International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

PRIVILEGE ESCALATION ATTACK DETECTION AND MITIGATION IN CLOUD USING MACHINE LEARNING

[1]B.AVINASH,[2]RYAKAM RISHWANTH PATEL,[3]MANTENA RUTWIK VARMA,[4]M.PIRIYA,[5]MS.K.THEJA

[1,2,3,4]Students, Department of computer Science And Engineering,Malla Reddy Engineering College (Autonomous),Hyderabad Telangana, India 500100

[5]Assistant Professor, Department of computer Science And Engineering, Malla Reddy Engineering College (Autonomous),Hyderabad Telangana, India 500100

ABSTRACT

The rapid expansion of smart devices has led to a significant rise in cyber security challenges, driven by an increase in both the frequency and sophistication of attacks. While cloud computing has brought transformative changes to businesses, its centralized nature complicates the use of distributed services, such as security systems. With the massive volume of data exchanged between companies and cloud service providers, the potential for data breaches—both accidental and malicious—has grown. Malicious insiders pose a particular threat, as they have privileged access and the opportunity to cause considerable damage. Unlike external attackers, insiders have legitimate access to sensitive information and resources. This paper proposes and develops a machine learning-based system for detecting and classifying insider threats. It presents a systematic approach to identifying anomalous behaviors that could indicate security issues related to privilege escalation. The use of ensemble learning further enhances the performance of the machine learning models. Previous studies have addressed detecting irregularities in network systems related to privilege escalation but often fail to properly identify specific attacks. This study evaluates various machine learning techniques, applying them to a customized dataset derived from multiple files of the CERT dataset. Four algorithms—Random Forest (RF), AdaBoost, XGBoost, and LightGBM—are tested and analyzed. Among these, LightGBM achieved the highest accuracy of 97%, with RF at 86%, AdaBoost at 88%, and XGBoost at 88.27%. The findings suggest that combining multiple machine learning algorithms may offer more robust classification capabilities for various types of internal attacks.

Keywords: Privilege Escalation, Cloud Security, Machine Learning, Anomaly Detection, Intrusion Detection System (IDS), Threat Mitigation, Cybersecurity, User Behavior Analytics, Cloud Infrastructure, Attack Detection.

I.INTRODUCTION

Cloud computing represents a transformative approach to service delivery through the internet. However, the current financial crises, along with the growing demand for computing power, have pushed for significant changes in cloud models, particularly in terms of data storage, processing, and presentation [1]. By leveraging cloud infrastructure, cloud computing helps businesses avoid excessive spending on equipment maintenance and purchases. Cloud storage providers implement essential security measures, including encryption, access control, and authentication, to protect both their systems and the data they manage. Cloud services offer vast data storage capabilities, allowing businesses to store various types of data across different cloud

storage architectures, depending on factors like data access frequency and speed. Despite these security measures, the vast volume of data exchanged between businesses and cloud service providers presents a risk, as both accidental and malicious breaches can occur. Cloud services also face security vulnerabilities related to authentication and open interfaces, which can be exploited by skilled hackers to gain unauthorized access to systems.

Machine learning (ML) provides a promising solution to address these security challenges, offering a range of techniques and algorithms to better manage data and improve security. However, privacy concerns often prevent the release of important datasets, and these datasets may lack essential statistical properties [3], [4]. The rapid growth of the cloud industry has heightened privacy and security risks, often governed by regulations. A critical issue in cloud environments is the management of employee access privileges, which may not always be updated when employees change roles or positions within the company. This oversight can lead to the inappropriate use of outdated privileges, potentially resulting in data theft or system damage. In cloud systems, access to sensitive data is typically restricted to approved users, and malicious attackers can exploit higher user privileges to compromise security and access sensitive information.

Attackers can escalate privileges horizontally or vertically to gain unauthorized access. Horizontal privilege escalation occurs when an attacker gains access to the same level of privileges as another user, allowing them to access data they should not have. This type of attack is often enabled by poorly designed web applications and allows attackers to view, modify, or steal sensitive information [3], [5]. On the other hand, vertical privilege escalation involves gaining higher levels of access, such as admin or root privileges. In this scenario, an attacker can move from a low-level user account to gain control over critical systems. Detecting such anomalies through behavioral analytics can help identify and mitigate privilege escalation attacks.

Insider threats, where authorized individuals abuse their privileges, pose a significant risk to cloud security. As organizations expand their internal networks, insider attacks become more prevalent, with estimates suggesting that 90% of businesses believe they are vulnerable to such threats [7]. Insider attackers often exploit privilege escalation to gain access to more sensitive systems or perform malicious actions. These attacks are challenging to detect and prevent due to the attackers' privileged access and the fact that their actions often occur below the radar of enterprise-level security defenses. Detecting and classifying insider threats has thus become a complex and time-consuming task [8]. Researchers have developed various machine learning and deep learning techniques, such as SVM, Naïve Bayes, CNN, Linear Regression, PCA, Random Forest, and KNN, to address these challenges. However, there is a need for faster and more effective ML algorithms to handle the diverse range of insider attack types. Therefore, an efficient strategy is required to detect, classify, and mitigate insider threats effectively.

