WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Hybrid Approach for Network Attacks Detection Based on Artificial Intelligence

[1]Ritika Parmar, [2]Prof. Ankit Mehto

[1 2] Department of Computer Science & Engineering
Bhopal Institute of Technology & Science, Bhopal

ABSTRACT:

During the last decade, the use of web-based apps has skyrocketed. E-banking, e-commerce, online blogs, and social media platforms have all converged into a single platform to share data and offering online services. Although web apps provide fantastic digital experiences, only safe web apps can provide services in a secure manner. Because these apps deal with confidential documents and operations, they are an easy, profitable, and viable target for attackers looking to gain access to secret information, generate financial gain, or engage in a range of illegal acts. The technology based on network is now achieving a huge response in our day to day life routine that may include the usage of mobile phones network, websites usage etc. For these purpose there must be reliability in the networks. In the recent years the number of attacks on the networks is constantly increasing, so this issue arise the need for the intrusion detection system. An Intrusion Detection System is a kind of detecting system which prevents the data in between the middle end from the client side as well as the server side. In the proposed algorithm several effective tools have been used which will surely sense attacks such as port or email scanning activities within the network. This work also explains about the features and applications of the intrusion detection system.

Keywords: Detection Methods, Intrusion Detection, Network Security.

1. INTRODUCTION

Due to the continual growth in the number of online assaults, data protection is already one of the most critical concerns in information security. More than 76 percent of the websites assessed were deemed insecure, according with Internet Security Treat Report (ISTR) 2017 [1-3]. In 60 percent of hacker attacks, web apps were either targeted or exploited as attack vectors, compared to one study. Including the most recent Verizon statistics [4], monetary gain motivates 95 percent of online application breaches. Furthermore, the number of browser security breaches increased by 35% during first quarter of comparison to the previous year, according to the research [5.] To ensure web application security, organizations have used a variety of protective measures. The most well-known security solution used by organizations to secure web applications after they have been launched is the Online Application Firewall (WAF) [6]. WAF checks web requests before sending them to the web application and stops them if they are judged risky. However, because it is a broad solution based on rules and guards against much more attack sequences, it is unable to grasp the context of unique web apps. Configuring WAF is like to creating an alarm system for a building without taking the layout into consideration. As a possible solution, intrusion detection systems (IDS) are developed primarily to secure online operations.

An intrusion detection system (IDS) is a security sensor that monitors and notifies the administration of intrusions. The Intrusion Prevention System (IPS) is an extension of a Intrusion Detection System (IDS) that can detect and, if required, stop assaults. IPS is similar to WAF in that it examines all traffic data to identify attacks. These solutions are more dynamic than WAF though they can detect known risks and identify aberrant activity using both signature and anomaly-based methodologies. They may learn about the complex ecology of a web - based application, including how stored procedures works, who the customers are, and also how they engage with the programme. In the realm of application online security, intrusion detection methodology is still very much in infancy. The most typical application of IDS is to monitor and detect malicious network operations [7]. Network-based attacks, on the other hand, have distinct characteristics from internet attacks. The first deals with the network layer, whereas for second deals with the application level. Second, today's online applications are complicated, data system, and frequently created by developers who lack adequate security skills. These apps are appropriate and relevant, capable of delivering dynamic information, facilitating engaging user experiences, and completing complicated corporate activities [8]. The threat landscape for all these apps varies depending on the company logic and skill set utilised to create them. As a result, establishing an IDS to identify suspicious behaviour on a website differs significantly from building an IDS to monitor network traffic. The aim of this assignment is to completely comprehend and outline the design strategy for a web traffic monitoring detection system. In this article, we look at a few different aspects of online applications and their traffic that might make designing a web IDS difficult, as well as how they impact IDS architecture. It would be tremendously helpful to programmers in creating a web IDS architecture that works.

