IJASRM

International Journal of Advanced Scientific Research and Management, Volume 4 Issue 6, June 2019

www.ijasrm.com

ISSN 2455-6378

Intrusion Detection Analytics: A Comprehensive Survey

Nerella Sameera and M. Shashi

Dept. of CS & SE, Andhra University College of Engineering(A),
Andhra University, Visakhapatnam, AP, INDIA

Abstract

Cyber threat is growing on par with the advancements in the field of computer technology and information age which makes Intrusion detection Systems (IDSs) to get a lot of attention now a days. IDS is an evolving research area in the field of cyber security, which is aimed to detect cyber-intrusions. The authors have surveyed many research papers on IDS in the resent past and the essence of their survey is presented in this paper by keeping in thought of helping research scholars in the area of IDS. This paper aims at presenting brief description of IDS and machine learning approach for its implementation. Though lot of literature survey on IDS exist, in this paper authors attempt to present a clear picture of IDS in all aspects through their extensive survey.

Keywords: *Intrusion, Machine Learning, NSL-KDD, Feature Reduction, Feature Extraction, Transfer Learning.*

1. Introduction

As the world is technically growing, maintaining security is a challenging issue. In order to grab the customers attention, many multinational companies relay on new technologies like cloud and mobile computing. Sometimes there may be a biggest betrayal behind these facilities. According to the resent survey carried out by an international company FROST & SULLIVAN [1], there will be a biggest cyber threat to many corporate companies in near future which leads to their financial disaster. According to this survey, any corporate company facing a cyber-challenge has to afford crores of dollars for it. This survey also elevates that for the coming five years there may be a loss of 370 lakh crores because of these cyber threats. Other than financial loss, these cyber-attacks may also lead to the loss of brand value and customer support. This problem does not belong to a specific company or to the specific country, it is a worldwide cyber issue. So, countries worldwide need to cooperate with each other to fight against this issue. Stock market, Chemical companies, Communication technologies, Retail market, Banking services, Media, Tourism, Consumer goods, etc. are the companies most effected by the cyber-attacks. Therefore, it is necessary to get insights into the concepts of security defense mechanisms and various techniques and trending topics in the area of information security [2].

Cyber-intrusion or cyber-attack is formally defined as any unauthorized activity of illegally penetrating into the cyber system by violating its security premises. Virus, Worms, Trojans, Rootkit, Spyware, etc. are different types of basic cyber-intrusions [3]. All these are the types of malware. Both viruses and worms are the malicious programs which usually enter into the system through malicious links or by downloading malicious email attachments, etc. Trojans are malicious software hidden under a legitimate host. Rootkit is an attack on retrieving root privileges of a victim. Spyware is a malicious software that stays across the computer system and records all the important information like number of bytes in, bytes out, internet usage data, user's personal information etc. without their knowledge.

There are four major attack categories. These are Denial of Service (DoS) attack, probing attack, Remote to Local (R2L) attack and User to Root (U2R) attack. In DoS attacks, attacker disrupts the legitimate user by sending overwhelming resource requests to the server. Probing is an attack in which attacker monitors the victim's systems for identifying vulnerability points for future exploitation. In Remote to User (R2U) attack, the attacker attacks the victim's system from a remote location and exploits vulnerabilities and finally gains the credentials of the authorized user. In User to Root (U2R) attack, first attacker enters the system as a legitimate user and later gains access to the administrator. Some other cyber-attacks are web-based attacks, DNS attacks, etc. SQL Injection and Cross site scripting are examples of web-based attacks. In SQL injection erroneous data is inserted into a website by exploiting vulnerability of a query or command. In cross site scripting, attacker inserts malicious scripts into the web pages. In DNS attacks attacker redirects the domain name to some malicious IP address.

Existing security measures like firewalls are no longer sufficient to deal with these emerging attacks. Because firewall only checks header of the data packet, it doesn't go through the content or details of the packet. IDSs are the systems introduced as a second line of security after firewalls, to handle cyber intrusions more efficiently. IDSs can go through the entire details of the packet to detect intrusions. After detection IDS alerts the system administrator for taking up further actions. This paper provides brief overview of IDS and various approaches for dealing with IDS. This paper also presents different IDS implementation techniques suggested by many researchers during the year 2014 to 18. Challenges and future enhancements are also suggested at the end of the paper.

