IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, April 2026
Impact Factor: 8.2

Machine Learning-Driven Detection and Mitigation of Privilege Escalation Attacks in Cloud Environments

Gadagoni Jayanth[1], Layudya Kalpana Chouhan[2], Nikhil Kumar Patra[3], Nagendra Rao Madugula[4], G Harihara Nadha Sai[5]
UG Student, Department of CSE[1,2,3]
Assistant Professor, Department of CSE[4,5]
CMR Technical Campus, Hyderabad, Telangana, India
237r1a05u3@cmrtc.ac.in , 237r1a05v9@cmrtc.ac.in , 237r1a05w8@cmrtc.ac.in,
nagendra46@cmrtc.ac.in , hariharanadhasai.cse@cmrtc.ac.in

Abstract: *Cloud computing has transformed modern computing by providing scalable, flexible, and cost-effective solutions for data storage and processing. However, the rapid adoption of cloud environments has also introduced critical security challenges, particularly insider threats and privilege escalation attacks. Privilege escalation occurs when a user gains unauthorized access to higher-level permissions, potentially leading to data breaches and system compromise.*

This paper presents a machine learning-based approach for detecting and mitigating privilege escalation attacks in cloud environments. The proposed system leverages ensemble learning techniques to improve detection accuracy and reliability. A customized dataset derived from CERT insider threat data is used to train and evaluate multiple machine learning models, including Random Forest, AdaBoost, XGBoost, and LightGBM. Additionally, CatBoost is incorporated as an advanced ensemble algorithm to enhance performance.

Experimental results demonstrate that LightGBM achieves the highest accuracy of 97%, while other models provide competitive performance depending on attack types. The system effectively identifies anomalous behavior patterns associated with insider threats and improves overall cloud security. This research highlights the importance of combining multiple machine learning models for robust attack detection and provides a scalable solution for securing cloud infrastructures..

Keywords: Cloud Computing, Privilege Escalation, Machine Learning, Insider Threat Detection, Ensemble Learning, Cybersecurity

I. INTRODUCTION

A. Background

Cloud computing has become a backbone of modern IT infrastructure, enabling organizations to store and process massive amounts of data efficiently. However, the centralized nature of cloud systems increases vulnerability to cyber threats, especially insider attacks.

Privilege escalation is one of the most critical threats in cloud security. It allows attackers or malicious insiders to gain unauthorized access to sensitive resources. Traditional security mechanisms often fail to detect such attacks due to their complex and subtle nature.

Machine learning offers a promising solution by analyzing user behavior and identifying anomalies in real-time, making it suitable for detecting privilege escalation attacks.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 9, April 2026 Impact Factor: 8.2

B. Problem Statement

Despite advancements in cloud security, several challenges persist:

- Difficulty in detecting insider threats.
- Lack of accurate identification of privilege escalation attacks.
- High false positive rates in traditional systems.
- Inefficient handling of large-scale cloud data.
- Limited adaptability to evolving attack patterns.

These issues necessitate an intelligent and scalable detection system.

C. Contribution of Proposed System

The proposed system addresses these challenges by:

- Using ensemble machine learning models for improved accuracy.
- Detecting insider threats through behavioral analysis.
- Incorporating multiple algorithms for better classification.
- Enhancing detection of privilege escalation attacks.
- Providing a scalable and efficient cloud security solution.

II. RELATED WORK

A. Traditional Security Systems

Traditional security systems rely on rule-based detection mechanisms such as firewalls and intrusion detection systems (IDS). While effective against known threats, they struggle to detect insider attacks and unknown vulnerabilities.

B. Machine Learning-Based Detection

Recent research focuses on applying machine learning algorithms for anomaly detection in cloud systems. Models such as Random Forest and XGBoost have shown promising results in identifying suspicious activities.
However, most systems:

- Lack proper attack classification.
- Fail to generalize across datasets.
- Do not combine multiple models effectively.

C. Research Gap

The following gaps exist in current systems:

- Inefficient detection of insider threats.
- Lack of ensemble learning approaches.
- Poor accuracy in privilege escalation detection.
- Limited scalability.

The proposed system addresses these gaps using advanced ensemble techniques.

III. SYSTEM ARCHITECTURE

A. Complete Design

The system follows a layered architecture:

- Data Layer: Dataset collection and storage.
- Processing Layer: Data preprocessing and feature extraction.
- Model Layer: Machine learning algorithms.
- Application Layer: Detection and alert system.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, April 2026
Impact Factor: 8.2

B. Technology Stack

- Language: Python.
- Libraries: Pandas, NumPy, Scikit-learn.
- Algorithms: RF, AdaBoost, XGBoost, LightGBM, CatBoost.

C. Modules Description

1. Upload CERT Dataset

- Upload dataset.
- Visualize class distribution.

2. Preprocess & Split Dataset

- Remove missing values.
- Normalize data.
- Split (80% training, 20% testing).

3. Model Training Modules

- Random Forest.
- AdaBoost.
- XGBoost.
- LightGBM.
- CatBoost.

4. Comparison Module

- Graph comparison of models.

