iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VII **Month of publication:** July 2020

DOI: https://doi.org/10.22214/ijraset.2020.30598

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VII July 2020- Available at www.ijraset.com

A Survey on Building an Effective Intrusion Detection System (IDS) using Machine Learning Techniques, Challenges and Datasets

Arvind T[1], Dr. K. Radhika[2]
[1]*UCSS, OU, HYD,*
[2]*Professor, Department of IT, CBIT, HYD*

Abstract: ***Accessibility is a critical issue for network security, to protect network resources. A self-explanatory system will therefore be developed to provide information to any organization whether public or private. There were many Instrusion Detection Systems(IDSs) proposed in the past by various researchers. This paper aims on surveying various IDS techniques and presenting a brief description of IDS, Datasets and machine learning approach for its implementation.***
Keywords: Intrusion Detection, Machine learning, Single Classifiers, Hybrid Classifiers, Ensemble Classifiers, KDD Cup 1999, NSL-KDD data set.

I. INTRODUCTION

Internet plays vital role in today's world. It's utilized in education, business, shopping, social networking and other critical infrastructures are dependent upon it for their day-to-day operation. This has increased risk of computer systems connected to the web becoming targets of intrusions by cyber criminals. Cyber criminals attack systems to realize unauthorized access to information, misuse information or to scale back the supply of data to authorized users. This leads to huge financial losses to companies besides losing their goodwill to customers. Intrusion prevention techniques like user authentication (e.g. using password or biometrics), information protection (e.g. encryption), avoiding programming errors and firewalls have been adopted to protect the computer systems. But, unfortunately these intrusion prevention techniques alone aren't adequate. There'll always be unknown exploitable weaknesses within the system thanks to design and programming flaws in application programs, protocols and operating systems. Therefore, we'd like mechanism to detect intrusions as early as possible and take appropriate actions [1] .

An intrusion is defined as any set of actions that compromise the integrity, confidentiality or availability of a resource [2] [3]. If a system is able to assure that these three security tokens are fulfilled, it is considered to be secure.There are two sorts of intrusion detection techniques: Misuse and Anomaly. Misuse detectors analyze system activity, trying to find events or sets of events that match a predefined pattern of events that describe a known attack. Because the patterns corresponding to known attacks are called signatures, misuse detection is sometimes called "signature-based detection." Anomaly detectors identify anomalies on a host or network. They function on the idea that attacks are different from legitimate activity and may therefore be detected by systems that identify these differences [4]. An Hybrid IDS can be defined as a combination of both signature and anomaly based IDS.

Data coming from various host activities including audit records of operating system, system logs and process activities is employed for analysis is understood as Host-based IDS.Data coming from network traffic is collected for analysis using sniffing software like TCPDUMP is understood as Network-based IDS.

II. MACHINE LEARNING TECHNIQUES

Machine learning is a branch of artificial intelligence that gives the systems, ability to learn automatically and improve from experience without being explicitly programmed. These techniques are adopted to recognize the patterns. Machine learning algorithms can be divided in to different types based on the purpose such as Supervised learning, Unsupervised learning,Semi-supervised learning and Reinforcement learning.

A. Standard/Single Classifiers

A classifier is an algorithm that maps the input data to a specific category. A standard classifier or a single classifier is an algorithm that uses a single algorithm.

