Arpita Das, 2023, 11:4
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

A Survey on Intrusion Detection System Types and Techniques

Arpita Das, Prof. Sumit Sharma
Vaishnavi Institute of Science & Technology, Bhopal, MP India

Abstract- One of the goals of smart environments is to improve the quality of human life in terms of comfort and efficiency. The Intrusion detection system has recently evolved into a technology for building smart environments. Security and privacy are considered key issues in any real-world smart environment based on the network model. This paper has list techniques of intrusion detection system which optimize the input dataset as well. Many of researchers work was detailed in the paper that help to understand the approaches of the intrusion detection system. Network has different types of attacks as per network type and requirements, so attacks were also mentioned in the paper.

Keywords: **Intrusion Detection System, Anomaly Detection, SNORT, SURICATA, Bro IDS.**

I. INTRODUCTION

The process of monitoring and analysing events in a computer system or network for signals of prospective incidents, which are violations or immediate threats of breaches of computer security rules, acceptable usage regulations, or standard security practises, is known as intrusion detection. An intrusion detection system (IDS) is a piece of software that automates the detection of intrusions. An intrusion prevention system (IPS) is software that performs all of the functions of an intrusion detection system while also attempting to prevent potential occurrences. Many of the same capabilities are provided by IDS and IPS technologies, and administrators may generally disable preventive measures in IPS systems, causing them to behave as IDSs. As a result, for the sake of brevity, the term intrusion detection and prevention systems (IDPS) is used to refer to both IDS and IPS technologies throughout the rest of this chapter.

Machine learning has been utilized to enhance intrusion detection during the previous few decades, and there is now a need for an up-to-date, detailed taxonomy and review of this recent work. There are several studies that use either the KDD-Cup 99 or the DARPA 1999 dataset to verify the creation of IDSs; nonetheless, there is no clear answer to the question of whether data mining approaches are more successful. Second, although being a crucial component in the efficacy of 'on-line' IDSs, the time spent creating IDS is not taken into account in the evaluation of some IDS strategies.

This study presents an up-to-date taxonomy, as well as a review of key research works on IDSs up to the present, as well as a categorization of the suggested systems based on the taxonomy. It gives an organised and complete overview of existing IDSs, allowing a researcher to rapidly become acquainted with the fundamental components of anomaly detection. This study also includes an overview of data-mining techniques used in the development of intrusion detection systems. The signature-based and anomaly-based methodologies (i.e., SIDS and AIDS) are outlined, as well as the strategies utilised in each. The difficulty of various AIDS approaches and their evaluation procedures is reviewed, followed by a series of recommendations identifying the optimal ways based on the type of the incursion.

II. RELATED WORK

In [5], Dash proposes two IDS techniques based on the intrusion detection algorithm for artificial neural networks and metaheuristic algorithms. According to the first technique, the second combined gravitational search with PSO should employ the gravitational search (GS) algorithm. The ANN is trained using the two approaches (GS and GS-PSO). Their effectiveness is confirmed by comparison testing against a number of well-known algorithms, including gradient descent, PSO, and GA.

Additionally, Mayuranathan et al. proposed an enhanced intrusion detection system in [6], where the distributed DoS (DDoS) detection was carried out by implementing the restricted Boltzmann machine classifier, and the feature selection mechanism was optimised by applying the random harmony search algorithm (RHS). The system underwent testing using the KDD'99 datasets, and the results showed a strong performance in terms of detection.

The UNSW-NB15 IDS dataset was used by the authors of [7] to build a filter-based feature-dropping approach utilising the XGBoost algorithm and apply ML algorithms like DT, ANN, KNN, support vector machine (SVM), and LR for accuracy prediction. They verified that the accuracy of binary classification increased from 88.13% to 90.85% using the newly designed approach. Just 90.85% of binary predictions were accurate overall, and 67.57% of multiclass predictions using DT, ANN, LR, KNN, and SVM, respectively.

In [8] authors describes a hybrid model for dimension reduction that combines the IG and PCA approaches with an ensemble classifier built on SVM, instance-based learning algorithms (IBK), and MLP. On the basis of the ISCX 2012, NSL-KDD, and Kyoto 2006+ datasets, the performance was evaluated. The accuracy rate was 98.24% and 99.95% in both NSL-KDD and Kyoto 2006, respectively, and they found the lowest FAR (0.01%), highest DR (99.10%), and lowest accuracy rate (99.01%) in the ISCX 2012 data set.

