IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024

# Machine Learning Approaches for Detecting and Mitigating Privilege Escalation Attack

**Miss. Rupali Marathe[1], Miss. Rutuja Zombade[2], Mr. Pankaj Kandekar[3], Mr. Omkar Bulbule [4], Asst. Prof. Dr. H. B. Jadhav[5]**
Department of Computer Engineering[1-5]
Adsul Technical Campus, Chas, Ahmednagar, India

**Abstract:** *Privilege escalation attacks are a serious threat to cloud computing security. In these attacks, an attacker exploits vulnerabilities in a system to gain elevated privileges, which can then be used to steal data, launch further attacks, or disrupt operations. Because of the recent exponential rise in attack frequency and sophistication, the proliferation of smart things has created significant cybersecurity challenges. Even though the tremendous changes cloud computing has brought to the business world, its centralization makes it challenging to use distributed services like security systems. Valuable data breaches might occur due to the high volume of data that moves between businesses and cloud service suppliers, both accidental and malicious. The malicious insider becomes a crucial threat tothe organization since they have more access and opportunity to produce significant damage. Unlike outsiders, insiders possess privileged and proper access to information and resources. In this work, a machine learning-based system for insider threat detection and classification is proposed and developed a systematic approach to identify various anomalous occurrences that may point to anomalies and security problems associated with privilege escalation. By combining many models, ensemble learning enhances machine learning outcomes and enables greater prediction performance. Multiple studies have been presented regarding detecting irregularities and vulnerabilities in network systems to find security flaws or threats involving privilege escalation. But these studies lack the proper identification of the attacks. This study proposes and evaluates ensembles of Machine learning (ML) techniques in this context. This project implements machine learning algorithms for the classification of insider attacks.*

**Keywords:** Artificial Intelligence, Industry, Intents, Insider Attack, Classification, Machine Learning Approaches,Networks, TF-IDF

## I. INTRODUCTION

Multiple studies have been presented regarding detecting irregularities and vulnerabilities in network systems to find security flaws or threats involving privilege escalation. But these studies lack the proper identification of the attacks. This study proposes and evaluates ensembles of Machine learning (ML) techniques in this context. They utilized the ‘‘CERT Insider Threat Tools’’ dataset since obtaining genuine business system logs is extremely challenging. Employee computer actions logs are included in the CERT dataset and certain organizational data such as employee’s departments and responsibilities. They built insider-threat detection models to emulate real- world companies using machine learning-based methods. Privilege escalation attacks involve an attacker gaining higher-level access permissions than originally intended, potentially compromising the entire cloud infrastructure. Traditional security measures may not be sufficient to detect and prevent these sophisticated attacks. This research explores the integration of machine learning into cloud security to fortify defences against privilege escalation threats. To detect privilege escalation attempts, our system employs supervised machine learning models trained on historical data and anomaly detection algorithms. These models analyse patterns of user behaviour, system interactions, and access requests to identify deviations from normal activities. By continuously learning and adapting to evolving threat landscapes, the system can identify suspicious activities indicative of privilege escalation attempts.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024

## II. LITERATURE SURVEY

| Title | Year | Description | Limitations |
|---|---|---|---|
| **P.Oberoi** Survey of various security attacks in basedin clouds-based environments. | 2017 | In this paper we have studied the various security attacks (in general) with reference to the Clouds (as per The Treacherous 12 – Cloud Computing. | Less Applicable. |
| **D.C. Le and A. N. Zincir Heywood,** Machine Learning based insider threat modelling and detection. | 2019 | This paper proposes a new framework in constructing a user- centred machine learning based insider threat detection system on multiple data granularity levels. | More Complex |
| **D. Tripathy, R. Gohil, and T. Halabi** ‘Detecting SQL injection attacks in cloudSaaS using machine learning,’’ | 2020 | The SQL injection attack is one of the most potential threat to a SaaS application. This may result in loss of sensitive and important data. The purposeof this research paper is to investigate the potential of using machine learning techniques for SQL injection detection onthe application level. | Less Applicable |
| **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. | 2022 | Cloud computing refers to the on-demand availability of personal computer system assets, specifically data storage and processing power. Without the client’s input. Emails are commonly used to send and receive data. | Less Secure |
| **Ajmal, S. Ibrar, and R. Amin** ‘‘Cloud computing platform: Performance analysis of prominent cryptographic algorithms,’’ | 2022 | In this paper cloud cryptography is a technique that uses encryption algorithms to secure data. The significant advantage of cloud storage is no difficulty to get to, low protection and fixing cost so every association is working with the cloud. | More Complex |
| **MUHAMMAD MEHMOOD1, RASHID AMIN,2MUHANA MAGBOUL ALI MUSLAM 3,JIANG XIE 4** Privilege Escalation Attack Detection and Mitigation in Cloud Using Machine Learning | 2023 | This paper implements machine learning algorithms for the classification of insider attacks. A customized dataset from multiple filles of the CERT dataset is used. | More complex |