©IJRASET: All Rights are Reserved

1) *Decision trees:* The decision tree algorithm classifies data employing a series of rules. It's a tree like structure, which makes it interpretable. The decision tree algorithm can automatically eliminate the irrelevant and redundant features. The learning process comprise feature selection, tree generation, and tree pruning. When training a decision tree model, the algorithm selects the most appropriate features individually and generates child nodes from the root node. The decision tree is a fundamental classifier. Some advanced algorithms, like the random forest and thus the extreme gradient boosting (XGBoost), consist of multiple decision trees[5].
2) *K-Nearest Neighbor(K-NN):* K-Nearest Neighbor (K-NN) is a simple and traditional non-parametric approach for classification that classifies the objects which are presented as points defined in feature space [6] [7]. From the input vector, it calculates the approximate distances between different points and assigns the unlabeled points to the foremost frequent class labels among considered in training samples of its k-nearest neighbors. In the process of K-NN model creation, k is an vital factor and for different k values generate different performances. If k is large, the model takes large classification time and influence the prediction accuracy. Conversely, the larger k is, the simpler the model is and the weaker the fitting ability.K-NN model is mentioned as an instant based learner not an inductive based learning approach [8]. The K-NN model does not contain the training stage, but only searches input vector and classifies new attributes.
3) *Support Vector Machine (SVM):* Vapnik was introduced Support vector machine in the mid-1990.The strategy in SVMs is to seek out a max-margin separation hyperplane in the n-dimension feature space. SVMs are able to do gratifying results even with small-scale training sets because the separation hyperplane is determined only by alittle number of support vectors. On the other hand, SVMs are sensitive to noise near the hyperplane. SVMs are able to solve linearproblems well. For nonlinear data, kernel functions are usually used. A kernel function maps the original space into a new space in order that the original nonlinear data can be separated. Kernel tricks are extesively present in both SVMs and other machine learning algorithms.
4) *Artificial Neural Network (ANN):* An artificial neural network is a unit of processing information. It mimics the neurons of the human brain. For pattern recognition problem multilayer perceptron (MLP) is the most generally used structure of the neural network [11]. The architecture of MLP consists of an input layer, one or more hidden layers with computational nodes, and an output layer. The interconnection between nodes has scalar weights and bias which are adjusted during the training phase. MLP usually train besides with back propagation learning algorithms referred to as back propagation neural network. Assigns random weights at beginning of training, then adjust weights during train and minimizing the error of misclassification.In supervised learning, the neural network is provided with labelled training set which learns a mapping from inputs x to outputs y , given a labelled set of inputs-output pairs $d = \{(x_i, y_i)\}_{i=1}^{N}$ where d is called the training set and N is the number of training examples. It is assumed that y_i is a categorical variable from some infinite set $y_i \epsilon \{1...C\}$ [16]. The multi–layer perceptron (MLP) is a type of ANN that is trained using supervised learning procedures. The MLP was used in [14] to detect intrusions based on an off-line analysis approach. In a different approach, MLP was used in [15] to detect intrusion on network data comparing its performance with Self-Organizing Maps (SOM).
5) *Genetic algorithms:* Genetic algorithms are catogorized as global search heuristics, and evolutionary computation that uses techniques inspired by evolutionary biology like recombination, selection, inheritance and mutation. Thus, genetic algorithms represent another kind of machine learning-based technique, capable of deriving classification rules [9] and/or selecting appropriate features or optimal parameters for the detection process [10] . In [13] rule evolution approach supported Genetic Programming (GP) for detecting novel attacks on networks is proposed. In their framework, four genetic operators, namely reproduction, mutation, crossover and dropping condition operators, are used to evolve new rules. New rules are used to detect novel or known network attacks. Experimental results show that rules generated by GPs with part of KDD 1999 Cup data set has a low false positive rate (FPR), a low false negative rate (FNR) and a high rate of detecting unknown attacks. However, an evaluation with full KDD training and testing data is missing in the paper.
6) *Fuzzy Logic:* The term of fuzzy logic was produced by Professor Lotfi Zadeh [23]. Fuzzy logic appears in many successful sophisticated systems in many application areas. There are some application areas where the two valued logic and the related binary decision could lead to inefficient solutions. Fuzzy logic offers several advantages to handle the binary decision problems [17]. There are some requirements arsing during the design and implementation of fuzzy system. The inputs and outputs of the fuzzy system should be well-defined, then the fuzzy partitions of the input and output universes should be established, then the fuzzy rule base must be completely prepared. Fuzzy partitions of the input values provide a significant way to define the real input value with each predefined linguistic term [18]. For generating a conclusion by a fuzzy system, first the crisp inputs are transformed to fuzzy sets by the fuzzifier, then from the fuzzified input, the fuzzy inference system calculates the fuzzy conclusion.At the end, the crisp output is prepared by defuzzification of the fuzzy conclusion [19]. In typical fuzzy inference