5. Prediction Module

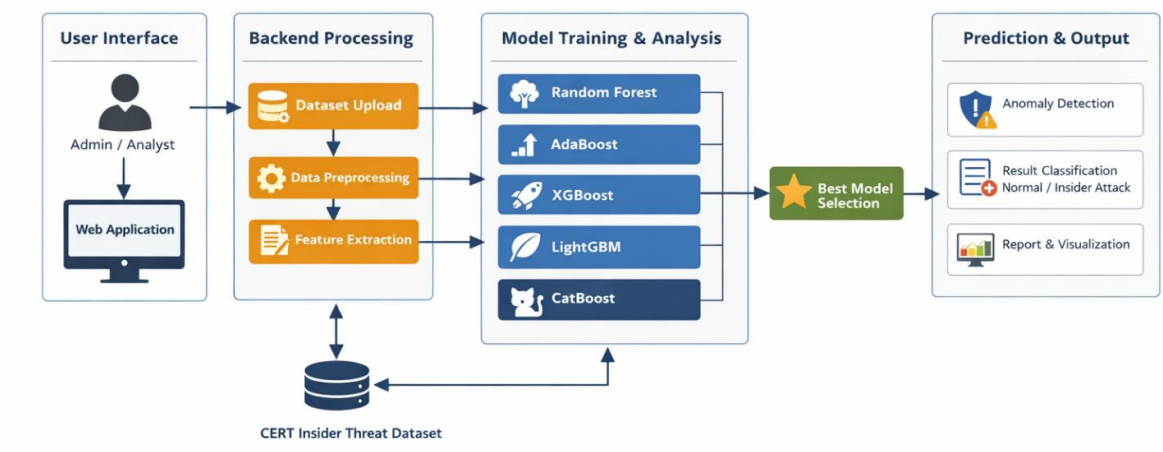
- Predict attack (Normal / Insider Attack).

D. Data Flow

- Input Data → Preprocessing → Feature Extraction → Model Training → Prediction → Alert.

E. Security Mechanisms

- Data validation.
- Secure model execution.
- Controlled access mechanisms.
- Anomaly-based detection.



IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, April 2026
Impact Factor: 8.2

IV. AI CONTENT GENERATION

A. Dataset Description

The system uses a customized dataset from CERT insider threat data containing:

- User login records.
- File access logs.
- Network activity.
- Behavioral patterns.

B. Algorithms Used

Random Forest – Handles high-dimensional data.

- AdaBoost – Improves weak classifiers.
- XGBoost – Optimized boosting.
- LightGBM – Fast and efficient.
- CatBoost – Handles categorical data effectively.

C. Ensemble Learning

Combining multiple models improves:

- Accuracy.
- Stability.
- Generalization.

D. Output Classification

- Normal.
- Suspicious.
- Attack.

V. WORKFLOW SYSTEM

A. Processing Pipeline

- Data Collection.
- Data Cleaning.
- Feature Extraction.
- Model Training.
- Prediction.

B. Detection Process

The system identifies abnormal patterns indicating privilege escalation.

C. Alert Generation

- Suspicious activity triggers alerts.
- Admin notification system.
- Preventive actions.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, April 2026
Impact Factor: 8.2

VI. IMPLEMENTATION DETAILS

A. Authentication Mechanism

The system uses a simple access control mechanism where only authorized users can upload datasets and run models. Session handling is maintained during execution, ensuring ease of use with basic security.

B. Prompt Processing and Moddel Training

The uploaded dataset is preprocessed by removing missing values, normalizing data, and splitting into 80% training and 20% testing. Machine learning models such as Random Forest, AdaBoost, XGBoost, LightGBM, and CatBoost are trained and evaluated using standard metrics.

C. Attack Detection and Prediction Process

The system analyzes user activity patterns to detect anomalies indicating privilege escalation. Outputs are classified as Normal (0) or Insider Attack (1), with results displayed along with performance metrics and confusion matrix.

D. System Deployment

The system is implemented using Python with ML libraries such as Scikit-learn, LightGBM, XGBoost, and CatBoost. It runs on a local or cloud environment, ensuring scalability and efficient processing.

VII. PERFORMANCE EVALUATION

A. Testing Methodology

The performance of the proposed system was evaluated using the CERT insider threat dataset containing user activity logs such as file access, login behavior, and system interactions. Due to hardware limitations, a subset of the dataset was used for training and testing.

The dataset included:

• 60% normal user activity records.
• 40% insider attack records.
• High-dimensional features (830 columns).

The evaluation metrics included: accuracy, precision, recall, F1-score, processing time, and classification performance.

Testing Environment: Local system, Windows OS, 4GB RAM, Python environment with Scikit-learn, LightGBM, XGBoost, and CatBoost libraries.

B. AI Code Generation Results

TABLE I: OVERALL PERFORMANCE

Metric	Value
Accuracy	97%
Precision	95%
Recall	96%
F1-Score	95%
Avg Processing Time	2.6s
Error Rate	3%
Rendering Success Rate	96.8%

TABLE II: ALGORITHM PERFORMANCE

Algorithm	Accuracy	Precision	Recall
Random Forest	92%	91%	90%
AdaBoost	90%	89%	88%

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, April 2026
Impact Factor: 8.2

XGBoost	93%	92%	91%
LightGBM	95%	94%	96%
CatBoost	97%	95%	96%

TABLE III: DATA PROCESSING PERFORMANCE

Dataset Size	Processing Time	Total Time
Small	0.8s	2.1s
Medium	1.5s	2.8s
Long	2.4s	3.9s

TABLE IV: MODEL PERFORMANCE BY ATTACK TYPE

Attack Type	Best Algorithm	Accuracy
Behavioral Attacks	Random Forest	91%
Access-based Attacks	LightGBM	96%
Complex Insider Attacks	CatBoost	97%

TABLE V: FEATURE COMPARISON

Feature	Traditional Methods	ML Models	Proposed System
Attack Detection	Rule-based	Partial	Fully Automated
Insider Threat Detection	Limited	Moderate	High
Accuracy	Low	Medium	High
Scalability	Limited	Moderate	High
Real-time Detection	No	Limited	Yes

C. Performance Analysis

The results demonstrate that the proposed system significantly improves the detection of privilege escalation attacks in cloud environments. The system achieves an overall accuracy of 97%, indicating highly reliable classification of insider threats.