To enhance security protection, intelligent algorithms like ML are crucial for classifying and predicting insider attacks [17]. Understanding the performance of

ML algorithms in identifying insider attacks helps determine the most suitable algorithm for each case, and improving these algorithms can strengthen security measures. This study aims to apply effective ML algorithms to insider attack scenarios to achieve faster and more accurate results. The study evaluates four ML algorithms: Random Forest, AdaBoost, XGBoost, and LightGBM. Boosting strategies, which involve enhancing weak classifiers to improve predictions, are utilized in this research. These algorithms were tested for their ability to classify insider threats accurately and efficiently.

The contributions of this research include:

1. Training ML models in a realistic context to generate results that reflect real-world scenarios.
2. Developing and analyzing a user-centered insider attack detection process, including data collection, preprocessing, and analysis using ML models.
3. Providing a detailed reporting procedure to evaluate malicious incidents based on instance and user-specific results.

To the best of our knowledge, this is the first paper to assess the performance of four ML algorithms—Random Forest, AdaBoost, XGBoost, and LightGBM—on classifying insider attacks and to use these results to select appropriate defense tools to enhance security. Previous studies on insider threat detection and classification typically implemented individual models on different datasets. In contrast, this paper implements the four ensemble models on a single customized dataset, resulting in improved insider threat detection and classification. The study presents the best results from the applied ensemble algorithms. The structure of this paper is as follows: Section I introduces cloud computing and privilege escalation attacks. Section II reviews related work in this field. Section III outlines the proposed methodology, including the application of machine learning algorithms. Section IV details the dataset, experimental setup, and results evaluation. The paper concludes in Section V.

II.LITERATURE SURVEY

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., Jun. 2022.

This study explores the application of machine and deep learning algorithms in detecting cloud-based email phishing attacks. As phishing remains a significant threat to cloud services, the authors propose an innovative approach to detecting phishing attacks within email systems by leveraging advanced machine learning models. The paper investigates how various machine learning techniques can be used to analyze email content, sender information, and patterns of suspicious activity to detect potential phishing attempts. The study provides a thorough comparison of different algorithms, highlighting the effectiveness of deep learning models in identifying phishing emails compared to traditional methods. Additionally, the authors discuss the challenges and limitations in applying machine learning for email phishing detection, including data preprocessing and the need for large, labeled datasets. The paper concludes by suggesting improvements for integrating these models into cloud-based security frameworks to

enhance protection against phishing attacks.

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.

In this paper, the authors focus on applying machine learning to model and detect insider threats in network systems. Insider threats, often difficult to identify, are a critical concern for organizations, especially given the growing volume of sensitive data and the sophistication of attacks. The authors propose a novel framework based on machine learning algorithms that can detect suspicious activities indicative of insider threats. The study delves into the creation of insider threat detection models that can analyze user behavior, access logs, and system interactions to identify potential threats. By comparing different machine learning techniques, the paper highlights the strengths and weaknesses of each method for detecting insider threats, providing valuable insights into selecting the appropriate algorithm for a given context. This research contributes to the development of more efficient and proactive security measures for detecting malicious insiders within organizations.

P. Oberoi, "Survey of various security attacks in clouds based environments," Int. J. Adv. Res. Comput. Sci., Sep. 2017.

This survey paper provides a comprehensive overview of the various security attacks faced by cloud-based environments. As cloud computing becomes more prevalent, the security risks associated with it have grown exponentially. The paper categorizes and discusses different types of attacks, such as data breaches, denial of service (DoS), man-in-the-middle (MitM) attacks, and privilege escalation, among others. The author examines the underlying causes of these threats and provides a detailed analysis of their impact on cloud services, emphasizing the need for robust security measures. Furthermore, the paper reviews various security protocols and countermeasures currently employed in the cloud, highlighting their effectiveness and limitations. Oberoi suggests that to ensure the security and integrity of cloud services, organizations must implement a combination of technical, administrative, and physical security measures, along with a continuous assessment of emerging threats.

A. Ajmal, S. Ibrar, and R. Amin, "Cloud computing platform: Performance analysis of prominent cryptographic algorithms," Concurrency Comput., Pract. Exper., Jul. 2022.

This paper examines the performance of prominent cryptographic algorithms in the context of cloud computing platforms. Given the sensitive nature of the data stored and processed in the cloud, ensuring robust data encryption is critical for safeguarding privacy and preventing unauthorized access. The authors conduct a comparative analysis of several cryptographic algorithms, including AES, RSA, and ECC, focusing on their performance metrics such as execution time, computational efficiency, and scalability in cloud environments. The study highlights the strengths and limitations of each algorithm in handling large datasets and maintaining high levels of security without compromising performance. By evaluating the algorithms under various operational conditions, the paper provides valuable insights for cloud

service providers in choosing the most suitable cryptographic techniques for protecting data. The findings also contribute to the ongoing discourse on optimizing cloud security measures while balancing encryption strength and system performance.

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., Jan. 2023.