©IJRASET: All Rights are Reserved

system, the fuzzy rule base is extracted from expert knowledge. To be able to handle all the possible input values, the fuzzy rule base must cover all the input universes. Hence, the step of the fuzzy rule base considered as the most critical step during the design of the fuzzy system. Typically, generating a complete fuzzy rule base in a multidimensional problem is difficult to be implemented because of the lack of information for all the possible fuzzy rules. In case of missing rule definitions, there could be some observation which is not covered by any of the fuzzy rules, in that case no conclusion can be gained from the rule base. The FRI methods can solve this situation [20-21].

7) Naive Bayes: It is simple and commonly used probabilistic classifiers based on Bayes theorem. On the basis of the class label given Naive Bayes assumes that the attributes are conditionally independent and thus tries to estimate the class-conditional probability. The typical structure of naïve bayes represented by a directed acyclic graph (DAG), where system variables are represented by node and influence of one node on another by link [22].

B. Hybrid Classifiers

The idea of the hybrid classifiers is to merge two or more machine learning algorithms
in order that the system improves the performance significantly. Generally, the hybrid method consists of two functional components, the primary one takes input raw data and produces intermediate results, then the other one takes intermediate results as an input and produces final results [23].In general hybrid classifiers based on clustering,pre-process the data for removing the irrelevant and inconsistent data from training samples of every class. Then the clustered data used as a training sample of classifiers. Finally, hybrid approach is a combination of two or more different techniques in which initially optimizing the performance and finally use model for prediction.

C. Ensemble Classifiers

Ensemble classifiers were proposed to enhance the performance of single classifiers. It's a process of merging multiple weak learners, trained on different training samples and merging their outputs into a single prediction. Generally, used ensemble methods are bagging, boosting and stacking[44],[45]. Though it's known that the weaknesses of the component classifiers get accumulated in the ensemble classifier, it's been providing an efficient performance in some combination, in order that the researchers are getting more interesting users of ensemble classifiers.

III. LITERATURE REVIEW

Intrusion detection started in 1980's and since then several techniques have been adopted to built intrusion detection systems [24]. presently building an effective IDS is an massive knowledge engineering task.System builders relay on their intuition and knowledge to pick the statistical measures for anomaly detection. Experts analyse and categorize attack scenarios and system vulnerabilities, and hand-code the corresponding rules and patterns for misuse detection. due to the manual and Adhoc nature of the event process, current IDSs have limited extensibility and adaptableness . Most IDSs only handle one particular audit data source, and their updates are expensive and comparatevely slow [25][26].Heba Ezzat Ibrahim et al.[27] proposed a multi-Layer intrusion detection system. The experimental results exibited by the suggested multi-layer model using C5 decision tree obtained higher classification rate accuracy, utilizing feature selection by Gain Ratio(GR), and fewer false alarm rate than MLP and naïve Bayes. Utilizing Gain Ratio raises the accuracy of U2R and R2L for the three machine learning techniques (C5, MLP and Naïve Bayes) notably. MLP has high classification rate when using the whole 41 features in Dos and Probe layers. Shanmugavadivu et al. [29] proposed an IDS based on fuzzy logic to detect an intrusion detection behavior within a network. They adopoted automated strategy for generation of fuzzy rules, which are obtained from the definite rules using frequent items. KDDCup99 dataset was taken for the experiment and after dimension reduction the model gives approximately 90% detection rate. K.Nageswara rao et al.[28] evaluated the influence of attribute pre-selection using Statistical techniques on real-world kddcup99 data set. Experimental result exibited that the accuracy of the C4.5 classifier can be improved with the robust preselection approach when compare to traditional feature selection stratagies but the sole drawback with this strategy is implementing correct attribute selection measure in C4.5 decision tree algorithm. Shah et al [30]. proposed a signature based IDS using SNORT and WTNPCAP on windows platform. Using this powerful software SNORT, real time traffic analysis has been performed and packet logging has been administered. In this work, there's a scope of improvement in processing time. Esmaily et al. [31] proposed a combined Multi-Layer Perceptron (MLP) and Decision tree based technique.All the 41 features of KDDCup99 dataset was used for experimental analysis, their results generated a significant low false alarm value but were also difficult to implement in real time traffic analysis.Ozgur Depren et al. [32], use DT and NN oriented algorithms to classify attack and normal records. In their hybrid IDS, they use Decision Support System (DSS) for