"Intrusion Detection System Vs Intrusion Prevention System"

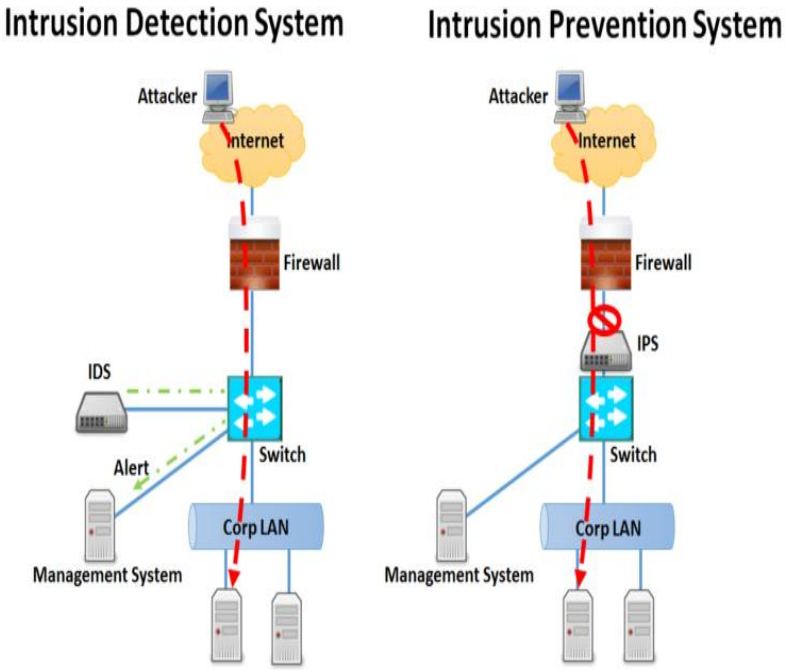

Figure 1: IDS vc IPS.

2. LITERATURE REVIEW

The functioning, key traits, and shortcomings of the previously outlined techniques offered by diverse writers are examined in this chapter.

Al-Jarrah et al. [1] introduced a traffic-based intrusion detection system (TIDS) for botnets, which are made composed of a sequence of infected computers called as bots that are administered remotely by a bot supervisor workstations. The suggested technique identifies infiltration by analysing the incoming packets instead of the packet payload that used a novel randomised data partitioned learning method (RDPLM). The authors devised an unique feature selection technique to provide a set of features that may be used to enhance intrusion detection. The approach has been shown to increase detection capability while reducing operational costs, and it is scalable to large scale networks.

Buczak and Guven [4] looked at neural network models for intrusion detection in term of algorithm complexity as well as enhanced security problems. The authors proposed many criteria for choosing the most effective intrusion detection system, including accuracy, algorithm complication, and time complexity.

Khor et al. [5] suggested a cascaded classifier intrusion detection system that improves intrusion detection capability for unusual intrusions. The proposed method first differentiates amongst uncommon and non-rare incursions, allowing each expert to concentrate on lesser subcategories. The strategy helps to reduce the impact of the most common incursion category, resulting in higher detection rates for unusual intrusions. Furthermore, double data transmission filtration enhances detection rates while lowering the processing cost of the strategy.

To increase the effectiveness of such an intrusion detection system, Aburomman & Ibne Reaz [6] devised an unique classifier ensemble approach. The writers used the suggested PSO generated weights scheme to form an ensemble and compared with the results to the Weighted Majority Algorithm (WMA). IDS performance has improved as a consequence of LUS meta optimisation of the collection of produced values.

Qassim et al. [7] looked at the characteristics that are best for identifying a variety of abnormalities in communication networks. The alarm classifier developed by the authors, A-IDS, can automatically assess as well as categorise anomalies found by a packet header-based anomaly detection system. The proposed technique analyses network flow of traffic, finds appropriate properties, and analyzes attack incoming traffic to historical data.

Govindarajan [8] presented a new hybrid intrusion detection method that integrates the radial basis function with the svm classifier. Experimenting with various intrusion detection data sets has shown that mixed model performs better homogeneity models.