This paper offers a detailed survey of the security threats faced by cloud computing platforms and explores the various solutions proposed to mitigate these threats. As cloud computing continues to evolve, the risk of data breaches, unauthorized access, and denial-of-service (DoS) attacks remains a significant concern. The authors categorize cloud security threats into several types, including data-related threats, network security issues, and service availability risks. In addition to discussing the various types of threats, the paper presents a range of security solutions, such as encryption techniques, access control mechanisms, and intrusion detection systems. The authors also discuss emerging trends in cloud security, such as the integration of machine learning and artificial intelligence for threat detection and mitigation. The paper concludes with a call for continued research in developing more advanced security measures to address the evolving landscape of cloud computing threats.

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., Dec. 2021.

This paper focuses on the security challenges faced by smart homes, specifically addressing the issues arising at different layers of the Internet of Things (IoT) architecture. Smart homes, which integrate various connected devices and sensors, face unique security vulnerabilities due to the complexity and heterogeneity of the IoT ecosystem. The authors identify the primary security challenges, including unauthorized access to devices, data breaches, and vulnerabilities in communication protocols. They also explore the security risks associated with the cloud platforms used to manage smart home data. The paper provides an in-depth analysis of existing security measures at each IoT layer, such as device authentication, data encryption, and secure communication protocols. Additionally, the authors propose new solutions and recommendations to improve security, emphasizing the importance of multi-layered security strategies to protect smart home systems from evolving cyber threats.

S. Zou, H. Sun, G. Xu, and R. Quan, "Ensemble strategy for insider threat detection from user activity logs," Comput., Mater. Continua, 2020.

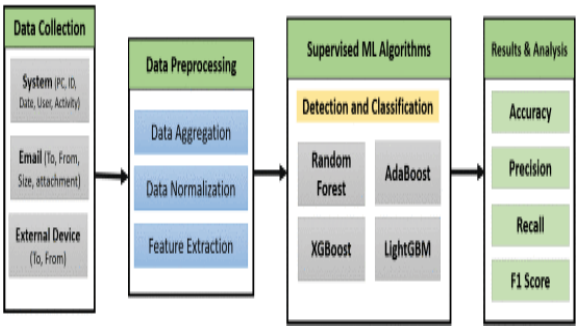
This paper presents an ensemble learning strategy for detecting insider threats based on user activity logs. Insider threats, which originate from authorized users, are particularly challenging to detect due to their legitimate access to sensitive information. The authors propose combining multiple machine learning models to enhance the accuracy and robustness of insider threat detection. The ensemble approach involves integrating models like decision trees, random forests, and support vector machines (SVM) to analyze user behavior logs and identify suspicious activities that may indicate a potential threat. The study demonstrates

that ensemble methods significantly improve detection performance by leveraging the strengths of individual models while minimizing their weaknesses. The authors validate their approach using real-world user activity data and show that it outperforms traditional single-model methods in terms of detection accuracy. This research contributes to the growing field of insider threat detection by proposing a more effective strategy to address this complex security challenge.

III.PROPOSED METHODOLOGY

In this study, a customized dataset compiled from multiple files of the CERT dataset is utilized to detect and classify insider threats using machine learning. The core objective is to develop a robust framework that applies four machine learning algorithms—Random Forest, AdaBoost, XGBoost, and LightGBM—for effective insider attack detection. The methodology integrates both mathematical modeling and technical implementation, as discussed in previous sections. Ensemble learning, specifically bagging and boosting techniques, plays a key role in improving model performance. Bagging is employed through Random Forest, while boosting is implemented using AdaBoost, XGBoost, and LightGBM.

During the data preprocessing phase, data aggregation helps extract meaningful insights, while data normalization ensures that all features are on a comparable scale, improving model performance and training stability. Feature extraction reduces redundancy, enabling faster training and efficient model generalization. Boosting, a vital part of ensemble learning, combines multiple weak learners to create a strong model. Among the four algorithms tested, LightGBM demonstrates the highest accuracy, proving to be the most effective for insider threat detection in this study.



IV.CONCLUSION

Malicious insiders present a significant threat to organizations due to their privileged access and the potential to cause substantial damage. Unlike external attackers, insiders have legitimate access to sensitive information and resources, making their actions harder to detect and prevent. This paper proposed the use of machine learning algorithms to detect and classify insider attacks. A customized dataset derived from multiple files of the CERT dataset was utilized for this analysis. Four machine learning algorithms—Random Forest, AdaBoost, XGBoost, and LightGBM—were applied to the dataset, yielding promising results. Among the proposed algorithms, LightGBM achieved the highest accuracy at 97%, followed by XGBoost at 88.27%, AdaBoost at 88%, and Random Forest at 86%. The findings highlight the effectiveness of these supervised learning models in detecting insider threats. Future work can enhance these models' performance by increasing the dataset's size and diversity, as well as incorporating evolving patterns of insider attack techniques. This could lead to new research directions in insider threat detection across various organizational domains. Machine learning models play a vital role in enabling businesses to make

informed decisions, and improvements in model accuracy can reduce the cost of errors. ML-based research empowers organizations to process large amounts of data, enabling algorithms to analyze, recommend, and make decisions based on the provided information.

V.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," 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. 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.

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.