©IJRASET: All Rights are Reserved

misuse detection using the KDD CUP99 dataset.Jaiswal et. al in [33] proposed a K-nearest neighbor and Ant colony optimization (KNN-A CO)approach for intrusion detection. ID3 algorithm is used for feature reduction which uses Information Gain and entropy for selecting the feature as a decision node. These reduced feature datasets are then classified using KNN-ACO classifier. Ioulianou et al [35]. proposed a signature based IDS for IOT networks which adopts both centralized and distributed IDS modules using Cooja simulator. A Denial of Service (DOS) attack scenario was created on IOT devices. They concluded that it supports application development for Contiki OS, but did not import the IDS modules to Contiki OS to test its performance in real world IOT environment. Wei-Chao Lin et-al proposed [46] a k-NN classifier to predict the state of every network packet, whether to be from a normal or attack traffic. This system is trained and evaluated using the KDD CUP'99 dataset, where the evaluation measures show a good prediction accuracy of 99.89% accurate predictions. However, because the k-NN classifier is a lazy classifier, the knowledge is extracted whenever a prediction is required, i.e., the training dataset is scanned each time a new packet enters the network, which is a very resource-consuming process that needs either expensive servers with high resources, or longer execution time that will degrade the quality of the services provided on the network.Revathi et.al. [34] select 15 features using CFS and test using various classifiers such as Random Forest, C4.5 decision tree, SVM, CART and Naïve Bayes. The results mentioned by the classifiers are compared and theerefore the outcome shows that Random Forest gives highest accuracy in detecting attacks. Ganapathy et al [47] proposed a new classification algorithm using C4.5 decision tree for effective classification. The same set of authors introduced the enhanced version of their algorithm with the help of intelligent agents [48]. Jaisankar et al [49] proposed a new rough set based decision tree algorithm for enhancing the intrusion detection accuracy. They used C 4.5 decision tree for decision making along with the fuzzy rough set theory. Srinivas Mukkamala et.al [36] proposed Support Vector Machine (SVM) and Neural Networks (NN) for intrusion detection system. The two primary reasons for using SVM for intrusion detection are: speed and scalability. The experiments were carried using DARPA 1998 dataset. The training time for SVMs is significantly shorter (17.77 sec) than that of neural networks (18 min). This becomes a crucial advantage in situations where retraining must be done quickly. The performance of SVM showed that SVM IDS have slightly higher rate of creating the correct detection than neural networks. However, SVMs can make only binary classifications which can be a disadvantage when IDS requires multi-class identifications.In [37] the authors proposed Principal Component Analysis (PCA) algorithm for dimension reduction. After dimension reduction the 16 relevant features of KDD99 dataset were further passed into Na¨ive Bayes classifier for prediction but the experiment was conducted with a few number of instances. Desale and Ade [43] proposed GA based feature selection method used different feature selection methods, Correlation based Feature selection (CFS), Information Gain (IG), and Correlation Attribute evaluator (CAE) for feature selection, and performance classified by Naïve bayes or J48. They used NSL-KDD dataset and selected the minimum number of features, and improved accuracy of Naïve Bayes classifier with reduced time.Abdullah et al. [39] also proposed a framework of IDS with selection of features within the NSL-KDD dataset that are based on dividing the input dataset into different subsets, and combining them using Information Gain (IG) filter. C. Khammassi et.al [41] suggested a wrapper based feature selection algorithm for intrusion detection by adopting the genetic algorithm (GA) as an heuristic search method and Logistic Regression (LR) as the evaluating learning algorithm. The suggested approach is labeled as GA-LR. GA derive from the natural selection process and it is under the category of evolutionary based algorithms [42]. GA has the following building blocks: an initial population, a fitness function, a genetic operator (variation, crossover and selection) and a stopping criterion. The experiments were done to evaluate the GA-LR ,using the KDD Cup 99 Dataset and thE UNSW-B15 Dataset. Decision Tree classifiers were applied to candidates feature subsets and the results suggested that GA-LR is an efficient method. Azad and Jha [38] proposed Fuzzy min-max neural network and Particle Swarm Optimization(PSO), the learning is executed by a series of hyper box expansions, the hyper box expansion depends on box size. PSO optimize hyper box min max values and classify the attacks. This technique evaluated using KDD CUP 1999 dataset and attained better performance compared with MLP. Pham et al. [40] proposed a hybrid model, which utilizes gain ratio technique as feature selection and bagging to combine tree-based base classifiers. Experimental results show that the best performance was produced by the bagging model that used J48 as the base classifier and worked on 35-feature subset of the NSL-KDD dataset.