Liu et al. [9] created SmoteAdaNL, a hybrid strategy that combines oversampling to enhance the quantity of flows in the marginalised group and then a diversified ensemble methodology to improve classifier generalisation. Miscategorized flows are given weights to assist improve classification results.

Marteau [11] proposed a novel similarity metric for symbolic sequential data in order to identify unanticipated threats. The researcher utilized the Sequence Covering technique for Intrusion Detection to focus on system call patterns in the suggested method (SC4ID). The SC4ID technique works by filling a string with a succession of substrings taken from a specified pool of sequences in even the most efficient way possible. SC4ID was tested on the well-known UNM and ADFA-LD invocation datasets.

Virtual Machine Introspection were developed by Mishra et al. [12] for fine-grained monitoring of VMs to identify assaults. In able to detect risks, the authors developed techniques for monitoring and analysing Tenant Virtual Machines (TVM) at the system and process call levels. The proposed framework has discovered rogue hidden processes, assaults that deactivate security mechanisms in the virtual machine, as well as attacks that modify the behaviour of legitimate processes to get access to sensitive information. The authors used the VMM-introspection layer's feature to identify and

select features in their proposed architecture, dubbed VMGuard. The authors then employed the Random Forest classifier to identify a common behaviour for different forms of TVM incursions, using the Bag of N-grams approach in combination with the Term Frequency-Inverse Document Frequency strategy.

Sklavounos et al. [13] introduced a new NIDS approach for DOS detecting attacks relying on the tabular cumulative sum (CUSUM) chart and the exponential weighting moving average (EWMA) chart, that they deployed to the NSL-UDP KDD's and ICMP source bytes in the testing dataset.

Suad Othman et al. [14] presented an intrusion detection model for a big data environment that uses a machine learning method known as SVM for classification and a characteristic selection strategy known as Chi-selector for feature extraction to minimise dimension in network traffic. To put the proposed approach to the test, the KDD datasets was employed.

The first PIDS-based IDS for identifying attack patterns in a LoRaWAN network was suggested by Danish et al. [15]. The system was built using the LoRaWAN protocol.

J. Arshad et al. [16] suggested a collaborative ID design for M2M-based IoT that depends on collaboration among IoT nodes to offer effective ID with minimal transmission, computation, and energy consumption. The suggested framework argued that data both from HIDS as well as NIDS should be used. The suggested paradigm intends to handle issues such as M2M effectiveness, node resource limits, and collaboration nature.

Subba et al. [17] devised a method for enhancing the efficiency of HIDS computation. After converting the system call to an n-gram vector, the suggested technique employs dimensionality reduction to shrink the input relevant features. Finally, a variety of machine learning techniques are used to assess the feature vectors to identify intrusive processes (Naive Bayes, MLP, C4.5 Decision Tree, and SVM). Using the ADFA-LD benchmarks, the proposed model was evaluated.

Parvat et al. [18] advocated the use of deep learning-based NIDS. A divide and conquer methodology was employed in the suggested method to combine several classifier model from a deep learning model.Using the NSL-KDD dataset, the system was assessed.

Devi et al. [19] utilised the Dynamic Neuro-Fuzzy Inference System to the information security of 5G wireless connectivity network infrastructure of IDS and used the KDD cup 99 data set for system testing.

Kolias et al. suggested a decentralized intrusion detection systems for wireless networks in Kolias et al. [20]. (IDS). To analyse the data for intrusion detection, the system employs classification rule induction as well as swarm intelligence theories. The suggested strategy was tested on the second version of the Aegean wireless incursion dataset.

Game theory was utilised by Gupta et al. [21] to detect and assess capacity malicious activities on 5G wireless small cell access points. The scientists also suggested an adaptable intrusion detection system that concentrated on the security problems of 5G wireless networks and employed a hidden Markov Model to identify an incursion.

