International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 11 Issue 12, December-2022, Impact Factor: 7.957

Intrusion Categories and Methods for Detection of Intrusive Act: A Review

Ankesh Gupta[1], Baldev Singh[2], Nilam Choudhary[3]

[1]Research Scholar, Department of Computer Science & Engineering VGU, Jaipur, Rajasthan, India
[2]Professor, Department of Computer Science & Engineering VGU, Jaipur, Rajasthan, India
[3]Associate Professor, Department of Computer Science & Engineering SKIT, Jaipur, Rajasthan, India

ABSTRACT

In current era, with the rapid progressive technologies the network-based system daily offers naïve assistances to its users. A vast community use open connected channel to transmit data on daily basis. However, with advanced working methodologies the virtual connected system aids its users in a variety of services but such services have also increased the fears for data security, some info may be a general data but some need high sheltering level during the transmission. Over past decades a rich number of approaches has offered by the investigators of related arena to combat the hateful actions against of data/network security but in front of highly sophisticated structure of modern data / network intrusive technologies the standing defensive policies are fails to effectively diagnose such activities. In order to detect signs of security problems at an alone or a network mechanism the applied course of actions is known as an attack / intrusion detection system. This paper exemplifies the classes of Intrusions and the methodologies which has offered by related field research community for recognizing of intrusive activities for helping of naïve researchers to better understand current hitches of this field and to draw the research scope for future investigation.

Keywords: Intrusions, Intrusion Detection System, Machine Learning, , HIDS, NIDS

INTRODUCTION

In current arena rapid increasing number of users utilize network system for sharing data and to complete several personal and/or business activities. However, with progressive methodologies vast community take an advantage of these mechanism on daily basis but with consistently growing number of network-based system connected by the facility of internet has grown the security fear for transits data worldwide. On the other hand, with naïve progressive methodologies the hacker's community regularly made an intrusive attempt to steal transits data by ducking the security constraints like confidentiality, integrity, and/or availability of a separate or a network system, activity is known as an attack action. Confidentiality means that transits material be only accessible for authorized users, integrity depicts the originality of transits data and availability depicts an accessibly of a system/resource at required time frame without degradative act. Intrusive activity may place in a diverse form thus data protection from open channel threats is one most important step in current time. In order to detect signs of security problems at an alone or a network machine the applied course of actions is known as an IDS system. Roughly, the whole attacks activities can be clustered under two groups, major and in minor attack classes which further categorize in two types of attacks [1][2]. Major class of attack that represent two type of attacks, Denial of Services (DoS) and Probe attacks. Minor class attacks which represent further two classes of attacks, Remote to Local(R2L) and User to Root (U2R) attacks [3]-[6], depicted in figure 1.

Denial of Service Attacks (Dos)targeted on available bandwidth or connectivity of networks through overflowing heavy data traffic or desires of connections for stopping lawful data handlers from the utilization of wished services. Typically, these types of attacks not implement for stealing or damage the form of information but such activities are causes of the loss of esteemed time and money for handling such circumstances.

Probe Attacksare implements by attackers to robotically scans network host open ports to halt the accessibility of genuine users to access materials and the facilities of host as well as network. For such activities the attacker community employ wide-ranging practices to fetches open ports over the targeted system or network, activity denoted as Probe Attacks. Ipsweep, Portsweep, Nmap and the Satan is few types of the attacks of this category.

Remote to Local Attacks (R2L)*w*ith implementation of these types of attacks the attacker community try to alter the form of transits data and/or to gain access of system resources even not having an authorize entry on targeted machine. Warezclient, Phf, Ftpwrite, Imap, Warezmaster are few types of attacks related to this category.