IV. CONCLUSION

In this paper, a detailed survey of major techniques implemented on intrusion Detection is presented. Building an effective intrusion detection system using Machine learning and Deep learning strategies have gotten a lot of consederation for network security. From the literature review discussed above, it is concluded that most of the researchers used classifiers and cluster methods as an Intrusion Detection System in prior. Later feature extraction strategies are utililzed to extract the important features, along with classifiers. In this concerned area, numerous researchers utilized hybrid classifiers for Intrusion Detection, which are a blend of feature extraction, clustering, and classification methods.

©IJRASET: All Rights are Reserved

Very few researchers utilized ensemble classifiers as Intrusion Detection techniques. The majority of the proposed techniques were evaluated on KDD CUP 1999 dataset, and NSL-KDD,a updated version of KDD'99 dataset. We propose a system where we endeavor to expand the effectiveness of the parameters in the intrusion detection system using a two-level methodology. In Level 1, We'd desire to compare any basic supervised or unsupervised learning algorithm and then in Level 2 we may like train the results from level 1 in ensemble classifier or a deep learning utilizing Artificial Neural Networks(ANN) and compare the parameters such as Accuracy, Precision, Recall,F-score. We assume that the implementation of ensemble classifier or an artificial neural network would formulate a much better way to detect anomalies in the intrusion detection system.