Peter [22] created and tested a set of distributed IDS algorithms for the Internet of Things that are suitable for tiny devices. The researchers utilised a trust management strategy that enables devices to deal with neighbour reputation data. In a processing and energy-efficient manner, the suggested technique discovered maliciously behaving units.

Table 1: Comparative of selected literature work.

The work	**Year Published**	**IDS type**	**Platform**	**Data source**	**Attack type that detected**
[11]	2018	HIDS	Host	System call	Unknown attack
[12]	2018	VMI-IDS	VM	Process and system call	Abnormal hidden processes. Attacks that debilitate security facilities. Attacks that alter the behavior of the authentic processes.
[13]	2018	NIDS	Network	UDP and ICMP source bytes	DOS attack.
[14]	2018	NIDS	Network	Network traffic	Not specific.
[15]	2018	PIDS	Network	Real time network traffic	Jamming attacks.
[16]	2018	CIDS	Host and Network	Data collective from host and network	Not specific.
[17]	2017	HIDS	Host	System call	Intrusive process.
[18]	2017	NIDS	Network	Network traffic	DOS, Probe, R2L, U2R.
[19]	2017	WIDS	Network	Network traffic	Land, Neptune, pod, Smurf, Tear drop.
[20]	2017	WIDS	Network	Wireless traffic	Intrusive traces from a wireless.
[20]	2017	WIDS	Network	Wireless traffic	Spoofing attack.
[21]	2017	DIDS	Host and Network	Network traffic	Attacks that try to fail communication between nodes.

The strategies discussed above have aided in correctly identifying intrusions in IDS, hence improving IDS security.

3. PROBLEM STATEMENT

The market of the intrusion detection system is not new, but seems to be in use around 20 years. After so many years the problems is not change even an inch because of adapting new technologies which makes it easy to get into any of the system as well as network for their sake. Some of the intrusion detection system also provides an alert but most of them does not provide accurate alerts and gives false alerts and they are of no use and importance as well. For example a general intrusion detection system will generate around 10k alerts. So, the management of several alerts is not manageable for the human analyst.

4. PROPOSED FRAMEWORK

In this work the explanation of several outlier detection techniques used, the used algorithms are negative selection as well as architecture of the neural network.

Hybrid approachGA-ANN (***Genetic Algorithm with Artificial Neural Network***) is presented in proposed work. The following are the steps taken for execution purpose in proposed work.

Step 1- In the first step the dataset will be loaded from the databases, also essential libraries will get load into it.

Step 2- The data which is obtained from the internet resources will be preprocessed.

Step 3- The proposed approach which is negative selection onto this the protocol classification will applied on the refined data in order to provide outputs in less time as well as the further classification will based on the given feature.

Step 4- Classification algorithm

Artificial neural network classification will be applied on the knowledge extraction on the basis of the negative selection algorithm.

In the final step the classified intrusion and non-intrusion data is mentioned on the final classification step.

4.1 Testing Datase For Proposed Framework

Because of the presence of the huge amount of training data records present in the 10% KDD'99 data sets, this model is evaluated on the subsets of 10% KDD dataset. The labeled datasets will have only one feature which represents that it is normal or not (a type of an attack).

There are certain type of attacks discussed below:

Back Attack: It comes in the DOS class. This attack work in opposition of the apache web server. It will have a bunch of requests which contains large number of front-slash (/) characters in the URL portrayal. As the server attempts to process every one of these solicitations, it winds up unfit to process other genuine solicitations and thus it refuses assistance to its clients.

Guess_Passwd Attack: Guess_passwd assault goes under R2L class. Guess_passwd assault is that the assailant attempts to access a client's record by over and over speculating the potential passwords. Any administration that requirements secret key to get to perhaps turns into an assaulted objective.

Ipsweep Attack: IPSweep assault goes under Probe class. IPSweep assault figures out which hosts are tuning in on system through an observation clear. It decides the running host and its administration types, and after that the gathered data can be utilized by assailants in arranging assaults and looking for defenseless PCs [17].