A feature selection method based on the Firefly algorithm (CFA) and the linear correlation coefficient (FGCC) was developed by [9] to identify network intrusion using the Decision Tree (DT) algorithm. They used the KDDCUP'99 dataset to test their strategy and obtained an accuracy percentage of 95.03%.

A feature reduction approach based on filter-based algorithms like the Input Gain Ratio (IGR), Correlation (CR), and ReliefF was introduced by the authors in [10]. (ReF). It generated feature subsets using an extra Subset Combination Method and the weighted average of each classifier (SCS). For the CIC-IDS2017 dataset, the number of features was reduced from 77 to 24, and for the KDDCUP'99 dataset, from 41 to 12. With the CIC-IDS2017 dataset and the KDDCUP'99 dataset, it provided an accuracy rate of 99.96% in 133.66 seconds with the rule-based classifier Projective Adaptive Resonance Theory (PART), the accuracy rate was 99.32%, and the needed time was 11.22%.

To increase the accuracy of identifying abnormalities caused by intrusions, the authors of [11] designed an IDS system based on MapReduce to obtain a modest and useful number of features from big datasets. In order to categorise normal and aberrant behaviour in mobile cloud computing (MCC) activities, the well-known KDDCUP'99 was employed for performance evaluation. To reduce the size of the training set and parallelize the input data, adaptive effective feature selection (EFS) was employed. They chose 15 features to test the effectiveness of their model, which had an accuracy rate of 93.90%.improving their living conditions and enhancing their livelihood prospects. (Khan, 2022).

III. DIFFERENT TYPES & DETECTION OF INTRUSION

1. Host-Based: Intrusion Detection System Host-based intrusion detection system are designed to monitor, detect, and respond to user system activity and attacks on a given host [12]. Some robust tools offer centralized audit policy management, supply data forensics, statistical analysis and evidentiary support, as well as provide some measure of access control. Host-based intrusion detection is best suited to combat internal threats and abnormal behaviors in the local networks, because of its ability to monitor and respond to specific user actions and file accesses on the host. The greater part of computer threats origin within concerns. Host based IDS relies on the single system and the audit log details are stored in every machine. If attacker takes over a system, then the attacker can tamper with IDS binaries and modify audit logs.

2. Network Intrusion Detection: Network intrusion detection deals with information passing on the wire between hosts, which typically referred to as "packet sniffers". The network IDS devices intercept packets traveling along various communication mediums and protocols [13]. The TCP/IP protocol is usually used. This captures the packets and analysed in a number of approaches. Several Network based Intrusion Detection devices simply compare the packet to a signature database. This verifies whether it contains any known attacks and malicious packet or not. It also verifies the packet and its activity, because that might indicate malicious behaviour of a specified transaction. In either case, NID should be regarded primarily as a boundary resistance. The difference between host-based and network-based intrusion detection is that Network Intrusion Detection (NID) deals with data transmitted from host to host but Host based ID is concerned with what happens on the hosts themselves.

3. Hybrid Intrusion Detection System: Hybrid intrusion detection systems facilitate management and alert notification from both network and host-based intrusion detection devices. Hybrid solutions provide logical complement to NID and HID - central intrusion detection management. Recently, Cisco released a module for their Catalyst 6000 switch that incorporates network intrusion detection directly in the switch, overcoming the first of these flaws. Additionally, ISS (Internet Security System) Network indicated that they are now capable of "packet-sniffing" at gigabit speeds [14].

4. Network-Node Intrusion Detection (NNID): Network-node intrusion detection (NNID) was developed to work around the intrinsic defects in traditional Network IDs. Network-node pulls the packet intercepting technology off of the wire and puts it on the host. With NNID, the "packet-sniffer" is positioned in such a way that it captures packets after they reach their final target or destination system. The received packet at the destination is then analysed just as if it were traveling along the network through a conventional "packet-sniffer". This scheme came from a HID-centric assumption that each critical host would already be taking advantage of host based technology. In this scheme a network-node (NN) is simply another component that can connect to the HID agent. A major disadvantage is that it only evaluates packets addressed to the host on it exists. Traditional network intrusion detection on the other hand monitors packets on the entire subnet. In this case, "Packet-sniffers" are incapable of viewing a complete subnet when the network uses high speed communications, switches or encryption. The advantage of NNID is its ability to defend specific hosts against packet based security issues in these complex environments. This will be very effective where conventional NID is ineffective.