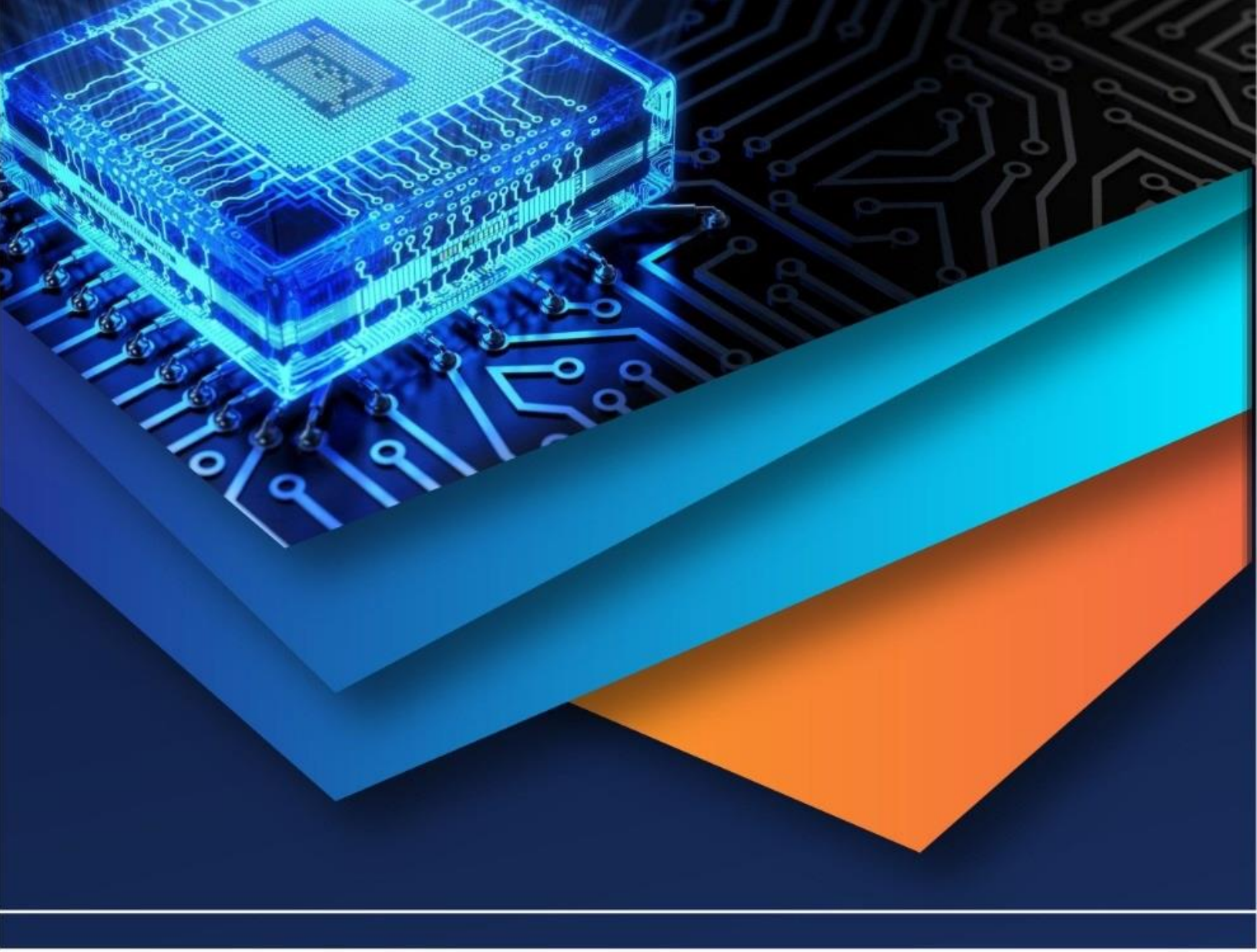
REFERENCES

[1] Lee, W., & Stolfo, S. (1998), "Data mining approaches for intrusion detection," In Paper presented at the proceedings of the seventh USENIX symposium (SECURITY'98). San Antonio, TX.
[2] Jian Pei Shambhu J. Upadhyaya Faisal Farooq Venugopal Govindaraju. Proceedings of the 20th International Conference on Data Engineering (ICDE'04) 1063-6382/04 $ 20.00 © 2004 IEEE .
[3] Debar, H., Dacier, M., and Wespi, A., "A Revised taxonomy for intrusion detection systems, Annales des Telecommunications", Vol. 55, No. 7–8, 361–378, 2000.
[4] Rebecca Bace and Peter Mell,"Intrusion Detection Systems", NIST Special Publication on Intrusion Detection Systems.
[5] Hongyu Liu, Bo Lang "Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey" Appl. Sci. 2019, 9, 4396; doi:10.3390/app9204396
[6] S. Manocha , M.A. Girolami, "An empirical analysis of the probabilistic K-nearest neighbour classifier", Science Direct, Pattern Recognition Letters, 28 (2007), 1818–1824.
[7] C.M.Bishop. (1995). Neural networks for pattern recognition. England: Oxford University.
[8] Mitchell, T. (1997). Machine learning. New york:MacHraw Hill.
[9] Bridges, Vaughn, "Fuzzy Data mining and genetic algorithms applied to intrusion detection," In:Proceedings of the National Information Systems Security Conference; 2000. pp. 13–31.
[10] Li W. "Using genetic algorithm for network intrusion detection," C.S.G. Department of Energy; 2004. pp. 1–8.
[11] S. Haykin, Neural networks: A comprehensive foundation (2nd ed.), Prentice Hall, New Jersey,U.S.A, 1999.
[12] Wei Lu ,I. Traore "Detecting new forms of network intrusion using genetic programming" The 2003 Congress on Evolutionary Computation, 2003. CEC '03,8-12 Dec. 2003.
[13] T.Lunt and I.Traore, "Unsupervised Anomaly Detection Using an Evolutionary Extension of K-means Algorithm",International Journal on Information and computer Science, Inderscience Pulisher 2 (May, 2008), 107-139.
[14] M. Moradi and M. Zulkernine, "A neural network based system for intrusion detection and classification of attacks," Proc. 2004 IEEE Int. Conf. Adv. Intell. Syst. Appl., 2004.
[15] A Bivens and C. Palagiri, "Network-based intrusion detection using neural networks," Neural Networks, vol. 12, pp. 579–584, 2002.
[16] K. Murphy, "Machine learning: a probabilistic perspective," Chance encounters: Probability in …, 2012. [Online]. Available: http://link.springer.com/chapter/10.1007/978-94- 011-3532-0_2. [Accessed: 06-Jan-2015].
[17] L. A. Zadeh, "Fuzzy Sets", Information and control, vol. 8, no. 3, pp. 338–353, 1965.