Neptune Attack: Neptune assault goes under DOS class Neptune assaults can make memory assets unreasonably full for an injured individual by sending a TCP bundle mentioning to start a TCP session. This parcel is a piece of a three-way handshake that is expected to set up a TCP association between two hosts. The SYN banner on this parcel is set to show that another association is to be set up. This parcel incorporates a caricature source address, to such an extent that the injured individual can't complete the handshake however had dispensed a measure of framework memory for this association. Subsequent to sending a significant number of these parcels, the injured individual inevitably comes up short on memory assets [18].

Unit Attack: POD assault goes under DOS class. Ping of death is brought about by an assailant sending a ping bundle bigger than the 65,535 bytes (ordinarily 64 bytes). Numerous PC frameworks can't deal with an IP bundle bigger than the greatest IP parcel size of 65,535, and regularly causes PC frameworks crash. It is illicit to send a ping parcel of size more prominent than 65,535, however a bundle of such size can be sent on the off chance that it is divided. At the point when a getting PC reassembles the parcel, a support flood happens, which regularly makes PC crash.

Smurf Attack: The Smurf Attack is a refusal of-administration assault in which huge quantities of ICMP bundles with the proposed injured individual's ridiculed source IP are communicated to a PC system utilizing an IP Broadcast address. This makes all hosts on the system answer to the ICMP demand, making huge traffic the unfortunate casualty's PC. For instance, on the off chance that there are n hosts associated with a system, at that point aggressor can make the whole host to send n answer bundle to the unfortunate casualty by sending a solitary parcel to organize.

Tear Attack: Teardrop assault goes under DOS class. Tear assault abuses by sending IP part parcels that are hard to reassemble. Ordinarily, a section parcel recognizes a balance that is utilized to amass the whole bundle to be reassembled by the getting framework. In the tear assault, the aggressor's IP puts a confounding balance an incentive in the resulting sections and if the accepting framework doesn't have the foggiest idea how to deal with such circumstance, it might make the framework crash.

5. COMPARISON PARAMETER

The experimental findings show that our IDS can detect abnormalities with a high level of accuracy and detection rate. The experiment findings are compared to the traditional approach to determine its optional result. The comparison with the recommended approach demonstrates the efficacy of the proposed effort. The computation parameters are discussed here, as well as the observed outcome.

1) Accuracy Evaluation:

When an intrusion is appropriately indicated, True Positive fact. If no attack has been discovered, we have a True Negative. If IDS detect an intrusion but this claim is incorrect, a False Positive warning is produced. At the conclusion, the non-intruder is discovered, and the intruder is truly in process, resulting in a False Negative (FN) occurrence. False Negative is the worst case scenario in which the procedure of all detection scenarios results in an incorrect alarm. Given these parameters, we evaluated our intrusion detection system (IDS) by calculating the accuracy value and the detection rate. Accuracy (ACC) is defined as the total number of outcomes divided by the number of intrusions.

$$ACC = \frac{TP + TN}{TP + FP + FN + TN}$$

1) Detection Rate:

On the other hand, the detection rate (DR) is the possibility that finds out the real intrusions from the given alarm.

$$DR = \frac{TP}{TP + FN}$$

2) Statistical Analysis:

According to the aforementioned definitions, the results of our experiments are summarized in Table 1 the experimental results indicate that our IDS can detect anomalies with relative accuracy and detection rate.

Precision = TP/ (TP+FP)

Recall = TP/ (TP+FN)

F-Measure=2*((Precision*Recall)/(Precision+ Recall))

Table 2: Result Analysis Algorithms

Algorithms	**Accuracy**	**Detection Rate**	**Precision**	**Recall**
K- Means	69.81	65.29	64.29	65.29
GA-ANN	94.06	98.12	93.23	94.72
SVM	71.08	66.50	65.50	66.50
NB	75.06	81.52	80.52	81.52

In the table given above shows the difference analysis between the algorithms.

