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

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.

DOI: 10.48175/568