The remaining part of the paper is organized as follows: Section 2 presents description of IDS, Section 3 gives machine learning approach to IDS, Section 4 discusses about bench mark datasets for implementation of IDS, Section 5 presents the details of existing research and finally conclusion is mentioned at Section 6.

2. Intrusion Detection Systems

Intrusion Detection System (IDS) is a software or hardware system that monitors a single computer or a network of computers for detecting malicious activity and accordingly IDSs are classified into Host based IDS (HIDS) and Network based IDS (NIDS) respectively [5]. On detecting the intrusion, IDS raise an alert (alarm) to the system administrator to take an appropriate action. HIDS aims at monitoring the behavior of a single host for detecting intrusions, whereas NIDS monitors the activities of the entire in-ward and out-ward traffic in the network, etc. Irrespective of the type, IDS follow two detection approaches. One is signature-based or misuse-based detection and the other is anomaly-based detection. Signature based attack detection methods are supervised methods requiring abundant labeled examples for formation of signatures for known attacks and compares each incoming packet signature with the learned signature patterns. So, this approach can only detect attacks to which a patch is already prepared. It is unable to detect zero-day attacks for which no patch exists. Anomaly based detection approach detects intrusions by observing the deviations of the packet's signature with the normal behavior. The packet which is deviated from the normal behavior is treated as attack. In this way anomaly-based approach is able to detect zero-day attacks but results in high false positive rates (FPR) because deviation from normal behavior may not always leads to attack. There exists another detection approach called hybrid approach [31], [36] which combined the two approaches. With hybrid IDS, first, known attacks are detected and separated by matching with the attack signatures and then among the remaining stream the unknown attacks are detected by observing deviations of such packet features from those of the normal packets.

3. Machine Learning Approach to IDS

Among various approaches for implementation of IDS Machine learning approach best suit for IDS as IDS needs to analyze extensive amounts of data. Machine learning offers many algorithms which can analyze huge amount of data and helps IDS in taking better decisions. Machine learning algorithms are broadly categorized as supervised and Unsupervised methods. Supervised methods predict class labels of entities based on the knowledge learnt from large collection of labeled data. Whenever labeled data is not available unsupervised methods like clustering are used as they do not require labeled data for pattern/ feature extraction. Since IDS needs to maintains labeled data related to known attacks and genuine traffic packets (benign), supervised methods are mostly preferred for the construction of IDS. K-NN [9], DT [25], Naïve Bayes [12], SVM [21], RF [30], NN [26], etc. are mostly used by many researchers for the construction of IDS. Along with this stand-alone approach of using a single classifier for IDS, there exist two other approaches for IDS; one is hybrid learning approach of using multiple heterogenous machine learning algorithms and the other is ensemble approach of combining multiple weak models of homogenous machine learning algorithms [39]. Both hybrid and ensemble approaches are used in attack detection to get more accurate prediction. Researchers in [4], [13],[14],[17], [28] models the IDS by using above said methods. Every method performs well in its own way but the specific method is selected based on the problem to be taken by the researcher. The ultimate goal is to constructs a model that efficiently classifies traffic packets between attack and benign. Classification performance is greatly improved by using appropriate data preprocessing, feature selection (feature extraction) and dimensionality reduction (feature reduction) technics [26].

Data pre-processing:

Data pre-processing is a promising step that should be done before going to build the classifier. Pre-processing is the task of cleaning the dataset and making it ready for model construction. Models constructed without proper pre-processing may lead to a bad detection. Pre-processing includes many tasks some of them are given below:

- Handling missing values: data may include some missing values those values should be handled either by removing them or replacing them with some suitable value like mean.

- Removing unused fields: Data may contain some unused fields which contribute nothing to construct a model. Those fields should be identified and removed carefully.
- Handling data ambiguity: Some datasets may contain ambiguous entries. If one instances of the dataset with some set of values leads to an attack and there exist another instance of the same dataset with the same set of values leads to a benign label this situation can be treated as data ambiguity. Those ambiguous fields should be removed.
- Handling categorical fields: Some machine learning algorithms needs only numeric data. But real-world attack data may also include categorical attributes. So, these categorical attributes need to be converted in to numeric by adopting good conversion methods.
- Normalization: Normalization is the process of scaling the data into a specific range. Min-Max and Z-score are two famous methods used for data normalization.