Graphical Comparison Analysis:

In this section an analysis of result is presented, the section gives an understanding of statistical graphical analysis.

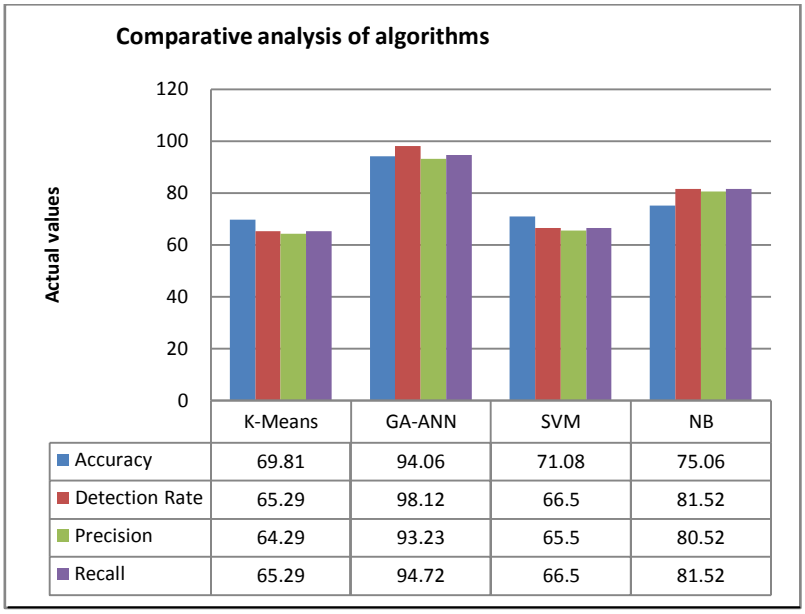

Figure 5.1: Comparison between the analyses of the algorithms.

In this section, previous approach and proposed approach result comparison is performed, as per the monitored results from implementation which is obtained is compared.

6. CONCLUSION

This work focuses on the identification of intrusion detection techniques. This provides a comprehensive review of intrusion detection systems, as well as attackers and detection technologies. Because the scope of IDS is not constrained and appears to change on a regular basis. The intrusion detection system (IPS) defines the security measures that are implemented. Even with the presence of the lifespan phase and the steps outlined, there are still hurdles to overcome. The anomaly detection and misuse detection strategies are reviewed, as well as alternative techniques that can be applied. The suggested study uses chosen ways to improve data mining algorithms as well as IDS. The suggested approach GA-ANN demonstrates efficiency in parameter-based results. In future studies, the technique's operation with mobile devices can be considered.

6.1 Future Work

The next study will encompass improved enhancements to the outliers detection technique, as well as the implementation of the technique on the network and the situation in which data packets and network routing will be used. In the future, the IDS might potentially be included in a mobile ad-hoc network. We can also change the decision tree classification model with any other model, as well as the classification accuracy using the presented work.

REFERENCES

[1]. O. Y. Al-Jarrah, O. Alhussein, P. D. Yoo, S. Muhaidat, K. Taha, and K. Kim, Data randomization and cluster-based partitioning for botnet intrusion detection, IEEE Transactions on Cybernetics, vol. 46, no. 8, pp. 1796–1806, 2016.
[2]. K. Kumar and S. Singh, Intrusion Detection Using Soft Computing Techniques, 2016.
[3]. S. Rajasegarar, C. Leckie, J. C. Bezdek, and M. Palaniswami, Centered hyperspherical and hyperellipsoidal one-class support vector machines for anomaly detection in sensor networks, IEEE Transactions on Information Forensics and Security, vol. 5, no. 3, pp. 518–533, 2010.
[4]. A. L. Buczak and E. Guven, A survey of data mining and machine learning methods for cyber security intrusion detection, IEEE Communications Surveys and Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.
[5]. K.-C. Khor, C.-Y. Ting, and S. Phon-Amnuaisuk, A cascaded classifier approach for improving detection rates on rare attack categories in network intrusion detection, Applied Intelligence, vol. 36, no. 2, pp. 320–329, 2012.
[6]. A. A. Aburomman and M. B. Ibne Reaz, A novel SVM-kNNPSO ensemble method for intrusion detection system, Applied Soft Computing Journal, vol. 38, pp. 360–372, 2016.
[7]. Q. S. Qassim, A. M. Zin, and M. J. Ab Aziz, Anomalies classification approach for network—based intrusion detection system, International Journal of Network Security, pp. 1159–1171, 2016.