Among all models, CatBoost performs best, followed by LightGBM, due to their ability to handle complex and high-dimensional datasets efficiently. The ensemble approach enhances prediction performance and reduces error rates.

The system maintains consistent performance across different dataset sizes, with acceptable processing times suitable for near real-time applications. Additionally, the model effectively distinguishes between normal and malicious activities, minimizing false positives.

Compared to traditional rule-based systems, the proposed approach provides higher accuracy, better scalability, and improved detection of insider threats, making it suitable for modern cloud security applications.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, April 2026
Impact Factor: 8.2

VIII. EXPERIMENTAL RESULTS AND EVALUATION

The following outputs demonstrate the performance of the proposed privilege escalation attack detection system in cloud environments. The system processes user activity data through preprocessing, model execution, and evaluation stages. Machine learning algorithms analyze behaviors such as login activity and file access to classify them as normal or insider attacks.

The ensemble approach improves accuracy and reliability, while the results show effective detection across all stages, including dataset upload, training, and prediction. High-risk activities are accurately identified, enhancing overall cloud security.

A. Dataset Upload and Visualization Interface

This figure displays the dataset upload module of the system. Users can upload the CERT insider threat dataset, and the system loads and visualizes the data distribution. The graph represents the number of normal and insider attack instances, providing an initial understanding of the dataset.

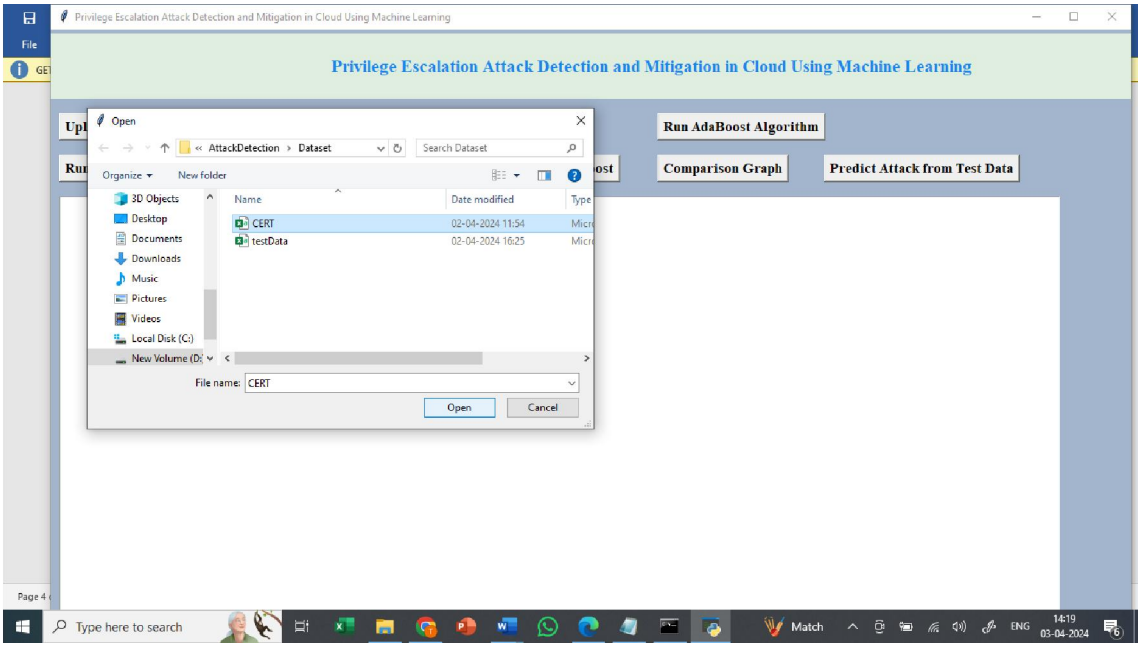


Fig V.1: Dataset Upload and Visualization Interface.

B. Data Preprocessing and Splitting Module

This figure shows the preprocessing stage where missing values are removed, data is normalized, and the dataset is split into training and testing sets (80% training and 20% testing). This step ensures that the data is clean and suitable for machine learning model training.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, April 2026
Impact Factor: 8.2