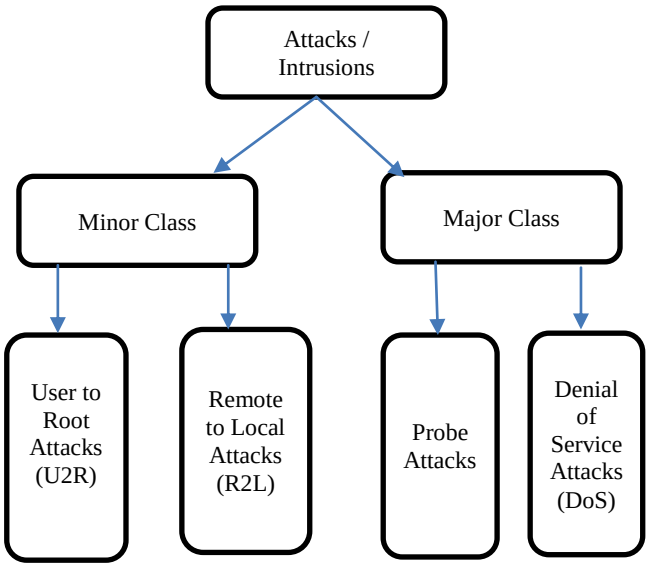

Fig. 1 Types of Attacks over a host or Network System

User to Remote Attacks (U2R), With implementation of these type of attack category an attackers made an attempt to takes the root rights over a sole or of a network through adoption of unlawful action. With such act attacker attain system access consent to fetches important files, exfiltrates through shared requests like mail and/or FTP. Loadmodule, Perl, Buffer Overflow are the few categories of the U2R attacks.

Lot of published efforts denoted that the attacks related to major class i.e Denial of service (DoS) and PROBE attacks can be acknowledgedby an accessible procedure but most of reachable systems has struggle to forecast the attacks that has belong to minor class i.e., Remote to user (R2L) and User to root attacks (U2R).P.Amudha et. al. [7] signified a basic structure of an Intrusion detection system, figure 2.

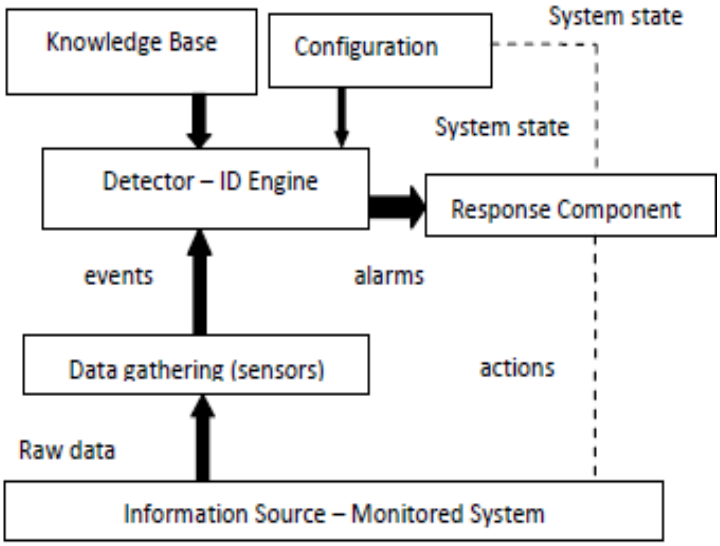

Fig. 2 Elementary Assembly of IDS [7]

Authors of [7] investigational approach has well described the mechanisms of noted architectural framework as

The devices related to ***data gathering*** unit are accountable to assemble statistics from monitored systems. The section of ***Detector – ID*** denoted the progressions of collected data to recognize intrusive act and to beeps an alarm as it fetches such activity. Further ***knowledge base section*** entails pre-processed info offered through the experts of network and composed by the devices. The device unit under section of ***configuration*** offer info over the active stage of intrusion detection system. The components of ***response unit***initiates reaction at the time of recognizing an intrusive act.

CATEGORIZATION OF IDS

The approach to sense security glitches is documented as IDS. Such schemes observe emotive actions of system through the implementing process of solitary functions to discover intrusive activities and to deliver data safety with ensuring

service steadiness of a network. On the bases of diverse parameters like system component for discovery of intrusive act, screening activity, technique responsivity acts an IDS can be roughly groups in few forms, depicted into the figure 3.