5. Anomaly based IDS: Anomaly based detection systems observes activities that deviate significantly from the established normal usage profiles as possible intrusions. For example, the normal profile of a user may contain the averaged frequencies of some system commands used in their login sessions [15]. This will raise an alarm when the frequencies are differs. So this have follows a continuous monitoring process. The key advantage of anomaly detection is that it does not necessitate preceding information’s or data of intrusion, so it can thus detect new intrusions.

6. Misuse Detection Systems: Misuse detection systems use patterns of well known attacks or feeble spots to find the intrusions. This system matches and identifies known intrusion using the set of patterns. For example, if a user failed to login more than four attempts within a specific time, then it will declare as password guessing attacks. This can be detected using a signature “if”. The main disadvantage is that it lacks the ability to detect the unknown attacks. The concept behind misuse detection schemes is that there are ways to represent attacks in the form of a pattern or a signature so that even variations of the same attack can be detected [16]. This means that these systems are similar to virus detection systems. They can detect many or all known attack patterns, but are of little use for as yet unknown attacks. An interesting point to note is that whereas anomaly detection systems try to detect the complement of bad behaviour, misuse detection systems try to recognize known bad behaviour using the given patterns. The major dilemma in misuse detection systems are how to write a signature that encompasses all possible variations of the pertinent attack, and how to write signatures that do not match non-intrusive activity.

IV. TECHNIQUES OF IDS

1. Supervised learning: In terms of idea, supervised learning can be viewed as a teacher who has environmental knowledge gleaned from input-output examples. The teacher offers advice to the neural network, explaining to it what constitutes normal and aberrant traffic patterns as well as harmful and benign activity.

In its most basic form, supervised learning involves having a teacher assess and identify a segment of a network connection [18]. The learning algorithm then uses the labelled training data to generalise the rules. Last but not least, the classifier employs the created rules to categorise fresh network connections and sends an alert if a connection is deemed dangerous.

2. Unsupervised learning: Unsupervised learning, in contrast to supervised learning, lacks a teacher to determine if a link is "good" or "poor." It has the capacity to automatically construct new classes from unlabeled data and learn from it. How unsupervised learning works is demonstrated using a clustering technique in [19, 20]. The clustering algorithm is used to first cluster the training data. The clustered weight vectors can also be labelled using a specific labelling procedure, for as by choosing a sample group of data from a cluster and labelling the cluster centre with the primary type of the sample. Lastly, the network connections can be categorised using the labelled weight vectors.

3. Genetic Algorithm: Unsupervised search techniques like genetic algorithms are frequently employed for optimisation issues [11]. The ideas of evolution and chromosomal natural selection are the foundation of genetic algorithms. Every chromosome in the original population of the population provides a potential answer to the challenge (an set of parameters). The "goodness" of each chromosome is determined using the evaluation function. Crossover and mutation are the two operators employed in assessment to create the new population or set of rules. Once the optimisation criteria are satisfied, the best person or chromosome is chosen as the outcome.

4. Tree of decisions: It is an additional method for performing characterisation. A classifier that appears as different hierarchical decays of data space is the decision tree [21]. There are two categories of nodes in the tree structure: leaf node (contains the evaluation of the objective quality, for example, normal or malevolent in twofold order assignment), and choice node (contains a condition on one of the properties for space division). Recursively, the decision tree's hierarchical structure divides the information space.

V. CONCLUSION

People are drawn to access the digital network because of the volume of data that is moving through it. Since a few decades ago, researchers have been working in the subject of network security, but vulnerabilities and new types of networks always give intruders a chance to engage in destructive activity. This study compiles the findings of numerous academic studies on attack detection and prevention. The survey revealed that machine learning models outperform traditional detection methods. The report also discussed various intrusion detection system types, along with their benefits and drawbacks. Methods for intrusion detection demonstrate that feature reduction will improve the models' capacity for learning and detection accuracy. Researchers may in the future offer a model that may identify intrusion with minimal effort.