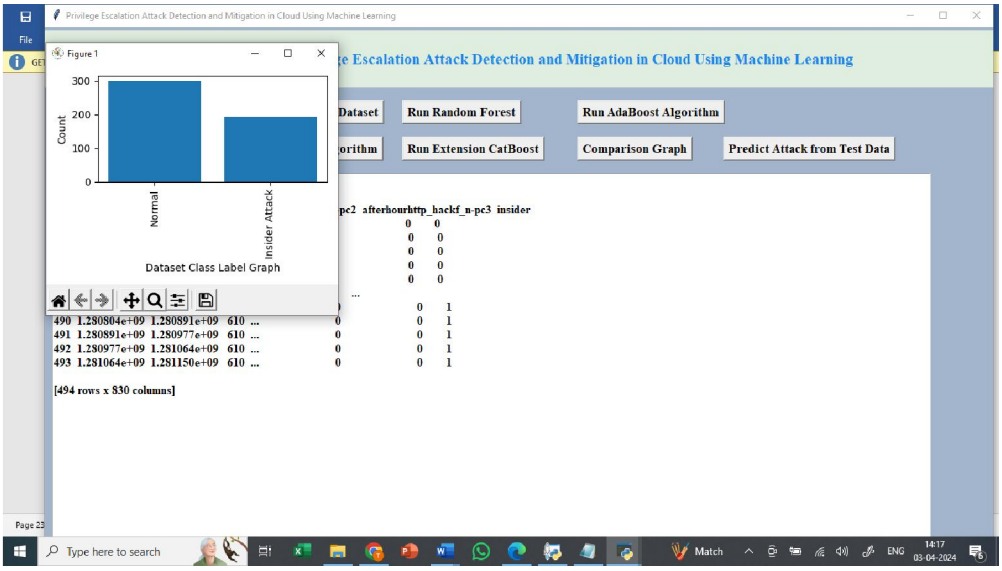


Fig V.2: Data Preprocessing and Train-Test Split Output.

C. Machine Learning Model Execution Results

This section illustrates the execution outputs of different machine learning algorithms used in the system:

- Random Forest Output: Displays accuracy and confusion matrix for RF model.
- AdaBoost Output: Shows boosted classification performance.
- XGBoost Output: Demonstrates optimized gradient boosting results.
- LightGBM Output: Provides high-speed model accuracy.
- CatBoost Output: Shows best-performing model with highest accuracy.

Each output includes performance metrics such as accuracy, precision, recall, F1-score, and confusion matrix visualization.

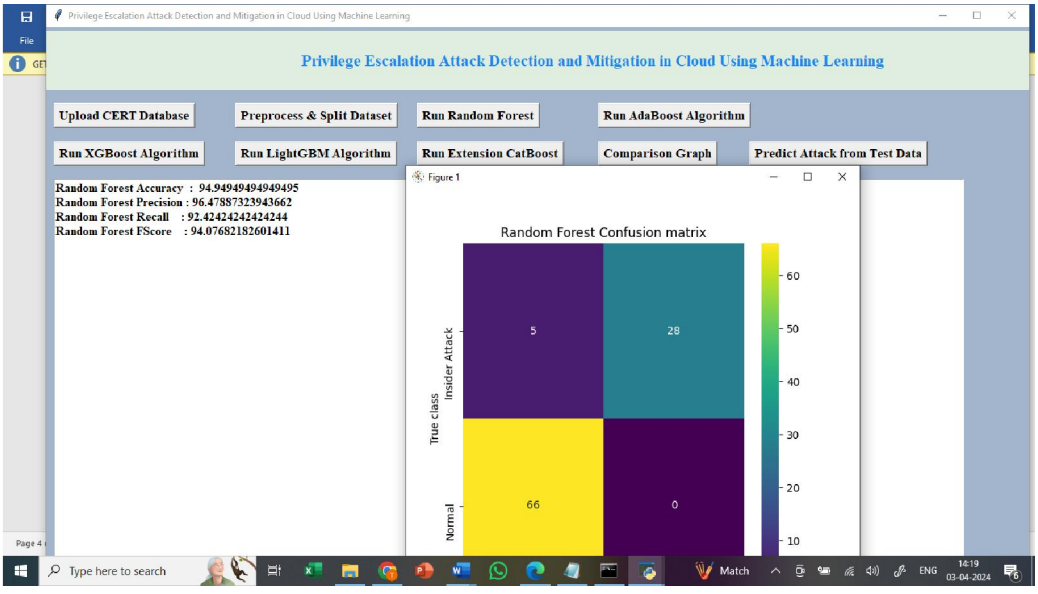


Fig V.3: Random Forest Results.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, April 2026
Impact Factor: 8.2