Feature selection (FS):

Not all features of the dataset are informative. There may exist some irrelevant features which needs to be ignored, otherwise they may lead to a reduced detection performance. FS is the process of selecting only significant features for attack detection process and ignoring the insignificant ones. There are two FS technics [32] one is filter method and the other is wrapper method.

- Filter Method: Feature selection by using filters is done by assessing the importance of each feature. Different kind of filters [7] include Information Gain (IG), IG Ratio, Genetic Algorithm (GA), Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), Swarm Based Algorithms, Bee Colony optimization, etc.
- Wrapper Method: Feature selection by using wrappers is done by assessing the contribution of each feature in improving the model performance. Any machine learning methods like NB, RF, C4.5, etc. can act as wrappers.

Dimensionality Reduction:

Dimensionality reduction is the process of transforming original raw features into the new dimensions (reduced set of features) by preserving the originality of the data. Correlation Feature Selection (CFS) [12], [23] and Principal Component Analysis (PCA) [15], [19], [23] are the examples of Dimensionality reduction techniques.

3.1 IDS Framework

After collecting a suitable data set, data pre-processing is performed. Later this pre-processed data is partitioned into training and testing data. A model is constructed on the training data by adopting any of the machine learning algorithms. The performance of the model is assessed by testing the model using testing dataset. Machine learning provides many metrics like accuracy, precision, recall, F1 measure, sensitivity and specificity etc. for assessing the performance of the model. The general framework of IDS is as shown in the Fig.1.

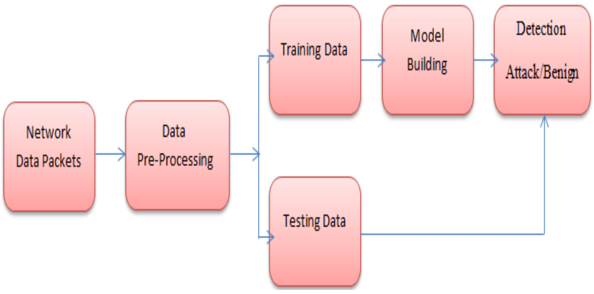

Fig 1: Block diagram of IDS

4. Benchmark Dataset for IDS

Good attack dataset is needed for implementing effective IDS. Many researchers used NSL-KDD dataset [8] which is a bench mark dataset for intrusion detection. NSL-KDD is a refined version of KDD dataset which is derived from DARPA dataset and it consists of 43 features (including class label) and 1, 47,907 instances. Each instance is labeled as either an attack or a benign activity. There are 40 distinct attacks in the dataset and all these attacks are grouped into four attack groups namely DoS, Porb, R2L and U2R. The dataset is highly dominated by the instances of DoS attacks and very less represented by U2R attacks. Distribution of different attack groups along with the details of individual attacks belongs to each group and the list of all attributes present in the dataset is clearly given in [9] in the form of figures and tables.

All features of NSL-KDD are distributed into three groups [10]. They are basic features, content features within a connection suggested by domain knowledge and traffic features. Basic features provide information about packet header, content features provide information about packet content and finally network traffic features gives statistical information representing all connections to the same destination machine computed using two-second time window.

There are some downloadable NSL-KDD files available in the repository [11]; namely, KDDTrain+.ARFF, KDDTrain+.TXT,KDDTrain+, KDDTrain+_20Percent.ARFF, KDDTrain+_20Percent.TXT, KDDTest+.ARFF, KDDTest+.TXT, KDDTest-21.ARFF, KDDTest-21.TXT. Some of these files representing full dataset and some are representing 20% of the dataset. Researchers can use these files according to their purpose.

5. Existing Approaches to IDS

Many researchers suggest different novel approaches for IDS implementation through their research papers.

Desale et. al in [12] focused on feature selection technique for selecting best features which will helps in the construction of a good model for IDS. They have used CFS technique by using mathematical intersection principle based Genetic Algorithm (GA) as a heuristic search algorithm. Features selected after CFS using the GA method are the intersection of combinations of population size and Generations. The effectiveness of feature selection technique performed after pre-processing is tested by using Naïve Bayes and J48 classifiers with the help of NSL-KDD dataset and achieves a good accuracy of 96.06% with Naïve Bayes classifier.

Jaswal et. al in [13] proposed a hybrid approach that uses the technique of k-means, support vector machine and association rule mining algorithm for implementing IDS. Initially data redundancy is controlled by applying k-means clustering algorithm. Later SVM is applied on top of these clusters and finally association rule mining is applied to classify the KDD’99 data instances into normal or anomaly.