REFERENCES

1. S. Sridevi, R. Prabha, K. N. Reddy, K. M. Monica, G. A. Senthil and M. Razmah, "Network Intrusion Detection System using Supervised Learning based Voting Classifier," 2022 International Conference on Communication, Computing and

Internet of Things (IC3IoT), Chennai, India, 2022, pp. 01-06.

2. Jamal, A. A., Majid, A. A. M., Konev, A., Kosachenko, T., & Shelupanov, A. (2021). A review on security analysis of cyber physical systems using Machine learning. Materials Today: Proceedings.

3. Yong Sik Kim, Moon Kyoung Choi, Sang Min Han, Chanyoung Lee, Poong Hyun Seong. "Development of a method for quantifying relative importance of NPP cyber attack probability variables based on factor analysis and AHP". Annals of Nuclear Energy, Volume 149, 2020.
4. Javed Ashraf, Marwa Keshk, Nour Moustafa, Mohamed Abdel-Basset, Hasnat Khurshid, Asim D. Bakhshi, Reham R. Mostafa, "IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities" Sustainable Cities and Society, Volume 72, 2021,

5. T. Dash, “A study on intrusion detection using neural networks trained with evolutionary algorithms,” Soft Computing, vol. 21, no. 10, pp. 2687–2700, 2017.

6. M. Mayuranathan, M. Murugan, and V. Dhanakoti, “Best features based intrusion detection system by rbm model for detecting ddos in cloud environment,” Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 3, pp. 3609–3619, 2019.

7. [26] Kasongo SM, Sun Y. Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset. Journal of Big Data. 2020;7(1):1-20.

8. [27] Salo F, Nassif AB, Essex A. Dimensionality reduction with IG-PCA and ensemble classifier for network intrusion detection. Computer Networks. 2019;148:164-75.

9. [28] Mohammadi S, Mirvaziri H, Ghazizadeh-Ahsaee M, Karimipour H. Cyber intrusion detection by combined feature selection algorithm. Journal of information security and applications. 2019;44:80-8.

10. [29] Kshirsagar D, Kumar S. An efficient feature reduction method for the detection of DoS attack. ICT Express. 2021.

11. [30] Mugabo E, Zhang QY, Ngaboyindekwe A, Kwizera VdPN, Lumorvie VE. Intrusion Detection Method Based on MapReduce for Evolutionary Feature Selection in Mobile Cloud Computing. International Journal of Network Security. 2021;23(1):106-15.

12. Sandip K. "Host based intrusion detection system. International Conference on Mechanical Engineering and Technology (ICMET-London 2011). ASME Press, 2011.

13. Vigna, Giovanni, Kemmerer RA. NetSTAT: A network-based intrusion detection system." Journal of computer security. 1999; 7(1): 37-71.

14. Ali AM, Zaim AH, Ceylan KG. A hybrid intrusion detection system design for computer network security. Computers & Electrical Engineering. 2009;35(3): 517-526.

15. Garcia-Teodoro, Pedro. Anomaly-based network intrusion detection: Techniques, systems and challenges. computers & security. 2009; 28(1) : 18- 28.

16. Depren, Ozgur. An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks. Expert systems with Applications. 2005; 29(4): 713-722.

17. Shobha Arya1 And Chandrakala Arya, “Malicious Nodes Detection In Mobile Ad Hoc Networks”, Journal of Information and Operations Management, ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, 2012, pp-210-212.
18. R. Vijayanand, D. Devaraj, And B. Kannapiran, ‘’A Novel Intrusion Detection System For Wireless Mesh Network With Hybrid Feature Selection

Technique Based On GA And MI,'' J. Intell. Fuzzy Syst., Vol. 34, No. 3, Pp. 1243–1250, 2018.

19. E. Kabir, J. Hu, H. Wang, And G. Zhuo, ''A Novel Statistical Technique For Intrusion Detection Systems,'' Future Gener. Comput. Syst., Vol. 79, Pp. 303–318, Feb. 2018.
20. E. Kabir, J. Hu, H. Wang, And G. Zhuo, ''A Novel Statistical Technique For Intrusion Detection Systems,'' Future Gener. Comput. Syst., Vol. 79, Pp. 303–318, Feb. 2018. Ban Mohammed Khammas. "Ransomware Detection using Random Forest Technique". ICT Express,Volume 6, Issue 4,2020,