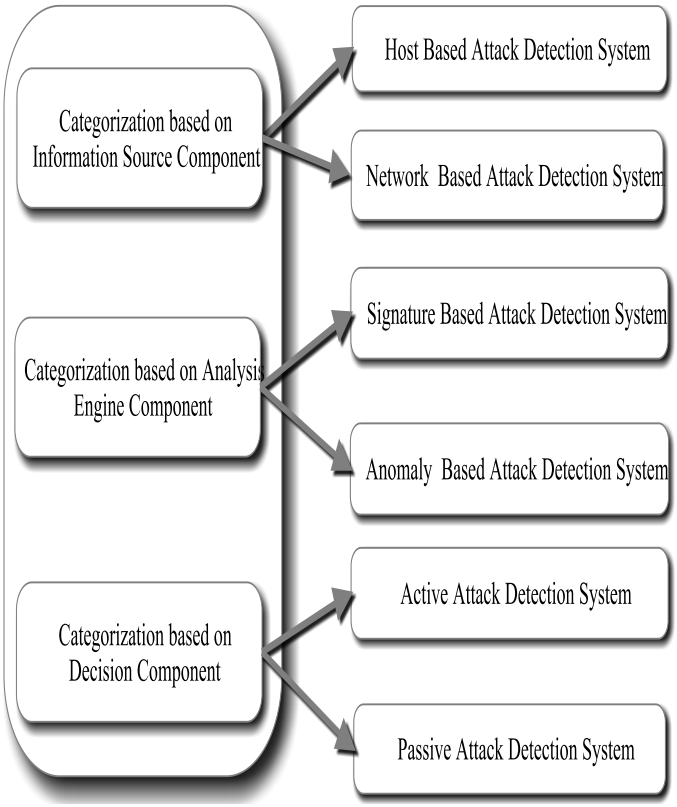

Fig. 3 Categorization of IDS

Host based intrusive discovery system inspect whole machine. Scanned each and every file, log and kernels entries to fetch the presence of intrusive act.Typically, this methodology utilizes differ habits, attain whole facts of system calls and tracks the whole facts. This mechanism denoted much more appropriate material in comparison of NIDS.

The mechanism of ***NIDS*** monitors the traffic of a network rather than an isolated machine. Few times the internal discovery mechanism of machine OS fails to discover intrusive activity due to high volume of data traffic, NIDS mechanism use keen hardware to authenticate network packets in order to discover the existence of any malicious or abnormal activity.

The ***signature base IDS*** is only useful to fetch known attacks. Approaches need for regular training procedure with updated labelled data to gets intrusive act in system. Once the approach has trained with updated signatures of intrusion the methodology professionally detects the intrusive activities in the system.

The **anomaly-based** IDS approaches usage regular statistics which denoted it significance from signature-based attack detection mechanism. It typically involves the creation of knowledge bases that contain the profiles of the monitored activities.

Active IDS approach not have any need of manual configuration; approaches have robotically setup to offer real-time security act. However, approach block attacking act at real time but its placement into the boundary of network is must

Opposite to an act of active IDS the working methodology of **passive IDS** only offered a warn massage to administrator for taking relative act.

RELATED EFFORTS

Since an advent of IDS method in 1980 [8], a vast number of approaches arises to detect, filter and to prevent system from an intrusive activity and to certify services continuity of machine. Table 1, presents the brief overview over the few recent connected works on IDS by adopting various practices.

Table.1. Assistance of ML Techniques in HealthCare

S. NO.	References	Description
1.	M. Mehmood et. al. [9], 2022.	Investigation approach suggest a fresh version of hybrid scheme for recognizing an intrusive act in system through the employment of three phases activity. At initial stage approach do data preprocessing activity through adopting the mechanism of transformation and min-max method. At next phase investigator apply feature selection methodology with scheme of random forest. At further and last phase, they use SVM and Adaptive Neuro-Fuzzy System in hybrid mode to enhance detection rate of attacks. With the simulative fallouts they denoted that proposed approach significantly detect abnormal patterns at a high rate.
2.	Cao B et. al. [10], 2022	With utilization of CNN and GRU practices in an ensemble form this effort has present a naïve hybrid approach for recognizing an intrusive act. Toresolve the positive & negative sample imbalance issues in an original dataset they Utilize ADASYN and RENN schemes for the processing of sample. Select optimal features by an ensemble approach of Random Forest and the PCA. With a diverse simulative effort, they have denoted the significant attained success of their proposed scheme.
3.	Fu Y. et. al. [11], 2022	With the utilization of the models of deep learning the investigators of this efforts have presents a naïve practice DLNID for detecting network anomalies. They utilize CNN method for extracting sequence features of data traffic and Bi-LSTM scheme for the learning process. They use adaptive synthetic sampling (ADASYN) for addressing the issues of data imbalance. To show the significance efforts of presented approach they consider NSL-KDD dataset and denoted that with proposed approach they have achieve 90.73% accuracy and 89.65% F1 score.
4.	M. Ashfaq Khan and Y. Kim [12], 2021	This investigation offers a hybrid intelligent intrusion detection system (HIIDS) to study critical features illustration from enormous unlabeled uncooked network traffic information. They have utilized the functionality of LSTM for recognizing temporal features and the mechanism of AE to identify global features. With simulative fallout they denoted success rate of proposed scheme, accuracyamount up to 97.52%
5.	Li Y. et. al. [13]. 2021	Another hybrid approach on the base of ADASYN (Adaptive Synthetic) and ID3 (Decision tree scheme) has discussed in this paper. Initially implemented approach transformed intrusive data through coding and after that oversampling process has perform though ADASYN algorithm. Furthermore, a decision tree model has built through ID3 approach. Approach attains 93.18% accuracy rate.
6.	J. Dong Lee et. al. [14], 2021	This study offers anew version of intrusion classification architecture identified asM-IDM (Multi-class Classification based Intrusion Detection Model). According to authors of this investigation the proposed approach uses real data through medical devices like monitors (electrocardiogram & thermometers). Simulative fallouts denoted that approach attain 96.7% accuracy level.
7.	Y. S. Sydney and M. Kasongo [15], 2020	With utilization of UNSW-NB15 and AWID IDS dataset this paper discussed a fresh deep learning-based IDS scheme WFEU-FFDNN.
8.	K.E.S.Hadeel Alazzam et.al. [16], 2020	This study proposed a fresh algo for selection of features to recognize intrusive activities with high rate of accuracy. The authors use the functionality of pigeon inspired optimizer to fetch optimal feature set.
9.	U. Ahmad et. al. [17], 2019	Study analyzes the act of classification technology for recognizing of intrusions. With the simulative efforts the authors denoted the advantages of MLP scheme to efficiently fetching intrusive act under irregulate traffic.
10.	A. Hajimirzaei et. al. [18], 2019	For detecting intrusive act this approach utilizes NN and bee colony scheme in a fresh way. For testing phase of approach, they use NSL-KDD dataset. The approach attains 98.41% detection accuracy.