## III. PURPOSE

Attackers target data sources because they have the most valuable and sensitive information. Every cloud user’s privacy and security are affected if data is lost. Insider threats are harmful operations carried out by people with authorization. In this problem we are providing best solution to avoid attack and detection of attack location. We evaluate the proposed system using real-world datasets and simulated privilege escalation scenarios. Performance metrics such as precision, recall, and false positive rates will be analysed to assess the effectiveness of the machine learning models in detecting and mitigating privilege escalation attacks.

### OBJECTIVE OF SYSTEM

- **Detection Enhancement:** Improve the current capabilities of privilege escalation attack detection by leveragingmachine learning algorithms.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024

- **Automated Mitigation:** Develop and integrate automated mitigation strategies to respond promptly to detectedprivilege escalation attempts.
- **Feature Engineering:** Explore and optimize relevant features for machine learning model training, including userbehaviour, access timestamps, and resource utilization.
- **Comprehensive Data Sources:** Utilize diverse data sources, including logs from authentication systems, access controllists, and system call traces, to provide a holistic view of user activities.
- **Evaluation Metrics:** Evaluate the proposed system's performance using real-world datasets and simulated scenarios.

## IV. PROPSED SYSTEM

The recent exponential rise in attack frequency and sophistication, the proliferation of smart things has created significant cybersecurity challenges. Even though the tremendous changes cloud computing has brought to the business world, its centralization makes it challenging to use distributed services like security systems. Valuable data breaches might occur due to the high volume of data that moves between businesses and cloud service suppliers, both accidental and malicious.

## V. ACTIVITY DIAGRAM

Attackers target data sources because they have the most valuable and sensitive information. Every cloud user's privacy and security are affected if data is lost. Insider threats are harmful operations carried out by people with authorization. With the fast growth of networks, many companies and organizations have established their internal networks. The malicious insider becomes a crucial threat to the organization since they have more access and opportunity to produce significant damage. Unlike outsiders, insiders possess privileged and proper access to information and resources. Insider risks may be defined and addressed using criteria including insider indications, detection approaches, and insider kinds. There are two sorts of analysis intervals: real-time, which may identify malicious activity in real-time, and offline anomaly detection, which gathers log data and looks for certain patterns.

## VI. APPLICATIONS

- Anomaly Detection: ML algorithms can analyze user behavior to detect unusual patterns, indicating potential privilege escalation attempts.
- User and Entity Behavior Analytics (UEBA): ML models can identify abnormal activities among users and entities, helping to detect unauthorized access or privilege escalation.
- Banking Application.
- Company Application.

## VII. RESULT

**Admin Dashboard:**

After admin login successfully admin can access his dashboard in below image admin can check register users.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024