[18] L. A. Zadeh, "Fuzzy Algorithms", Information and control, vol. 12, no. 2, pp. 94–102, 1968.
[19] S. Dhopte and N. Tarapore, "Design of Intrusion Detection System Using Fuzzy Class-Association Rule Mining Based On Genetic Algorithm", International Journal of Computer Applications, vol. 53, no. 14, pp. 20-27, 2012.
[20] S. Sivanandam, S. Sumathi, S. Deepa, et al., "Introduction to Fuzzy Logic using MATLAB", Springer, vol. 1, 2007. DOI:10.1007/978-3-540-35781-0 [27] Z. C. Johanyak and S. Kovacs, "A Brief Survey and Comparison on´ Various Interpolation Based Fuzzy Reasoning Methods", Acta Polytechnica Hungarica, vol. 3, no. 1, pp. 91–105, 2006.
[21] Mohammad Almseidin, Zilveszter Kovacs,"Intrusion Detection mechanism using Fuzzy rule interpolation" arXiv preprint arXiv:1904.08790, 2019 - arxiv.org
[22] Pingj ie Tang, Rang-an Jiang, Mingwei Zhao, "Feature selection and design Of intrusion detection system based on k-means and triangle area support vector machine", Second International Conference on Future Networks,pp.144-148,2010.
[23] J. -S. Jang, C. -T. Sun, and E. Mizutani, Neuro- fuzzy and soft computing: A computational approach to learning and machine intelligence. Prentice Hall, New Jersey, USA, 1996.
[24] Yogendra kumar jain and Upendra,"An efficient Intrusion Detection Based on Decesion Tree Classsifier using Feature Reduction". International Journal of Scientific and Research Publication, Volume 2, Issue1, January 2012
[25] Anusha Jayasimhan,Jayant Gadge," Identifying Intrusion Patterns using a Decision Tree", International Journal of Computer Applications (0975 – 8887) Volume 45– No.9, May 2012.
[26] Lee,Salvatore J. Stolfo," A framework for constructing features and models for intrusion detection systems," ACM Transactions on Information and System Security, Vol. 3, No. 4, November 2000, Pages 227–261.
[27] Heba Ezzat Ibrahim,Sherif M. Badr, Mohamed A. Shaheen," Adaptive Layered Approach using Machine Learning Techniques with Gain Ratio for Intrusion Detection Systems", International Journal of Computer Applications (0975 – 8887),Volume 56– No.7, October 2012.
[28] K.Nageswara rao, D.RajyaLakshmi, T.Venkateswara Rao," Robust Statistical Outlier based Feature Selection Technique for Network Intrusion Detection",International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.
[29] Ioulianou, P., Vasilakis, V., Moscholios, I., Logothetis, M.: A signature-based intrusion detection system for the internet of things. Information and Communication Technology Form (2018).