Besides of above efforts several of other investigated efforts [19-23] has also made an attempt to fill the gaps of this filed through attaining naïve high detection rate of intrusive act in system or over a network. Diverse groups of investigators apply different methodologies like utilize sole optimize technique, use the features of two separate algorithm into a combined form and fetch new way to choose optimal feature for recognizing intrusive act efficiently. However, with each approach investigators of this field try to attain a better IDS model but still not a sole approach is capable to outperform with modernization of traffic data and in form of real time solution. Some of the key challenges of IDS scheme are discussed in further section of this paper.

ISSUES WITH PRESENT IDS ALGORITHMS

Over past few years, huge approaches have been projected by the numerous investigators and continuously exclusive thoughts are arises on a daily basis for improving the QoS of present IDS but each one handy method has its own restraints. Among several an operational structure of handy intrusion detection approach is one most issue, most algorithms are built on the base of sole classification algorithm thus face same hitches as the base method face to handle data, main cause of failure in real time scenario. Apart from this issue handy methodologies of IDS have few significant limitations which can be express as

- Utmost practices are not fitsto work speedily with uphold the detection efficiency of intrusive act, especially in high traffic network scenario.
- Required manual updating efforts constantly from operator, without update process approaches fails to maintain its qualitive functionalities.
- Harvests low accurate fallouts with modernization of network parameters and are inflexible.
- Techniques efficiently detect an intrusive sign through which it has been trained but most of time fail to detect new intrusive act which comes with novel signatures.
- Moreover, manipulative cost of the most of handy systems are too high.

However, to improve QoS of IDS algorithms a vast research community of this field has puts their lot of efforts by adopting naïve pattern of implementation but different approach performs differently and often face noteworthy issues to detect intrusive act with maintaining of high accuracy rate. This dilemma of existing systems highly needs the further investigation into this field.

CONCLUSION

In this paper, we discussed about IDS mechanisms, its categories, current efforts of related field investigators and about of contemporary issues of handy IDS algorithms. Typically, for recognizing signs of security issues at standalone or a network machine the applied course of actions is known as an IDS. These schemes rapidly perform screening operation, continuously examine the stirring actions of machine for noticing intrusive activities. With the detailing of IDS its categories have also discussed in this paper to aid new investigator to better understand this mechanism. Several of related field investigating efforts have denoted to show the current activeness of this field for further research. Finally on the base of literature investigation process a number of hitches of current IDS system has also discussed which shows that even after implementation of a vast IDS algorithms this field is still open for the further investigation as each and every offered approach of this field is not able to outperform in real time arena, consist their unique restraints. Such dilemma of existing IDS mechanism denoted that filed is still open for further investigational effort to design and implement a more efficient algorithm of IDS.