Goeschel et. al in [14] proposed a model for reducing false positives by combining SVM, Decision Trees and Naïve Bayes methods. Initially SVM is used to classify the KDDCUP 99 data packets into attack and normal and then all the attack instances are classified by decision tree into known and unknown attacks. The classified unknown attacks are submitted to Naïve Bayes and likeliness to the other attacks are determined. If high similarity is found it indicates a true positive otherwise this new alert should be submitted to farther investigation.

Peng et. al in [15] have proposed a clustering method based on Mini Batch Kmeans with PCA (PMBKM) for IDS. First, they have applied PCA to reduce the data dimensionality and on top of these they have applied mini-batch k-means algorithm to cluster the data by making use of K-Means++ to initialize the cluster centers. Clusters are updated in each iteration by a new random sample from the data.

Malik et. al in [16] classify network intrusions by applying pruned DT classifier. DT pruning is performed using both single (SO-DTP) and multi (MO-DTP) -objective particle swarm optimization (PSO) algorithms.

Saleh et. al in [17] proposes a Hybrid IDS (HIDS) with three main contributions. First contribution is Naïve Base feature selection (NBFS) technique for dimensionality reduction with two submodules: Feature effect identification (FEI) and mutual effect Identification (MEI). FEI identifies the importance of a single feature whereas MEI identifies the mutual importance a pair of features using NB classifier in a trial and error method. The second contribution is the Optimized Support Vector Machines (OSVM) for outlier rejection which is initially learned using the highly descriptive examples of each class, then is used to remove outliers from the input training dataset and the last contribution is the prioritised KNN (PKNN) for classification. PKNN is the enhancement of KNN which considers average distance from K nearest neighbors to the input point to be classified.

Hachmi et. al in [18] proposed a multi-objective optimization process (MOP_IDS) that aims to control false negatives and false positives by using multiple IDSs. MOP_IDS composed of four steps; namely, clustering inter-alerts, filtering, clustering inter-IDS, and optimization. Authors have experimented the proposed method on DARPA and NSL-KDD dataset.

Vasan et. al in [19] experimented the effectiveness of PCA for intrusion detection. They have identified the optimal number of principal components as ten for intrusion detection. They have also found that PCA enhances the classification accuracy when data is noise free.

Hajimirzaei et. al in [20] proposed a new IDS based on a multilayer perceptron (MLP) network, artificial bee colony (ABC) and fuzzy clustering algorithms. Homogeneous subsets of training data are prepared with fuzzy clustering. ABC is used to optimize the MLP parameters while training MLP and the optimized MLP is used for final classification of attack and normal.

Thaseen et. al in [21] have proposed an intrusion detection model that uses rank-based chi-square feature selection technique and multi class SVM classifier. Special parameter tuning technic is employed to tune the parameters of SVM using a validation dataset. This optimal SVM is used for classification of traffic packets

Gautam et. al in [22] have proposed Host based Intrusion Systems Model (HISM) to detect host-based intrusions using logfiles that are generated by a single personal computer. They have used two types of computational neural network models, namely, Generalized Regression Neural Network (GRNN) model and Multilayer Perceptron Neural Network (MPNN) model and achieved high accuracies with reduced FPR.

Varghese et. al in [23] experimented and tested the effectiveness of two feature reduction technics PCA and CFS on different machine learning algorithms (RF, J48, NBTree, LibSVM, Bagging with REP Tree, PART and MLP) using NSL-KDD dataset. Their performance results in a conclusion that out of all classifiers RF gives good classification accuracy when applied on PCA.

Ferriyan et. al in [24] emphasis on applying GA for selecting optimal features. For this they have prepared three training datasets: ON, RM and OA based on relevance of features w.r.t attacks. Optimal features are selected from the three datasets using GA with one-point cross over. RF is applied on these selected features of the datasets for getting classification of labels.

Ariafar et. al in [25] proposed an optimized framework for network attack detection using K-means and DT methods. GA is used for optimizing the parameters (value of K and number of runs) of K-means and confidence parameter of DT. This optimized k-means is used for grouping the data into clusters. The new data with updated cluster labels is submitted to classification using optimised DT classifier for attack detection. Their study aimed to improve the performance of NEC approach proposed by Chen et. al in [28].