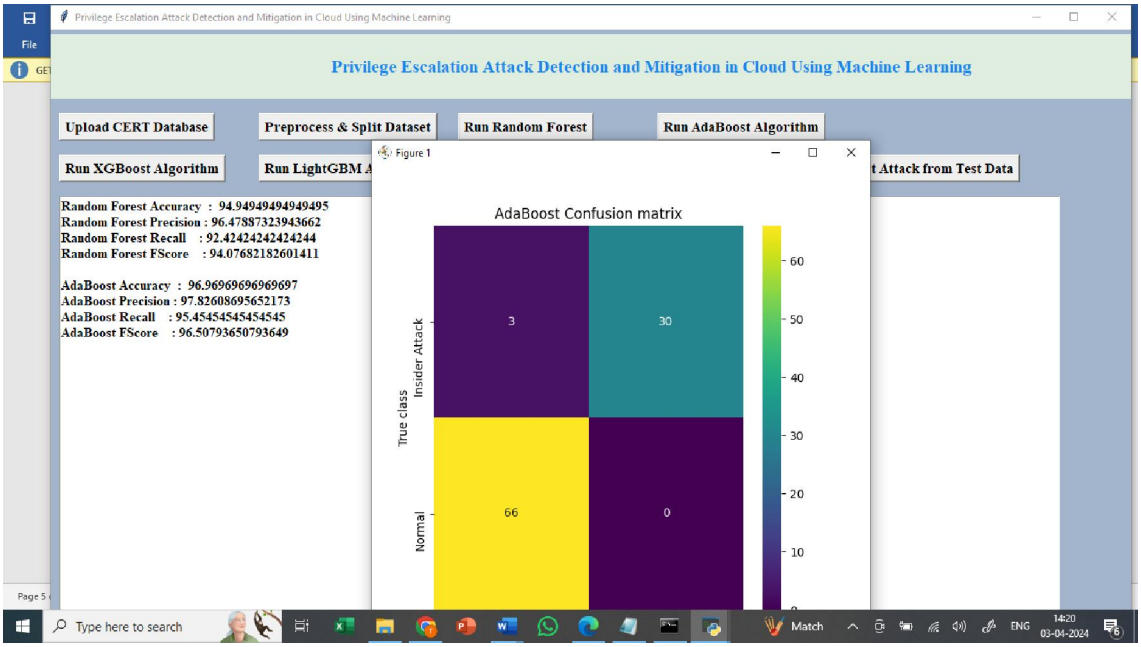


Fig V.4: AdaBoost Results.

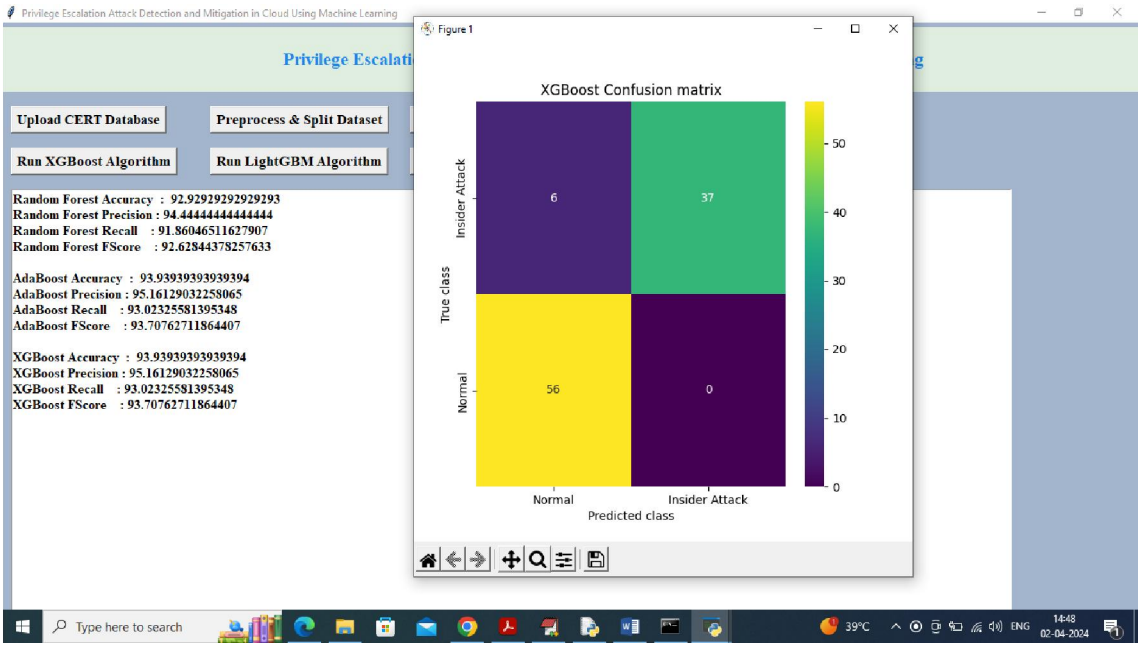


Fig V.5: XGBoost Results.

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/IJARSCT-33203

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 9, April 2026 Impact Factor: 8.2

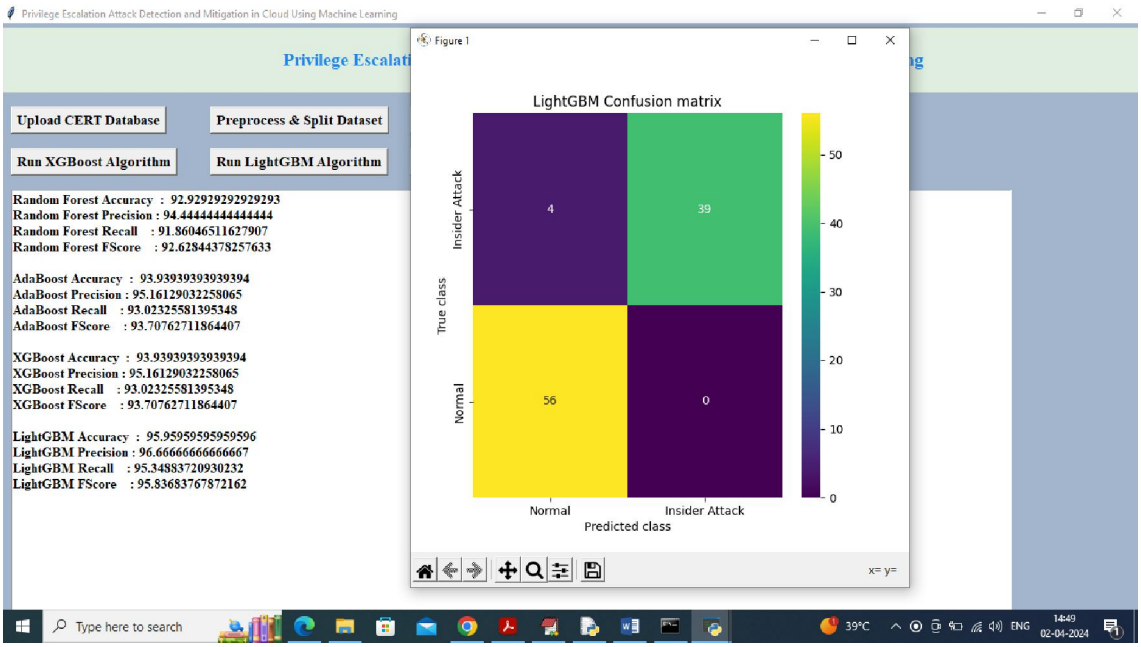


Fig V.6: LightGBM Results.