REFERENCES

[1]. Tavallaee, M.; Bagheri, E.; Lu,W.; Ghorbani, A.A. A detailed analysis of the KDD CUP 99 data set. In Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, 8–10 July 2009; IEEE: Manhattan, NY, USA, 2009
[2]. Fu, Y.; Du, Y.; Cao, Z.; Li, Q.; Xiang, W. A Deep Learning Model for Network Intrusion Detection with Imbalanced Data. Electronics 2022, 11, 898.
[3]. Anita K. Jones and Robert S. Sielken “Computer System Intrusion Detection A Survey “International Journal of Computer Theory and Engineering, Vol.2, No.6, December, 2010.
[4]. Neelam Sharma, Saurabh Mukherjee, A Novel Multi-Classifier Layered Approach to Improve Minority Attack Detection in IDS, Procedia Technology, Volume 6, 2012, Pages 913-921.
[5]. P. Sharma, S. Saxena and Y. Mohan Sharma, "An Efficient Decision Support Model Based on Ensemble Framework of Data Mining Features Assortment & Classification Process," 2018 3rd International Conference on Communication and Electronics Systems (ICCES), 2018, pp. 487-491,
[6]. Jaiswal, O., Saini, P.K., Shalini, Sharma, Y.M. (2021). Analyze Classification Act of Data Mining Schemes. In: Goyal, D., Gupta, A.K., Piuri, V., Ganzha, M., Paprzycki, M. Second International Conference on Information Management and Machine Intelligence. Lecture Notes in Networks and Systems, vol 166. Springer.
[7]. Arul, Amudha & Subburathinam, Karthik & Sivakumari, S. “Classification Techniques for Intrusion Detection An Overview. International Journal of Computer Applications., 2013, 76. 33-40.
[8]. James P. Anderson. Computer Security Threat Monitoring and Surveillance, 1980. Last accessed: Novmeber 30,2008.
[9]. M. Mehmood, T. Javed, J. Nebhen, S. Abbas, R. Abid et al., "A hybrid approach for network intrusion detection," Computers, Materials & Continua, vol. 70, no.1, pp. 91–107, 2022.
[10]. Cao B, Li C, Song Y, Fan X. Network Intrusion Detection Technology Based on Convolutional Neural Network and BiGRU. Comput Intell Neurosci. 2022 Apr 12;2022:1942847
[11]. Fu Y, Du Y, Cao Z, Li Q, Xiang W. A Deep Learning Model for Network Intrusion Detection with Imbalanced Data. Electronics. 2022; 11(6):898

[12]. M. Ashfaq Khan and Y. Kim, "Deep learning-based hybrid intelligent intrusion detection system," Computers, Materials & Continua, vol. 68, no.1, pp. 671–687, 2021.
[13]. Li Y, Xu W, Li W, Li A, Liu Z. Research on hybrid intrusion detection method based on the ADASYN and ID3 algorithms. Math Biosci Eng. 2021 Jan;19(2):2030-2042.
[14]. J. Dong Lee, H. Soung Cha, S. Rathore and J. Hyuk Park, "M-idm: a multi-classification based intrusion detection model in healthcare iot," Computers, Materials & Continua, vol. 67, no.2, pp. 1537–1553, 2021.
[15]. Y. S. Sydney and M. Kasongo, "A deep learning method with wrapper based feature extraction for wireless intrusion detection system," Computers & Security. Elsevier, vol. 92, pp. 15, 2020.
[16]. K. E. S. Hadeel Alazzam and Ahmad Sharieh, "A feature selection algorithm for intrusion detection system based on pigeon inspired optimizer," Expert Systems with Applications. Elsevier, vol. 148, pp. 113249, 2020.
[17]. U. Ahmad, H. Asim, M. T. Hassan and S. Naseer, "Analysis of classification techniques for intrusion detection," in 2019 Int. Conf. on Innovative Computing, New Delhi, India, IEEE, pp. 1–6, 2019.
[18]. A. Hajimirzaei and N. J. Navimipour, "Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm," ICT Express, vol. 5, no. 1, pp. 56–59, 2019.
[19]. B. Ingre, A. Yadav and A. K. Soni, "Decision tree based intrusion detection system for NSL-KDD dataset," in Int. Conf. on Information and Communication Technology for Intelligent Systems, Springer, pp. 207–218, 2017.
[20]. S. Aljawarneh, M. Aldwairi and M. B. Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," Journal of Computational Science, vol. 25, pp. 152–160, 2018.
[21]. C. Yin, Y. Zhu, J. Fei and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," IEEE Access, vol. 5, pp. 21954–21961, 2017.
[22]. A. M. Yogita Hande, "A survey on intrusion detection system for software defined networks (sdn)," Research Anthology on Artificial Intelligence Applications in Security. IGI Global, vol. 16, no. 1, pp. 20, 2021.
[23]. A. R. Javed, M. O. Beg, M. Asim, T. Baker and Al-Bayatti, "Alphalogger: Detecting motion-based sidechannel attack using smartphone keystrokes," Journal of Ambient Intelligence and Humanized Computing, pp. 1–14, 2020.