Chowdhury et. al in [26] proposed a method for detecting malwares which uses data pre-processing followed by feature extraction using n-gram and PE followed by PCA based feature reduction methods for enhancing detection accuracy. ANN with feed forward is applied as a classifier.

Jaiswal et. al in [27] proposed a K-nearest neighbor and Ant colony optimization (KNN-ACO) approach for intrusion detection. ID3 algorithm is used for feature reduction which uses IG and entropy for selecting the feature as a decision node. These reduced feature datasets are then classified using KNN-ACO classifier.

Chen et. al in [28] proposed a new ensemble clustering (NEC) approach for intrusion detection using DB Scan, One SVM, Agglomerative Clustering and Expectation Maximization methods, where in each method take a specific subspace of the original dataset and comes with classified labels, finally all the resulted labels are ensembled and evaluated using a voting model.

Syarif et. al in [29] have proposed a model which uses RF based binary PSO for feature selection wherein, at each generation, the process of attribute selection is performed using binary PSO, and within the PSO loop, classification is performed using RF. KNN is used for classification of traffic packets.

Farnaaz al in [30] built an IDS by applying RF classifier for detecting attack groups like DOS, R2L, Probe and U2R. They have initially pre-processed the data followed by feature subset selection by applying Symmetrical uncertainty (SU) measure on the pre-processed data and applied RF classifier only on the selected feature subsets.

Chiba et. al in [31] proposed a Cooperative and Hybrid Network IDS (CH-NIDS) which is a network intrusion detection system that can detect both known and unknown cloud-attacks. CH-NIDS applies snort on the network packets for detecting known attacks as a first phase of detection and as a second phase of detecting unknown attacks, it applies optimized Back Propagation Neural Network (BPNN) on the undetected packets of phase 1.CH-NIDS should be deployed at frontend and backend of cloud for effective detection.

Tchakoucht et. al in [32] selects most important set of features using filter and wrapper methods. IG and CFS methods are used as filters and NB, RF, C4.5 and REP Tree classifiers are used as wrappers. The importance of a feature is evaluated taking into account all the feature selection methods and the contribution of the feature in the improvement of accuracy and efficiency. Classification was applied on the selected best features in feature selection phase.

Balakrishnan et. al in [33] proposes Optimal Feature Selection (OFS) algorithm combined with two-step classification process. OFS is a feature selection strategy which uses IG-Ratio for selecting best features. Rule based classifier was applied on the selected features as a first step of classification and then further classification is carried out by SVM.

Saxenaet. al in [34] proposes an SVM-PSO method for intrusion detection. SVM-PSO uses standard PSO for selecting SVM parameters and binary PSO for selecting best feature subset and SVM is used for classification of labels.

Paulauskas et. al in [35] analyses the influence of data pre-processing on attack detection by using different machine learning methods like Decision Trees, Naïve Bayes and Rule-Based classifiers with NSL-KDD dataset.

Tesfahun et. al in [36] proposes a hybrid approach for intrusion detection which detects both known and unknown attacks using two layers. First layer implements signature-based IDS using RF classifier and blocks detected (known) attack instances. The second layer implements anomaly-based IDS by applying ensemble of one-class SVM classifiers with bootstrap aggregating technique on the normal instances filtered out from the first layer. The detected attacks from this second layer are again blocked and updated to the train set.

Chabathula et. al in [37] have made an experiment on the effect of dimensionality reduction with PCA on different machine learning algorithms like Support Vector Machines (SVM), K-Nearest Neighbors (KNN), J48 Tree algorithm, Random Forest Tree classification algorithm, Adaboost algorihm, Nearest Neighbors generalized Exemplars algorithm, Naïve Bayes probabilistic classifier and

Voting Features Interval classification algorithm. Tre algorithms gives highest classification accuracy.

6. Conclusion

This paper presents brief information about IDS followed by machine learning approach to its implementation. Recent enhancements in the evaluation of intrusions detection systems are also mentioned in this paper as per the research made by various researchers. Even though all the approaches suggested by different researchers differed in their own way, there is a commonality of adopting knowledge from the train dataset which is in same characteristic with the test dataset. As new and unpatched attacks are evolving day by day, existing attack patterns are no longer sufficient to detect zero-day attacks. This inability to evaluate IDS against current and evolving intrusions is a major practical concern. Scarcity of labelled data in the field of security is a big hurdle for evaluation of effective IDS. As knowledge sharing helps to improve the detection accuracy our future focus of the research is on knowledge sharing IDS. Two promising directions are identified.