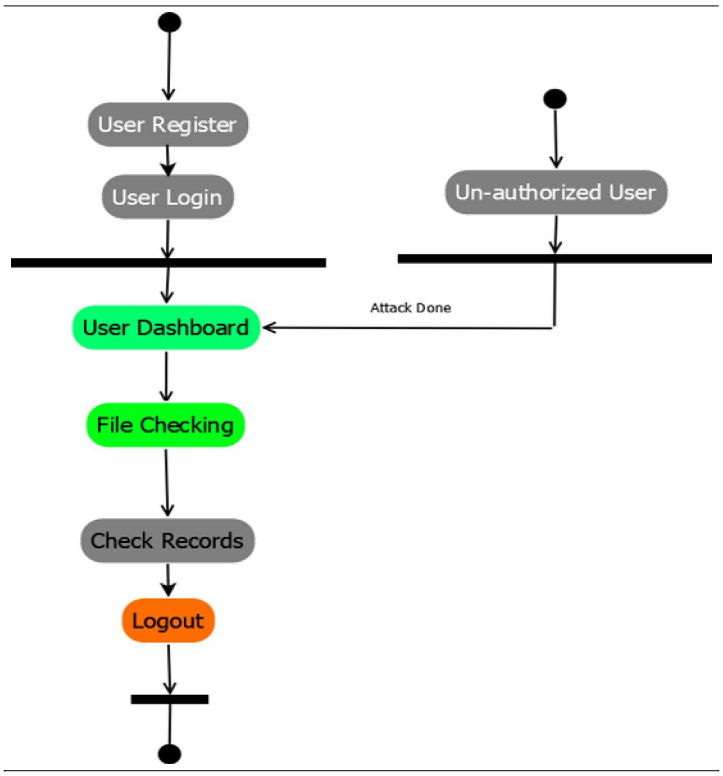
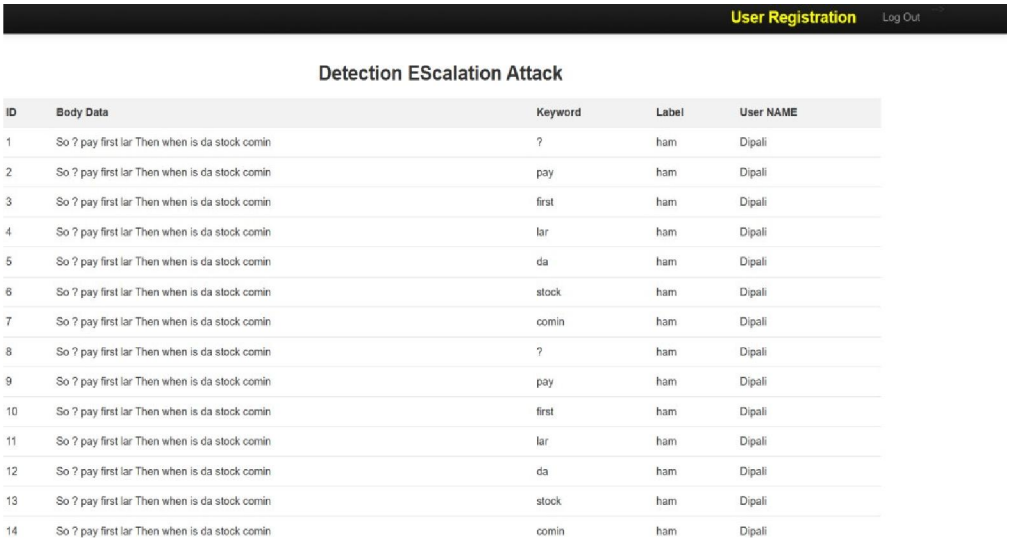





Fig .1 Admin Dashboard

**Trained Data:**
After admin login admin can train dataset to detect attacks.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024




| ID | Body Data | Keyword | Label | User NAME |
|---|---|---|---|---|
| 1 | So ? pay first lar Then when is da stock comin | ? | ham | Dipali |
| 2 | So ? pay first lar Then when is da stock comin | pay | ham | Dipali |
| 3 | So ? pay first lar Then when is da stock comin | first | ham | Dipali |
| 4 | So ? pay first lar Then when is da stock comin | lar | ham | Dipali |
| 5 | So ? pay first lar Then when is da stock comin | da | ham | Dipali |
| 6 | So ? pay first lar Then when is da stock comin | stock | ham | Dipali |
| 7 | So ? pay first lar Then when is da stock comin | comin | ham | Dipali |
| 8 | So ? pay first lar Then when is da stock comin | ? | ham | Dipali |
| 9 | So ? pay first lar Then when is da stock comin | pay | ham | Dipali |
| 10 | So ? pay first lar Then when is da stock comin | first | ham | Dipali |
| 11 | So ? pay first lar Then when is da stock comin | lar | ham | Dipali |
| 12 | So ? pay first lar Then when is da stock comin | da | ham | Dipali |
| 13 | So ? pay first lar Then when is da stock comin | stock | ham | Dipali |
| 14 | So ? pay first lar Then when is da stock comin | comin | ham | Dipali |

Fig.2 Train data

**Send Mail**

User can send mail if mail contain spam so system will detect spam or ham.

