Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, No.8, May : 2024

DETECTION OF CYBER ATTACKS IN NETWORK BY USING MACHINE LEARNING TECHNIQUES

Mrs. P. Sri Jyothi, Department of Information Technology, Vignan's Institute of Information Technology(A), Visakhapatnam-530049
Mr. Mamidi Sasidhar, MCA Student, Department of Master of Computer Applications, Vignan's Institute of Information Technology(A), Visahkapatnam-530049

Abstract:
The swift advancements in computing and telecommunications technologies have introduced substantial and intricate transformations in comparison to previous eras. While these emerging technologies offer immense advantages to individuals, businesses, and governmental bodies, they also present challenges such as ensuring the safeguarding of sensitive information, fortifying storage platforms, and guaranteeing data accessibility. A prominent concern in today's landscape is cyber warfare, which has spawned numerous issues for both individuals and organizations, reaching a magnitude where it could undermine public and national security, perpetrated by an array of entities including criminal syndicates, skilled operatives, and cyber activists. To counter these looming threats, Intrusion Detection Systems (IDS) have been engineered to threat cyber Attacks. In a recent investigation, machine learning algorithms like Support Vector Machines (SVM) were deployed to identify port scan attempts utilizing the newly introduced CICIDS2017 dataset, yielding accuracy rates of 97.80% and 69.79% respectively. Instead of SVM, alternative algorithms such as Random Forest, Decision Tree, Logistic Regression and Artificial Neural Networks (ANN) could be leveraged, potentially achieving accuracies of 93.29%, 63.52%, 99.93%, and 99.11% respectively.

Introduction:
Cyber-crime is rampant, exploiting vulnerabilities across computing environments. Ethical hackers focus on identifying vulnerabilities and suggesting mitigation strategies. Effective techniques are urgently needed in the cyber security community to address the ever-evolving and intricate landscape of cyber threats targeting computer networks has underscored the indispensable role of machine learning in bolstering cybersecurity defenses. The advancements in computing and communication technologies have ushered in transformative changes, offering myriad benefits to individuals, businesses, and governmental entities. Nonetheless, they also pose formidable challenges, including safeguarding data, securing stored information, and ensuring data accessibility. Cyber terrorism has emerged as a formidable menace, posing significant threats to both public and national security, orchestrated by diverse groups with malicious intent. To counter these digital incursions, Intrusion Detection Systems (IDS) have been devised as a proactive Defense Mechanism. In a recent examination, support vector machine (SVM) algorithms were deployed to detect port scan attempts with precision rates of 97.80% and 69.79% respectively, showcasing their efficacy in identifying potential threats. Alternative algorithms such as Random Forest (RF), Logistic Regression (LR), Decision Tree(DT) and Artificial Neural Networks (ANN) present comparable accuracy rates to SVM, with potentials of achieving 93.29%, 63.52%, 99.93%, and 99.11% respectively.

Literature Survey:
The frequency of attacks on networked systems has risen dramatically, with attackers' tactics evolving continuously. Issues such as data privacy, data platform security, and data availability have made cyber terrorism a significant global concern. Acts of cyber terrorism, orchestrated by an array of entities ranging from criminal syndicates to seasoned professionals and activists, pose significant threats to both public and national security. As a pivotal defence mechanism against such attacks, intrusion detection plays a crucial role, with Machine Learning offering a promising avenue for crafting robust Intrusion Detection Systems (IDS). In this investigation, deep learning and support vector machine

(SVM) algorithms are leveraged to identify port scan attempts utilizing the newly curated CICIDS2017 dataset. An Introduction to Network Intrusion Detection Systems (IDS): An IDS, whether in the form of software-based applications or hardware devices, 2 6 serves as a critical tool for identifying malicious activities within a network. Intrusion detection techniques are categorized into anomaly-based and signature-based approaches, with developers employing a plethora of methodologies to detect intrusions effectively. Information security encompasses a comprehensive array of measures designed to safeguard information from unauthorized access, usage, disclosure, destruction, modification, or any form of damage.

Conclusion:

In summary, this research provided assessments of Machine Learning (ML) techniques such as Decision Trees (DT), Random Forest (RF), Artificial Neural Network (ANN), Logistic Regression (LR), and Ensemble methods using the contemporary CICIDS2017 dataset. Findings demonstrate that the Ensemble method outperformed DT, RF, ANN, and LR. Future investigations will delve into the application of these techniques in identifying diverse cyber threats, including reconnaissance attempts, utilizing Apache Hadoop and Spark frameworks. By leveraging historical attack data stored in repositories, these techniques facilitate the prediction of cyber threats by scrutinizing patterns and anomalies in network traffic. Through a comparative analysis of the efficacy of DT, RF, ANN, LR, and Ensemble methods, this study aims to ascertain the most effective technique for enhancing cyber threat detection capabilities.

References:

[1] K. Graves, Ceh: Official certified ethical hacker review guide: Exam 312-50. John Wiley & Sons, 2007.
[2] R. Christopher, “Port scanning techniques and the defense against them,” SANS Institute, 2001.
[3] M. Baykara, R. Das¸, and I. Karado ˘gan, “Bilgi g ¨uvenli ˘gi sistemlerinde kullanilan arac¸larin incelenmesi,” in 1st International Symposium on Digital Forensics and Security (ISDFS13), 2013, pp. 231–239.
[4] S. Staniford, J. A. Hoagland, and J. M. McAlerney, “Practical automated detection of stealthy portscans,” Journal of Computer Security, vol. 10, no. 1-2, pp. 105–136, 2002.
[5] S. Robertson, E. V. Siegel, M. Miller, and S. J. Stolfo, “Surveillance detection in high bandwidth environments,” in DARPA Information Survivability Conference and Exposition, 2003. Proceedings, vol. 1. IEEE, 2003, pp. 130–138.
[6] K. Ibrahimi and M. Ouaddane, “Management of intrusion detection systems based-kdd99: Analysis with lda and pca,” in Wireless Networks and Mobile Communications (WINCOM), 2017 International Conference on. IEEE, 2017, pp. 1–6.
[7] N. Moustafa and J. Slay, “The significant features of the unsw-nb15 and the kdd99 data sets for network intrusion detection systems,” in Building Analysis Datasets and Gathering
Experience Returns for Security (BADGERS), 2015 4th International Workshop on. IEEE, 2015, pp. 25–31.
[8] L. Sun, T. Anthony, H. Z. Xia, J. Chen, X. Huang, and Y. Zhang, “Detection and classification of malicious patterns in network traffic using benford’s law,” in Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), 2017. IEEE, 2017, pp. 864–872.
[9] S. M. Almansob and S. S. Lomte, “Addressing challenges for intrusion detection system using naive bayes and pca algorithm,” in Convergence in Technology (I2CT), 2017 2nd International Conference for. IEEE, 2017, pp. 565–568.
[10] M. C. Raja and M. M. A. Rabbani, “Combined analysis of support vector machine and principle component analysis for ids,” in IEEE International Conference on Communication and Electronics Systems, 2016, pp. 1–5.