[8]. M. Govindarajan, Evaluation of ensemble classifiers for intrusion detection, World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, vol. 10, no. 6, pp. 876–884, 2016.
[9]. Z. Liu, R. Wang, and M. Tao, SmoteAdaNL: a learning method for network traffic classification, Journal of Ambient Intelligence and Humanized Computing, vol. 7, no. 1, pp. 121–130, 2016.
[10]. W. Hu, J. Gao, Y. Wang, O. Wu, and S. Maybank, Online adaboost-based parameterized methods for dynamic distributed network intrusion detection, IEEE Transactions on Cybernetics, vol. 44, no. 1, pp. 66–82, 2014.Beghdad R., Critical study of neural network in detecting intrusions, Elsevier, Computers and Security, Vol. 27, pp. 168-175, 2008.
[11]. Marteau, P.-F., Sequence covering forefficient host-based intrusion detection. IEEE Transactions on Information Forensics and Security, 2018.
[12]. Mishra, P., et al., VMGuard: A VMI-based Security Architecture for Intrusion Detection in Cloud Environment. IEEETransactions on Cloud Computing, 2018.
[13]. Sklavounos, D., A. Edoh, and G. Paraskevopoulos, Utilization of Statistical Control Charts for DoS Network Intrusion Detection. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 2018. 7(2): p. 166-174.
[14]. Othman, S.M., et al., Intrusion detectionmodel using machine learning algorithm on Big Data environment. Journal of BigData, 2018. **5**(1): p. 34.
[15]. Danish, S.M., et al. Network IntrusionDetection System for Jamming Attack in LoRaWAN Join Procedure. in 2018 IEEEInternational Conference on Communications (ICC). 2018. IEEE.
[16]. Arshad, J., et al., A novel framework for collaborative intrusion detection for M2M networks. International Conference on Information and Communication Systems (ICICS), IEEE, 2018.
[17]. Subba, B., S. Biswas, and S. Karmakar. Host based intrusion detection system using frequency analysis of n-gram terms. in Region 10 Conference, TENCON 2017-2017 IEEE. 2017. IEEE.
[18]. Parvat, A., et al. Network IntrusionDetection System Using Ensemble of Binary Deep Learning Classifiers. in International Conference on Smart Trends for Information Technology andComputer Communications. 2017.Springer.
[19]. Devi, R., et al., Implementation ofintrusion detection system using adaptive neuro-fuzzy inference system for 5G wireless communication network. AEU-International Journal of Electronics and Communications, 2017. **74**: p. 94-106.
[20]. Kolias, C., V. Kolias, and G. Kambourakis, TermID: a distributedswarm intelligence-based approach for wireless intrusion detection. InternationalJournal of Information Security, 2017. **16**(4): p. 401-416.
[21]. Gupta, A., R.K. Jha, and S. Jain, Attackmodeling and intrusion detection system for 5G wireless communication network. International Journal of Communication Systems, 2017. **30**(10): p. e3237.
[22]. Deepak, K., et al. Distributed IntrusionDetection System for TCP Flood Attack.inProceedingofInternationalConference on Intelligent Communication, Control and Devices.2017. Singapore: Springer Singapore.
Khan, Z.A. and P. Herrmann. A trustbased distributed intrusion detection mechanism for internet of things. in Advanced Information Networking and Applications (AINA), 2017 IEEE 31st International Conference on. 2017. IEEE.