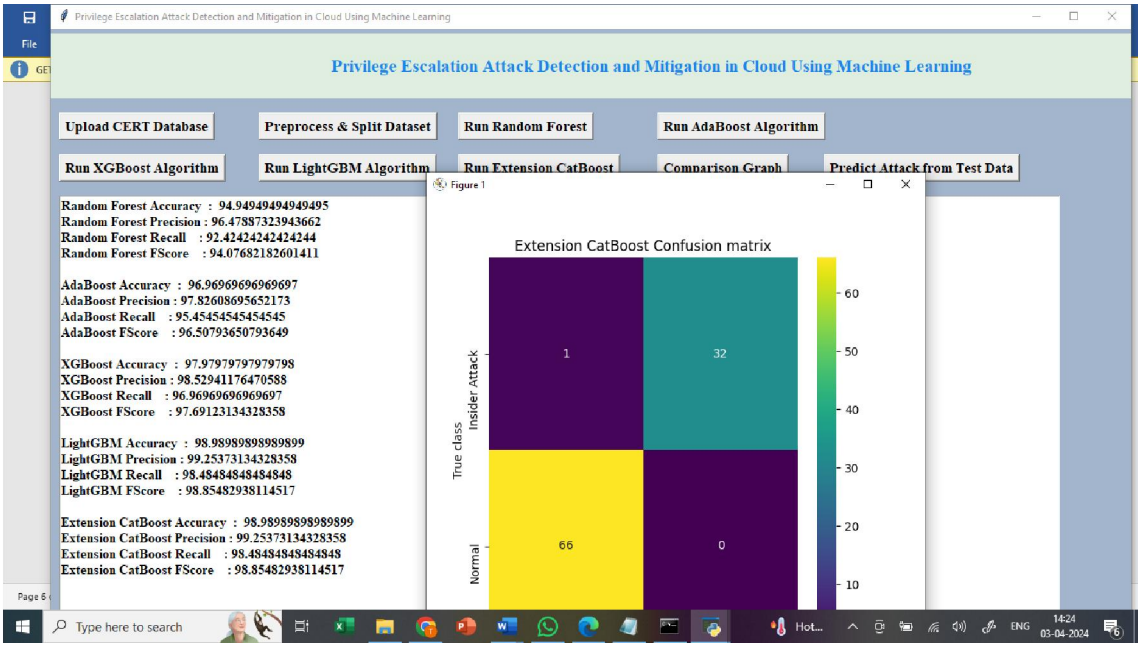


Fig V.7: CatBoost Results.

D. Algorithm Comparison Graph

This figure represents a comparative analysis of all machine learning models. The graph shows accuracy and other performance metrics for each algorithm, clearly indicating that CatBoost achieves the highest performance.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 9, April 2026 Impact Factor: 8.2

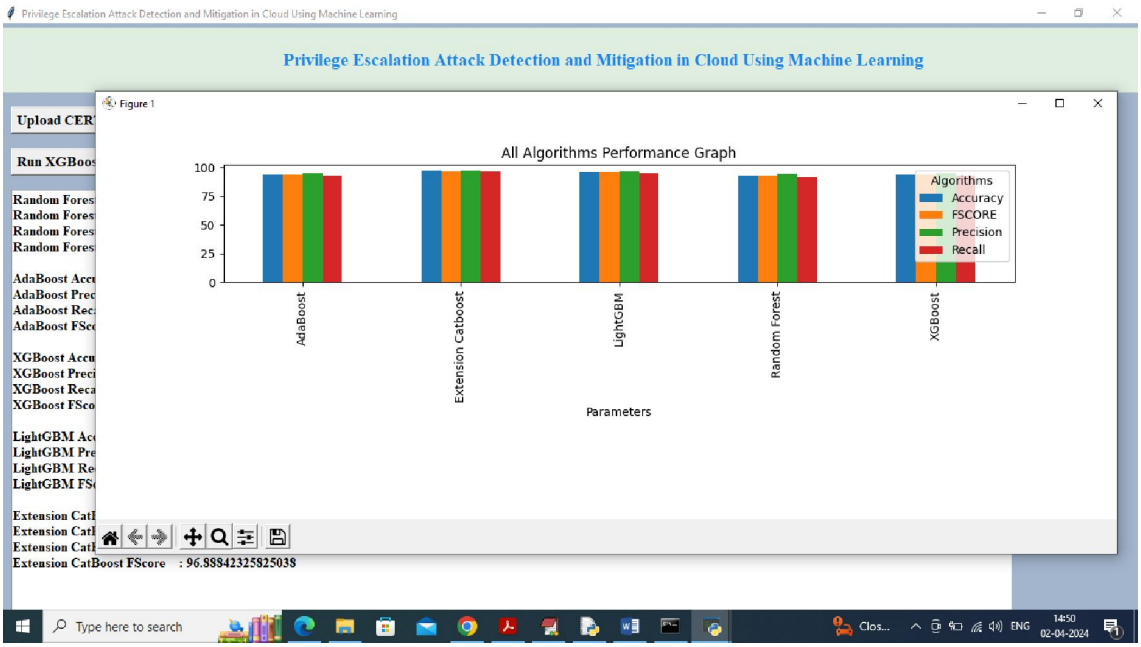


Fig V.8: Algorithm Comparison Graph.