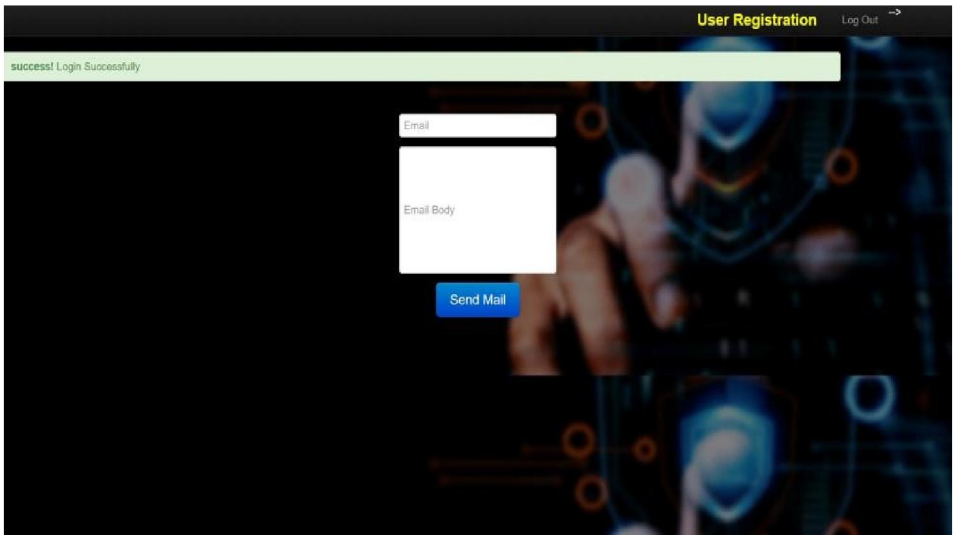
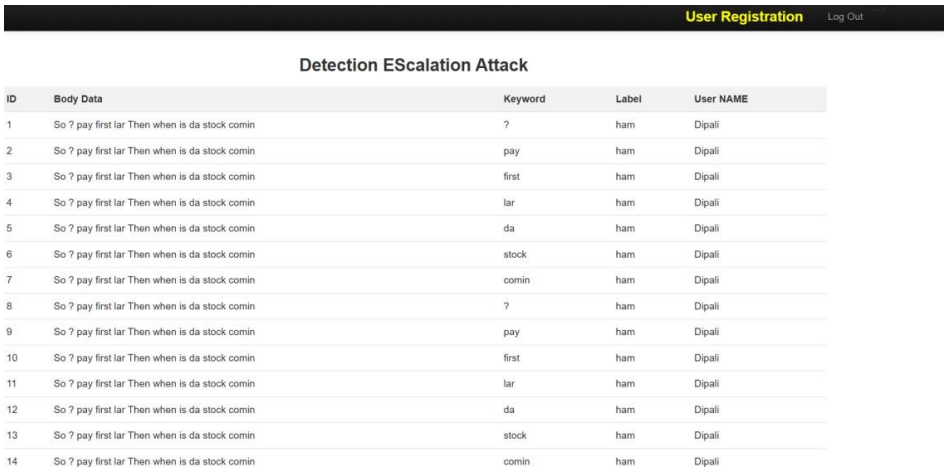



**Fig 3. Send mail.**

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024

**Detection of spam**




| ID | Body Data | Keyword | Label | User NAME |
|---|---|---|---|---|
| 1 | So ? pay first lar Then when is da stock comin | ? | ham | Dipali |
| 2 | So ? pay first lar Then when is da stock comin | pay | ham | Dipali |
| 3 | So ? pay first lar Then when is da stock comin | first | ham | Dipali |
| 4 | So ? pay first lar Then when is da stock comin | lar | ham | Dipali |
| 5 | So ? pay first lar Then when is da stock comin | da | ham | Dipali |
| 6 | So ? pay first lar Then when is da stock comin | stock | ham | Dipali |
| 7 | So ? pay first lar Then when is da stock comin | comin | ham | Dipali |
| 8 | So ? pay first lar Then when is da stock comin | ? | ham | Dipali |
| 9 | So ? pay first lar Then when is da stock comin | pay | ham | Dipali |
| 10 | So ? pay first lar Then when is da stock comin | first | ham | Dipali |
| 11 | So ? pay first lar Then when is da stock comin | lar | ham | Dipali |
| 12 | So ? pay first lar Then when is da stock comin | da | ham | Dipali |
| 13 | So ? pay first lar Then when is da stock comin | stock | ham | Dipali |
| 14 | So ? pay first lar Then when is da stock comin | comin | ham | Dipali |