[23]. Siraj M. M., Maarof M. A., Hashim S.Z.M., Intelligent Alert Clustering Model for Network Intrusion Analysis, International J. Advance Soft Comput. Appl. Vol. 1(1), pp. 33-48, 2009.
[24]. Hlaing T., Feature Selection and Fuzzy Decision Tree for network Intrusion Detection, International journal of Informatics and Communicational Technology, Vol. 1(2), pp. 109-118, 2012.
[25]. Kim D. S., Nguyen H., Park J. S., Genetic Algorithm to Improve SVM Based Network Intrusion Detection System, Proceedings of the 19th International Conference on Advance Information Networking and Applications, Vol. 2, pp. 155-158, 2005.
[26]. http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/1998data.html
[27]. kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
[28]. Ghorbani A. A., Lu w., Tavallaee M., Network Intrusion Detection and Prevention, Springer Science + Business Media, LLC 2010.
[29]. Labib K., Vemuri V. R., Detection and Visualizing Denial-of-Service And Network Probe Attacks Using Principal Component Analysis, Third Conference on Security and Network Architecture, SAR'04, June 2004.
[30]. Veerabhadrappa, L. Rangarajan,Multi-level Dimensionality Reduction Methods using Feature Selection and Feature Extraction, IJAIA, Vol.1, No.4, October 2010.
[31]. Daza L., Acuna E., Feature Selection based on a data quality measure, proceedings of the world congress on Engineering, Vol. II, 2008.
[32]. Witten I. H., Frank E., Data Mining : Practical Machine Learning Tools and Techniques, Elsevier, Morgan Kaufmann Publishers, 2005.
[33]. Ayman Taha#1, Osman M. Hegazy, A Proposed Outliers Identification Algorithm for Categorical Data Sets.
[34]. Dewan Md. Farid, Mohammad Zahidur Rahman, Anomaly Network Intrusion Detection Based on Improved Self Adaptive Bayesian Algorithm journal of computers, vol. 5, no. 1, january 2010.
[35]. Zengyou He1, Xiaofei Xu1, Joshua Zhexue Huang2, Shengchun Deng, FP-Outlier: Frequent Pattern Based Outlier Detection 2011.
[36]. Agusti Solanas a,1, Enrique Romero b,2, Sergio Gómez, Feature Selection and Outliers Detection with Genetic Algorithms and Neural Networks.
[37]. A. Koufakou1 E.G. Ortiz1 M. Georgiopoulos1 G.C. Anagnostopoulos2 K.M. Reynolds,A Scalable and Efficient Outlier Detection Strategy for Categorical Data 19th IEEE International Conference on Tools with Artificial Intelligence.
[38]. Hans-Peter Kriegel, Peer Kröger, Erich Schubert, Arthur zimeck, Outlier Detection in Arbitrarily Oriented Subspaces, 2012 IEEE 12th International Conference on Data Mining.
[39]. Ozlem GURUNLU ALMA 1♠, Serdar KURT, Aybars UĞUR, Genetic Algorithm Based Outlier Detection Using Bayesian Information Criterion in Multiple Regression Models Having Multicollinearity Problems, G.U. Journal of Science 22(3): 141-148 (2009)
[40]. Ayman Taha#1, Osman M. Hegazy, A Proposed Outliers Identification Algorithm for Categorical Data Sets.
[41]. Ayman Taha, Ali S Hadi, A General Approach for Automating Outliers Identification in Categorical Data 2013 IEEE.
[42]. A. Zimek, E. Schubert, and H.-P. Kriegel, A survey on unsupervised outlier detection in high-dimensional, Statistical Analysis and Data Mining, vol. 5, no. 5, pp. 363–387, 2012.
[43]. H. Dai, F. Zhu, E.-P. Lim, and H. H. Pang, Detecting extreme rank anomalous collections, in Proceedings of the SIAM (SDM), pp. 883–894, 2012.