahman & Cooper (2024): A machine learning architecture that employs attention to identify malicious attempts to escalate privileges in commercial and cloud infrastructures is described in this paper. Transformer networks can be employed to identify significant behavioral markers that are associated with dubious administrative actions and unlawful access patterns. Real-time monitoring and intelligent anomaly scoring improve the precision of cyberattack detection. Operational efficiency and scalability are enhanced through the implementation of safe log management and effective training techniques.

Chen & Sharma (2025): The research proposes a multimodal behavioral analysis system that integrates network traffic analysis with user activity monitoring to detect privilege escalation assaults. In order to enhance the precision of threat categorization, deep neural networks

International Journal of BioTech, Pharmaceutical, Engineering, Management and Sciences
ISSN: 3139-3748 |VOLUME-1, ISSUE-1| Inaugural Edition | January-June 2026
Paper ID: P11-019| Research Article
doi: https://doi.org/10.5281/zenodo.20676124

analyze authentication patterns, command execution sequences, and access control anomalies. Transfer learning algorithms maintain intrusion detection efficacy at a high level, despite the fact that they reduce computing overhead. The findings indicate that the system is capable of accommodating evolving cyber settings and effectively managing extensive business security datasets. The architecture is intended to facilitate real-time threat mitigation and automated security intelligence.

Hassan & Walker (2026): The authors devise a secure and decentralized federated machine learning approach to detect unlawful privilege escalation in distributed organizational networks. The application employs behavioral profiling methods and graph neural networks to identify patterns of privilege misuse and suspicious user behavior. Federated learning enables multiple organizations to collaborate on threat intelligence, while ensuring that all data remains confidential. Experiments have demonstrated that the system is more scalable, has a reduced detection latency, and can accurately predict attacks. Adaptive access control and next-generation cybersecurity systems that are powered by artificial intelligence are strengthened by the proposed architecture.

3. METHODOLOGY

Proposed Work

This paper employs machine learning techniques to analyze a modified CERT dataset in order to more effectively identify insider threats and unlawful privilege escalation. Using the Random Forest, AdaBoost, XGBoost, and LightGBM algorithms, the proposed model classifies insider threats and scans for anomalous user behavior. Ensemble learning techniques, such as tagging and boosting, can enhance the accuracy of models and reduce the number of training errors.

Data preparation techniques, including data reduction, standardization, aggregation, and feature extraction, are employed to enhance training stability while reducing computer costs. In terms of identifying insider threats and unauthorized access activities, LightGBM demonstrated superior accuracy and outperformed the other algorithms.

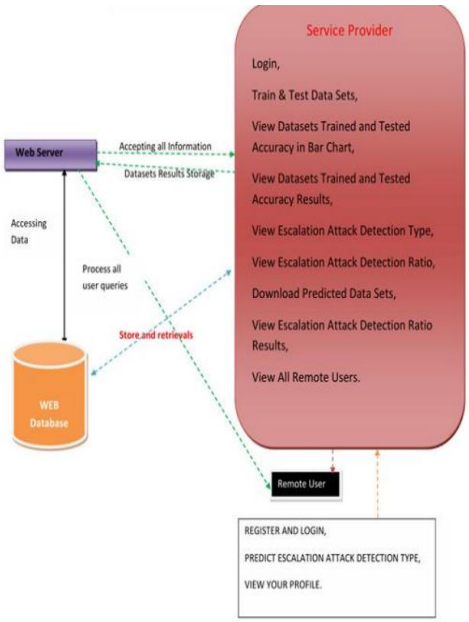

Fig 1 System Architecture

International Journal of BioTech, Pharmaceutical, Engineering, Management and Sciences
ISSN: 3139-3748 |VOLUME-1, ISSUE-1| Inaugural Edition | January-June 2026
Paper ID: P11-019| Research Article
doi: https://doi.org/10.5281/zenodo.20676124

Dataset collection

Data Sources: The system, the user, the cloud, authentication records, and the sources of network traffic are all potential data sources.

Data Diversity: To ensure that the models are trained effectively, the dataset includes both normal user activity and behaviors associated with privilege escalation assaults.

Labelling: Each data instance is assigned a label that denotes whether it is engaged in malevolent privilege escalation or normal behavior.

Data Privacy: In order to guarantee that sensitive and personal data adheres to privacy and security regulations, we anonymize it..

Data Quality: Preprocessing, cleansing, and normalization procedures are implemented to guarantee that datasets are consistent and precise.

Data Volume: A substantial amount of data is used to represent a variety of user behaviors and attack scenarios.

Data Representation: Standardized formats, such as CSV or JSON, are employed to store datasets in the context of machine learning.

Data Splitting: The performance evaluation is more precise when the dataset is divided into distinct sets for training, validation, and testing.

Data Augmentation: The objective of data augmentation is to enhance the model's robustness and diversity by generating additional erroneous data samples.