One is Intrusion Detection Network (IDN) and the other is Transfer learning (TL). Different collaborative IDSs formed as a network for sharing attack knowledge constitute an IDN. The IDN [5] aims to reduce the FPR while dealing with zero-day attacks by reducing the latency in formation and dissemination of signature of new attacks through knowledge sharing. However, some of the nodes become victims of zero-day attacks unless they rely on hybrid architecture which includes signature based as well as anomaly-based detection methods leading to some FPR. Transfer learning [38] offers promising solutions to handle this problem. TL is a recent advancement of machine learning that builds models for target domains with minimal or no labelled training examples leveraging the knowledge learnt from a related source domain having abundant training examples.

Reference

[1] FROST & SULLIVAN https://ww2.frost.com/, Accessed March, (2019).

[2] N. Sameera and M. Shashi, A Survey on cyber security analytics. International journal of computer science and engineering. vol 6, issue 11, PP. 649-652, Nov (2018).

[3] Carol Fung and Raouf Boutaba, Auerbach, “Cyber Intrusions” Intrusion Detection Networks: a Key to Collaborative Security, (2017).

[4] B. Setiawan, S. Djanali and T. Ahmad, A study on intrusion detection using centroid-based classification. 4th information systems international conference Bali. Indonesia, Nov (2017).

[5] Carol Fung and Raouf Boutaba, Auerbach :“Intrusion Detection.” Intrusion Detection Networks: a Key to Collaborative Security, (2017) .

[6] N.Sameera and M. Shashi, Encoding approach for intrusion detection using PCA and KNN classifier. Springer AISC series. Unpublished.

[7] Balasaraswathi VR, Sugumaran M and Hamid Y, Feature selection techniques for intrusion detection using non-bio-inspired and bio-inspired optimization algorithms. Journal of Communications and Information Networks. Dec 1;2(4):107-19, (2017) .

[8] Botes FH, Leenen L and De La Harpe R, Ant colony induced decision trees for intrusion detection. In ECCWS 16th European Conference on Cyber Warfare and Security (p. 53). Academic Conferences and publishing limited, (2017).

[9] N. Sameera and prof. M. Shashi, Protocol specific intrusion detection using KNN classifier. International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; Volume 6 Issue V, (2018).

[10] https://kdd.ics.uci.edu/databases/kddcup99/task.html,Accessed Feb, (2019).

[11] Dhanabal L and Shantharajah SP, A study on NSL-KDD dataset for intrusion detection system based on classification algorithms. International Journal of Advanced Research in Computer and Communication Engineering.4(6):446-52, (2015).

[12] Kannan A, Maguire Jr GQ, Sharma A and School, Genetic algorithm-based feature selection algorithm for effective intrusion detection in cloud networks. In IEEE 12th International Conference on Data Mining Workshops pp. 416-423, (2012).

[13] Jaswal K, Kumar P and Rawat S, Design , Development of a prototype application for intrusion detection using data mining. 4th international conference on reliability, infocom technologies and optimization (ICRITO) (trends and future directions) pp. 1-6. IEEE, (2015)

[14] Goeschel and Kathleen, Reducing False positives in intrusion detection systems using data-mining techniques utilizing support vector machines, decision trees, and naive Bayes for off-line analysis. In Southeast Con 30 (pp. 1-6). IEEE, (2016).

[15] Peng K, Leung VC and Huang Q, Clustering approach based on mini batch K means for intrusion detection system over Big Data. IEEE Access.;6:11897-906, (2018).

[16] Malik AJ and Khan FA, A hybrid technique using binary particle swarm optimization and decision tree pruning for network intrusion detection. Cluster Computing.21(1):667-80, (2018).

[17] Saleh AI, Talaat FM and Labib LM, A hybrid intrusion detection system (HIDS) based on prioritized k-nearest neighbors and optimized SVM classifiers. Artificial Intelligence Review.:1-41, (2017).

[18] Hachmi F, Boujenfa K and Limam M, Enhancing the Accuracy of Intrusion Detection Systems by Reducing the Rates of False Positives and False Negatives Through Multi-objective Optimization. Journal of Network and Systems Management.27(1):93-120, (2019).

[19] Vasan KK and Surendiran B, Dimensionality reduction using Principal Component Analysis for network intrusion detection, Perspectives in Science.1;8:510-2, (2016).