©IJRASET: All Rights are Reserved

[30] Shah, S.N., Singh, M.P.: "Signature-based network intrusion detection system using snort and winpcap".International Journal of Engineering Research & Technology (IJERT) 1(10), 1–7 (2012)
[31] Esmaily, J., Moradinezhad, R., Ghasemi, J.: Intrusion detection system based on multi-layer perceptron neural networks and decision tree. In: 2015 7th Conference on Information and Knowledge Technology (IKT). pp. 1–5. IEEE (2015).
[32] Ozgur Depren, Murat Topallar, Emin Anari im, M. Kemal Ciliz,"An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks" " in Expert Systemswith Applications Volum me 29, Issue 4, November 2005, Pages 713–722
[33] Jaiswal S, Saxena K, M ishra A and Sahu SK, "AKNN-ACO approach for intrusion detection using KDDCUP'99 dataset." 3rd InternationalConference on Computing for Sustainable Global Development (INDIACom),pp. 628-633.IEEE, (2016).
[34] S. Revathi, and A. Malathi, "A detailed Analysis on NSL-KDD Dataset Using Various Machine Learning Techniques for Intrusion Detection", InternationalInt. J. Advanced Networking and Applications Volume: 07 Issue: 04 Pages: 2828-2834 (2016) ISSN: 0975-0290.
[35] Ioulianou, P., Vasilakis, V., Moscholios, I., Logothetis, M.: A signature-based intrusion detection system for the internet of things. Information and Communication Technology Form (2018).
[36] Srinivas Mukkamala, Guadalupe Janoski, Andrew Sung, "Intrusion Detection: Support VectorMachines and Neural Networks," In Proceedings of the IEEE International Joint Conference on Neural Networks, 2002, pp. 1702-1707
[37] Neethu, B.: "Classification of intrusion detection dataset using machine learning approaches." International Journal of Electronics and Computer Science Engineering 1(3), 1044–1051 (2012)
[38] Chandrashekhar Azad, Vijay Kumar Jha," Fuzzy min–max neural network and particle swarm optimization based intrusion detection system", Microsyst Technol, 2016.
[39] Abdullah, M., Balamash, A., Alshannaq, A., Almabdy, S., 2018. Enhanced intrusion detection system using feature selection method and ensemble learning algorithms. International Journal of Computer Science and Information Security (IJCSIS).
[40] Pham, N.T., Foo, E., Suriadi, S., Jeffrey, H., Lahza, H.F.M., 2018.Improving performance of intrusion detection system using ensemble methods and feature selection, in: Proceedings of the Australasian Computer Science Week Multiconference, ACM. p. 2. doi: 10.1145/3167918.3167951.
[41] C. Khammassi and S. Krichen, ''A GA-LR wrapper approach for feature selection in network intrusion detection,'' Comput. Secur., vol. 70,pp. 255–277, Sep. 2017.
[42] J. McCall, ''Genetic algorithms for modelling and optimisation,'' J. Comput. Appl. Math., vol. 184, no. 1, pp. 205–222, Dec. 2005.
[43] Mr. Ketan Sanjay Desale, Ms. Roshani Ade,"Genetic Algorithm based Feature Selection Approach for Effective Intrusion Detection System", International Conference on Computer Communication and Informatics,pp.1-6,2015.
[44] Chih-Fong Tsai, Y.-F. H.-Y.-Y. (2009). Intrusion detection by machine learning: A review. expert systems with applications,ELSEVIER .
[45] Dewan Md. Farid, M. Z. (2011). Adaptive Intrusion Detection based on Boosting and. International Journal of Computer Applications .
[46] W.-C. Lin, S.-W. Ke, and C.-F. Tsai, "CANN: An intrusion detection system based on combining cluster centers and nearest neighbors," Knowledge-based systems, vol. 78, pp. 13-21, 2015.
[47] Ganapathy S, Yogesh P, Kannan A, (2011), "An intelligent intrusion detection system for mobile ad-hoc networks using classification techniques", Computers and Communication Information Systems (CCIS), pp. 117-122.
[48] Ganapathy S, Yogesh P, Kannan A, (2012), "Intelligent agent-based intrusion detection system using enhanced multiclass SVM", Computational intelligence and neuroscience, Vol. 2012, pp. 1-9.
[49] Jaisankar N, Ganapathy S, Yogesh P, Kannan A, (2012), "Intelligent intrusion detection system using fuzzy rough set based C4. 5 algorithm", International ACM Conference proceedings on Advances in Computing, Communications and Informatics, pp. 596-601.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)