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 2, January 2024

Privilege Escalation Attack Detection and Mitigation in Cloud using Machine Learning

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

Abstract: *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 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. 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, examples

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 defenses 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 analyze patterns of user behavior, 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

II. 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

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 2, January 2024

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 analyzed to assess the effectiveness of the machine learning models in detecting and mitigating privilege escalation attacks.

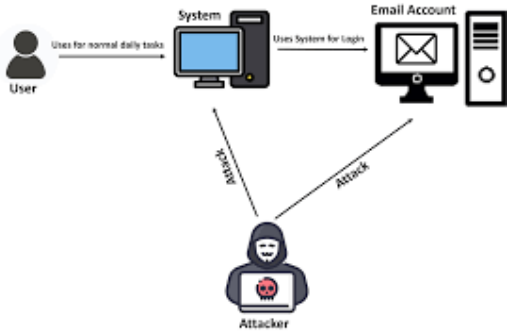
III. OBJECTIVE OF SYSTEM

- **Detection Enhancement:** Improve the current capabilities of privilege escalation attack detection by leveraging machine learning algorithms.
- **Automated Mitigation:** Develop and integrate automated mitigation strategies to respond promptly to detected privilege escalation attempts.
- **Feature Engineering:** Explore and optimize relevant features for machine learning model training, including user behavior, access timestamps, and resource utilization.
- **Comprehensive Data Sources:** Utilize diverse data sources, including logs from authentication systems, access control lists, 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. PROPOSED SYSTEM

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.

V. SYSTEM ARCHITECTURE



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. 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

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 2, January 2024

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.

VII. 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 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, "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.