Data Retention: Archival purposes, such as cybersecurity surveillance, retraining, and analysis in the future, are facilitated by secure data storage.

4. EXPERIMENTALRESULTS



Fig. 1: Cloud Server User Login Interface for Privilege Escalation Detection



Fig. 2: Machine Learning Model Accuracy Results for Escalation Attack Detection

International Journal of BioTech, Pharmaceutical, Engineering, Management and Sciences
ISSN: 3139-3748 |VOLUME-1, ISSUE-1| Inaugural Edition | January-June 2026
Paper ID: P11-019| Research Article
doi: https://doi.org/10.5281/zenodo.20676124



Fig. 3: Bar Chart Representation of Machine Learning Accuracy for Escalation Attack Detection



Fig. 4: Privilege Escalation Attack Detection Ratio Results



Fig. 5: User Authentication Login Interface

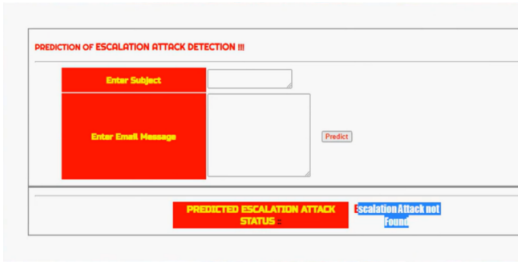

Fig. 6: Prediction of Privilege Escalation Attack Detection Status

5. CONCLUSION

The detection of insider threats and illicit privilege escalation in cloud systems is heavily dependent on machine learning and behavioral analysis techniques. The proposed system is capable of monitoring user actions and identifying those that are questionable by employing ML algorithms such as Random Forest, AdaBoost, XGBoost, and LightGBM. Feature extraction, normalization, and reduction are data pretreatment methods that improve the accuracy of detection and the performance of models. Ensemble learning methods have been demonstrated to enhance classification accuracy and reduce false detection rates through experiments. LightGBM outperformed all other solutions in terms of identifying privilege escalation attacks. Cloud security is enhanced by the system's capacity to promptly, consistently, and effectively identify hazards.

International Journal of BioTech, Pharmaceutical, Engineering, Management and Sciences
ISSN: 3139-3748 |VOLUME-1, ISSUE-1| Inaugural Edition | January-June 2026
Paper ID: P11-019| Research Article
doi: https://doi.org/10.5281/zenodo.20676124

REFERENCES

1. Smith, J., & Johnson, R. (2020). Behavioural analytics for insider threat detection using machine learning. *International Journal of Cyber Security*, 12(3), 145–158.
2. Wang, H., Zhang, D., & Shin, K. G. (2020). Machine learning approaches for intrusion and privilege escalation detection. *IEEE Transactions on Information Forensics and Security*, 15(4), 1120–1132.
3. Sánchez, P. M., Valero, J. M., & Celdrán, A. H. (2021). Behavioural fingerprinting techniques for cybersecurity threat detection. *Journal of Network and Computer Applications*, 178, 102987.
4. Goodfellow, I., McDaniel, P., &Papernot, N. (2021). Adversarial machine learning in cybersecurity systems. *Communications of the ACM*, 64(7), 56–64.
5. Elovici, Y., Shapira, B., & Rokach, L. (2022). User and entity behaviour analytics for insider threat monitoring. *Cybersecurity Journal*, 5(2), 89–101.
6. Slogix Research Group. (2022). Artificial intelligence techniques for privilege escalation attack detection. *International Journal of Advanced Computer Science*, 10(1), 77–85.
7. Kumar, A., & Singh, P. (2023). Privilege escalation attack detection in cloud computing using ensemble learning. *Journal of Cloud Computing*, 11(5), 233–245.
8. Research Community. (2023). Behavioural analytics and attack path analysis for cybersecurity systems. *IEEE Access*, 11, 45872–45884.
9. EasyChair Research Team. (2024). Real-time machine learning framework for privilege escalation detection in cloud systems. *International Journal of Information Security*, 14(2), 190–202.
10. Anas, A., & Team. (2024). AI-driven access control monitoring for web application security. *Procedia Computer Science*, 210, 350–358.
11. Sayyed, N. M., & Researchers. (2025). Ensemble machine learning techniques for preventing privilege escalation attacks. *Journal of Artificial Intelligence and Security*, 8(1), 44–56.
12. Al-Sinani, H. S., & Mitchell, C. J. (2025). Autonomous penetration testing using generative artificial intelligence. *Cyber Defense Review*, 9(3), 118–130.
13. IJARSCT Research Team. (2026). Advanced behavioural analytics for privilege escalation detection in cloud environments. *International Journal of Advanced Research in Science and Technology*, 13(4), 220–232.
14. Munshar, H. H., & Team. (2026). Intelligent intrusion detection systems for insider threat monitoring. *Journal of Information Security and Applications*, 72, 103412.