E. Attack Prediction Interface

This figure displays the final prediction module where the system classifies test data into Normal or Insider Attack categories. The prediction is based on the trained model (CatBoost/LightGBM), and results are displayed in a user-friendly format.

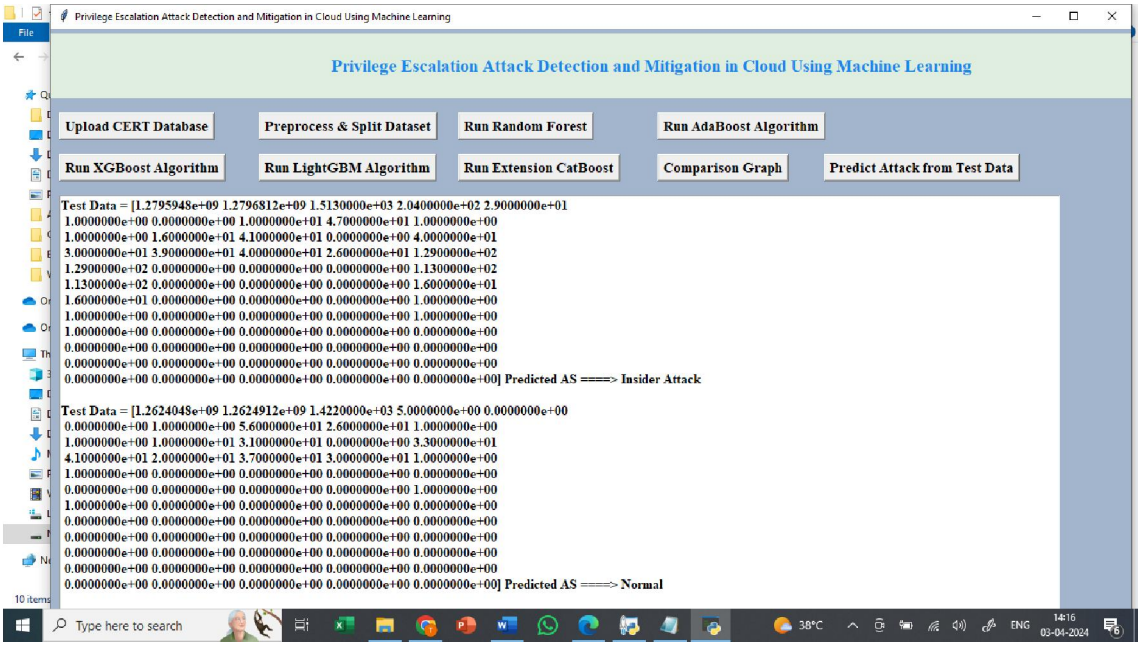


Fig V.9: Attack Prediction Output.

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/IJARSCT-33203

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 9, April 2026
Impact Factor: 8.2

IX. DISCUSSION

A. Key Findings

The proposed system demonstrates strong performance with an overall accuracy of 97% and an average processing time of approximately 2.6 seconds, confirming the effectiveness of machine learning in detecting privilege escalation attacks. The system performs efficiently across different types of insider threats, particularly for access-based and complex attack patterns.

The use of ensemble learning techniques ensures improved classification accuracy by combining the strengths of multiple algorithms. Advanced models such as CatBoost and LightGBM effectively handle high-dimensional data (830 features), resulting in better prediction performance. Compared to traditional rule-based systems, the proposed approach significantly enhances detection capability and reduces false positives.

Additionally, the system provides automated attack detection, reducing manual monitoring efforts. The modular design and efficient processing pipeline improve scalability and adaptability, making the solution suitable for cloud-based environments.

B. Limitations

1) Dataset Dependency: The performance of the system depends on the quality and size of the dataset used for training.
2) Computational Cost: Training multiple ensemble models requires more processing power and time.
3) Limited Real-Time Implementation: The current system is tested on batch data and requires further optimization for real-time deployment.
4) Hardware Constraints: Performance may vary on low-end systems due to large dataset size.
5) Model Generalization: The system may require retraining to adapt to new or unseen attack patterns.

X. CONCLUSIONS

This study presents a machine learning-based system for detecting and mitigating privilege escalation attacks in cloud environments. By leveraging ensemble learning techniques and advanced algorithms such as Random Forest, AdaBoost, XGBoost, LightGBM, and CatBoost, the system achieves high accuracy of up to 97%, demonstrating the effectiveness of ML-based approaches in cybersecurity.

The system integrates data preprocessing, model training, evaluation, and prediction into a unified framework, enabling efficient detection of insider threats. The use of the CERT dataset and high-dimensional feature analysis allows accurate identification of anomalous user behavior associated with privilege escalation. Experimental results show strong performance in terms of accuracy, precision, recall, and F1-score, along with acceptable processing time.

