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: 7.301
Volume 3, Issue 1, August 2023

Review on Clustering and Classification techniques in Intrusion Detection Systems

Dr. S. Sandosh[1], Akila Bala[2], Nithin Kodipyaka[3]
Assistant Professor Sr., School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India [1]
Student, School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India [2]
Student, School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India [3]

Abstract: *In the modern cyber world, the proportion of security threats is cumulating every day, and many researchers and security specialists are focusing on IDS (Intrusion Detection Systems) and the patterns in recognizing the alerts / events to detect and prevent them. The researchers and security specialists believe that the IDS is best way to protect the network and information assets. Hence this paper is focused on various threats and potential of IDS with its patterns in detecting the alerts / events. Basically, IDS has three different styles in detection the threats: Signature-based Detection (SD), Anomaly-based Detection (AD), and Stateful Protocol Analysis (SPA). The main area where the researchers and security specialists focusing is on techniques and algorithms used for clustering and classification. This paper mainly supports in understanding and analysing the various patterns on clustering and classifying the previous alerts / events which mainly supports in detection of threats with accuracy. This review will help to increase the detection accuracy of the IDS by enhancing the clustering and classification techniques which supports efficient execution of IDS over the network.*

Keywords: Networking, Clustering, Classification, Intrusion Detection System.

REFERENCES

[1] Erman, J., Arlitt, M., Mahanti, A., 2006. Traffic classification using clustering algorithms. In *Proceedings of the 2006 SIGCOMM workshop on Mining network data* (pp. 281-286).
[2] Z. G. Sheng, S. S. Yang, Y. F. Yu, A. V. Vasilakos, J. A. McCann,and K. K. Leung, "A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities," IEEE Wireless Communications Magazine, vol. 20, no. 6, pp. 91– 98, 2013.
[3] Heady, R., Luger, G., Maccabe, A., &Servilla, M. (1990). The architecture of a network level intrusion detection system (No. LA-SUB-93-219). Los Alamos National Lab.(LANL), Los Alamos, NM (United States); New Mexico Univ., Albuquerque, NM (United States). Dept. of Computer Science.
[4] Maswood, M.M.S., Develder, C., Madeira, E. Medhi, D., 2017. Energy-efficient dynamic virtual network traffic engineering for north-south traffic in multi-location data center networks. *Computer Networks*, *125*, pp.90-102.
[5] Lackman, R.A., Spragins, J.D., Tipper, D., 1992. Scheduling real-time., non-real-time traffic under nonstationary conditions. *Annals of Operations Research*, *36*(1), pp.193-224.
[6] Mukkamala S, Janoski G, Sung A. Intrusion detection using neural networks and support vector machines. Paper presented at: Proceedings of the 2002 International Joint Conference on Neural Networks. IJCNN'02 (Cat. No. 02CH37290). Honolulu, HI, USA: IEEE; vol. 2, 2002:1702-1707.
[7] Garcia-Teodoro P, Diaz-Verdejo J, Maciá-Fernández G, Vázquez E. Anomaly-based network intrusion detection: techniques systems and challenges. ComputSecur. 2009;28(1-2):18-28.
[8] Liao, H.J., Lin, C.H.R., Lin, Y.C., Tung, K.Y., 2013. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, *36*(1), pp.16-24.
[9] Sandosh, S., Govindasamy, V., Akila, G., Deepasangavy, K., FemidhaBegam, S., Sowmiya, B., 2019. A progressive intrusion detection system through event processing: challenges and motivation. In *2019 IEEE International Conference on System, Computation, Automation, and Networking (ICSCAN)* (pp. 1-7). IEEE.

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: 7.301
Volume 3, Issue 1, August 2023

[10] Zhang, S., Liu, Y. and Yang, D., 2022. A Novel IDS Securing Industrial Control System of Critical Infrastructure Using Deception Technology. *International Journal of Digital Crime and Forensics (IJDCF)*, *14*(2), pp.1-20.
[11] Scherer, P., Vicher, M., Drazdilova, P., Martinovic, J., Dvorsky, J., Snasel, V., 2011. Using SVM and clustering algorithms in IDS systems. In *Proc. Int Conf. Dateso 2011, 2011*.
[12] Amudha, P., Karthik, S., Sivakumari, S., 2013. Classification techniques for intrusion detection-an overview. *International Journal of Computer Applications*, *76*(16)
[13] Erman, J., Arlitt, M., Mahanti, A., 2006. Traffic classification using clustering algorithms. In Proceedings of the 2006 SIGCOMM workshop on Mining network data (pp. 281-286).