[20] Hajimirzaei B and Navimipour NJ, Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm. ICT Express, (2018).

[21] Thaseen IS and Kumar CA, Intrusion detection model using fusion of chi-square feature selection and multi class SVM. Journal of King Saud University-Computer and Information Sciences. 1;29(4):462-72, (2017).

[22] Gautam SK and Om H, Computational neural network regression model for Host based Intrusion Detection System. Perspectives in Science. 1;8:93-5, (2016).

[23] Varghese JE and Muniyal B, An investigation of classification algorithms for intrusion detection system—A quantitative approach. International Conference on Advances in Computing, Communications and Informatics (ICACCI)(pp. 2045-2051). IEEE, (2017).

[24] Ferriyan, A., Thamrin, A.H., Takeda, K. and Murai, J, Feature selection using genetic algorithm to improve classification in network intrusion detection system. International Electronics Symposium on Knowledge Creation and Intelligent Computing (IES-KCIC) (pp. 46-49). IEEE, September, (2017).

[25] Ariafar E and Kiani R, Intrusion detection system using an optimized framework based on datamining techniques. IEEE4th International Conference on Knowledge-Based Engineering and Innovation (KBEI),pp. 0785-0791, (2017).

[26] Chowdhury M, Rahman A and Islam R, Protecting data from malware threats using machine learning technique. 12th IEEE Conference on Industrial Electronics and Applications (ICIEA) (pp. 1691-1694). IEEE, (2017).

[27] Jaiswal S, Saxena K, Mishra A and Sahu SK, A KNN-ACO approach for intrusion detection using KDDCUP'99 dataset. 3rd International Conference on Computing for Sustainable Global Development (INDIACom),pp. 628-633.IEEE, (2016).

[28] Chen W, Kong F, Mei F, Yuan G and Li B, A novel unsupervised anomaly detection approach for intrusion detection system. 3rd international conference on big data security on cloud (bigdata security), international conference on high performance and smart computing (hpsc), and international conference on intelligent data and security (ids).pp. 69-73. IEEE, (2017).

[29] Syarif AR and Gata W, Intrusion detection system using hybrid binary PSO and K-nearest neighborhood algorithm. 11th International Conference on Information & Communication Technology and System (ICTS), pp. 181-186. IEEE, (2017).

[30] Farnaaz N and Jabbar MA, Random forest modeling for network intrusion detection system. Procedia Computer Science.89:213-7, (2016).

[31] Chiba Z, Abghour N, Moussaid K and Rida M, A cooperative and hybrid network intrusion detection framework in cloud computing based on snort and optimized back propagation neural network. Procedia Computer Science.83:1200-6, (2016).

[32] Tchakoucht TA and Ezziyyani M, Building a fast intrusion detection system for high-speed-networks: probe and DoS attacks detection. Procedia Comput Sci.127:521-30, (2018).

[33] Balakrishnan S, Venkatalakshmi K and Kannan A, Intrusion detection system using Feature selection and Classification technique. International Journal of Computer Science and Application. 1;3(4):145-1, (2014).

[34] Saxena H and Richariya V, Intrusion detection in KDD99 dataset using SVM-PSO and feature reduction with information gain. International Journal of Computer Applications. 98(6), (2014).

[35] Paulauskas N and Auskalnis J, Analysis of data pre-processing influence on intrusion detection using NSL-KDD dataset. Open Conference of Electrical, Electronic and Information Sciences (eStream)(pp. 1-5). IEEE, (2017).

[36] Tesfahun, Abebe, and D. Lalitha Bhaskari, Effective hybrid intrusion detection system: A layered approach. International Journal of Computer Network and Information Security 7.3 (2015): 35.

[37] Chabathula, Krupa Joel, C. D. Jaidhar and MA Ajay Kumara, Comparative study of Principal Component Analysis based Intrusion Detection approach using machine learning algorithms. In Signal Processing, Communication and Networking (ICSCN), 3rd International Conference , pp. 1-6. IEEE, (2015).

[38] Weiss K, Khoshgoftaar TM, Wang D, A survey of transfer learning. Journal of Big Data. ec;3(1):9, (2016).

[39] Kazienko, Przemysław, Edwin Lughofer, and Bogdan Trawiński, Hybrid and ensemble methods in machine learning. J. UCS special issue. J Univers Comput Sci 19.4 : 457-461, (2013).