**Fig 4 Spam mail**

**Graph**

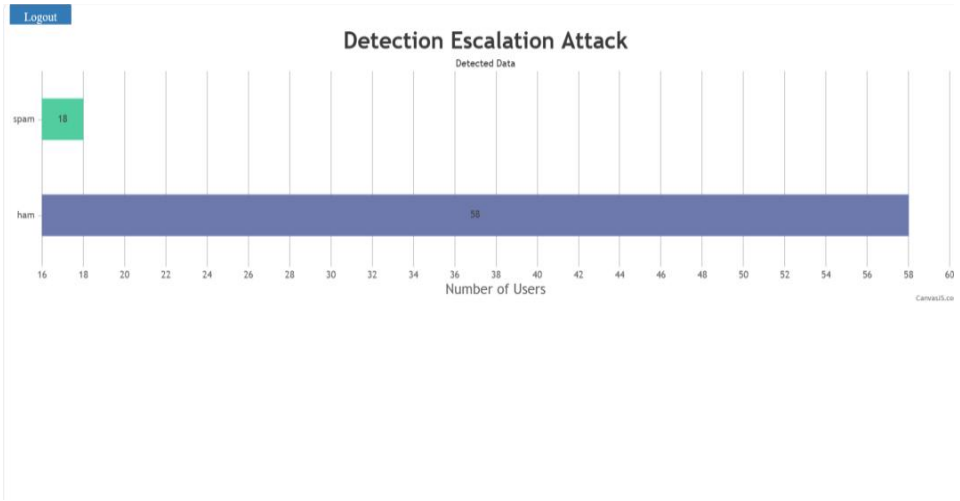



Fig 5 Graph

## VIII. CONCLUSION

The malicious insider becomes a crucial threat to the organization since they have more access and opportunity to produce significant damage. Unlike outsiders, insiders possess privileged and proper access to information and resources. This paper proposed machine learning algorithms for detecting and classifying an insider attack. A customized dataset from multiple files of the CERT dataset is used in this work. Using these super- vised machine learning algorithms, this paper demonstrated the effective experimental results having higher accuracy in the classification report.

## IX. ACKNOWLEDGMENT

We express our heartfelt gratitude to our esteemed mentors and professors, especially, for their invaluable guidance in our academic and project endeavours. We also extend our thanks to the COMPUTER ENGINEERING Department and its staff for their continuous support. Our sincere thanks go to Dr. P.M. Patil Principal of Adsul Technical Campus Chas, Ahmednagar for his support and permission to complete this project. We appreciate the assistance of our

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 6, April 2024

department's support staff, and we're grateful to our parents, friends, and all those who supported us throughout 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.
[2] D. C. Le and A. N. Zincir-Heywood, "Machine learning based insider threat modelling and detection", Proc. IFIP/IEEE Symp. Integr. Netw. Service Manag. (IM), pp. 1-6, Apr. 2019.
[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.
[3] A. Ajmal, S. Ibrar and R. Amin, "Cloud computing platform: Performance analysis of prominent cryptographic algorithms", Concurrency Comput. Pract. Exper., vol. 34, no. 15, pp. e6938, Jul. 2022.
[4] 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.
[5] 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.
[6] 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.
[7] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido and M. Marchetti, "On the effectiveness of machine and deep learning for cyber security", Proc. 10th Int. Conf. Cyber Conflict (CyCon), pp. 371-390, May 2018.
[8] D. C. Le, N. Zincir-Heywood and M. I. Heywood, "Analysing data granularity levels for insider threat detection using machine learning", IEEE Trans. Netw. Service Manag., vol. 17, no. 1, pp. 30-44, Mar. 2020.
[9] Privilege Escalation Attack Detection and Mitigation in Cloud Using Machine Learning MUHAMMAD MEHMOOD1 , RASHID AMIN 1,2 , MUHANA MAGBOUL ALI MUSLAM 3 , (Member, IEEE), JIANG XIE 4 , (Fellow, IEEE), AND HAMZA ALDABBAS 5 17 May 2023