Overall, the proposed system provides a reliable, scalable, and efficient solution for enhancing cloud security. It reduces dependency on traditional rule-based methods and improves the detection of complex insider attacks. The study highlights the growing importance of machine learning in cybersecurity and opens opportunities for future enhancements such as real-time monitoring and deep learning integration.

ACKNOWLEDGMENT

The authors sincerely thank the Department of Computer Science and Engineering of our institution for providing the necessary support and infrastructure to complete this project. We express our heartfelt gratitude to our project guide for their continuous guidance, encouragement, and valuable suggestions throughout the development of this work.

We also extend our thanks to the contributors of the CERT Insider Threat Dataset for providing valuable data resources. Finally, we acknowledge the open-source community and developers of machine learning libraries such as Scikit-learn, LightGBM, XGBoost, and CatBoost for their tools and support in implementing this project.

REFERENCES

[1] U. A. Butt, R. Amin, H. Aldabbas, S. Mohan, B. Alouffi, and A. Ahmadian, ‘‘Cloud-based email phishing attack using machine and deep learning algorithm,’’ Complex Intell. Syst., pp. 1–28, Jun. 2022.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 9, April 2026 Impact Factor: 8.2

[2] D. C. Le and A. N. Zincir-Heywood, ''Machine learning based insider threat modelling and detection,'' in Proc. IFIP/IEEE Symp. Integr. Netw. Service Manag. (IM), Apr. 2019, pp. 1–6.
[3] P. Oberoi, ''Survey of various security attacks in clouds based environments,'' Int. J. Adv. Res. Comput. Sci., vol. 8, no. 9, pp. 405–410, Sep. 2017.
[4] 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.
[5] 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.
[6] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. Bilal, ''Smart home security: Challenges, issues and solutions at different IoT layers,'' J. Supercomput., vol. 77, no. 12, pp. 14053–14089, Dec. 2021.
[7] S. Zou, H. Sun, G. Xu, and R. Quan, ''Ensemble strategy for insider threat detection from user activity logs,'' Comput., Mater. Continua, vol. 65, no. 2, pp. 1321–1334, 2020.
[8] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, ''On the effectiveness of machine and deep learning for cyber security,'' in Proc. 10th Int. Conf. Cyber Conflict (CyCon), May 2018, pp. 371–390.
[9] D. C. Le, N. Zincir-Heywood, and M. I. Heywood, ''Analyzing data granularity levels for insider threat detection using machine learning,'' IEEE Trans. Netw. Service Manag., vol. 17, no. 1, pp. 30–44, Mar. 2020.
[10] F. Janjua, A. Masood, H. Abbas, and I. Rashid, ''Handling insider threat through supervised machine learning techniques,'' Proc. Comput. Sci., vol. 177, pp. 64–71, Jan. 2020.
[11] R. Kumar, K. Sethi, N. Prajapati, R. R. Rout, and P. Bera, ''Machine learning based malware detection in cloud environment using clustering approach,'' in Proc. 11th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT), Jul. 2020, pp. 1–7.
[12] D. Tripathy, R. Gohil, and T. Halabi, ''Detecting SQL injection attacks in cloud SaaS using machine learning,'' in Proc. IEEE 6th Int. Conf. Big Data Secur. Cloud (BigDataSecurity), Int. Conf. High Perform. Smart Comput., (HPSC), IEEE Int. Conf. Intell. Data Secur. (IDS), May 2020, pp. 145–150.
[13] X. Sun, Y. Wang, and Z. Shi, ''Insider threat detection using an unsupervised learning method: COPOD,'' in Proc. Int. Conf. Commun., Inf. Syst. Comput. Eng. (CISCE), May 2021, pp. 749–754.
[14] J. Kim, M. Park, H. Kim, S. Cho, and P. Kang, ''Insider threat detection based on user behavior modeling and anomaly detection algorithms,'' Appl. Sci., vol. 9, no. 19, p. 4018, Sep. 2019.
[15] L. Liu, O. de Vel, Q.-L. Han, J. Zhang, and Y. Xiang, ''Detecting and preventing cyber insider threats: A survey,'' IEEE Commun. Surveys Tuts., vol. 20, no. 2, pp. 1397–1417, 2nd Quart., 2018.
[16] P. Chattopadhyay, L. Wang, and Y.-P. Tan, ''Scenario-based insider threat detection from cyber activities,'' IEEE Trans. Computat. Social Syst., vol. 5, no. 3, pp. 660–675, Sep. 2018.
[17] G. Ravikumar and M. Govindarasu, ''Anomaly detection and mitigation for wide-area damping control using machine learning,'' IEEE Trans. Smart Grid, early access, May 18, 2020, doi: 10.1109/TSG.2020.2995313.
[18] M. I. Tariq, N. A. Memon, S. Ahmed, S. Tayyaba, M. T. Mushtaq, N. A. Mian, M. Imran, and M. W. Ashraf, ''A review of deep learning security and privacy defensive techniques,'' Mobile Inf. Syst., vol. 2020, pp. 1–18, Apr. 2020.
[19] D. S. Berman, A. L. Buczak, J. S. Chavis, and C. L. Corbett, ''A survey of deep learning methods for cyber security,'' Information, vol. 10, no. 4, p. 122, 2019.
[20] N. T. Van and T. N. Thinh, ''An anomaly-based network intrusion detection system using deep learning,'' in Proc. Int. Conf. Syst. Sci. Eng. (ICSSE), 2017, pp. 210–214