http://www.jctjournals.com ISSN(ONLINE):2278 – 3814

Volume-11, Issue-06, June, 2022
JOURNAL OF COMPUTING TECHNOLOGIES (JCT)
International Journal
Page Number: 01-07

A Literature Survey On Intrusion Detection Systems DoS attack detection Using Different Machine Learning

Jay Prakash Gawande,[1] Prof. Darshna Rai,[2]
[1]M.Tech Student Cyber Security, [2]Assistant Professor,
[1,2]Department of Computer Science and Engineering
[1,2]School of Research & Technology (SORT), People's University, Bhopal, INDIA
jaygawande0@gmail.com[1] darshanarai@peoplesuniversity.edu.in[2]

***Abstract*—Intrusion detection system (IDS) is regarded as the second line of defense against network threats. IDS DDoS discussed in this literature survey present on overview of existing techniques for detection DOS attacks. There are many techniques which are used to design IDSs for specific scenario and applications. Artificial intelligence techniques are widely used for threats detection. This paper presents a critical study on genetic algorithm, artificial immune, and artificial neural network (ANN) based IDSs techniques used in wireless sensor network (WSN). In the last decade there are different methods are presented in the area of IDS DODS detection in terms of cyber attacks. There are different cyber attacks are happened in on line portal and IaaS discussed in this paper. Also discussed the properties of IDS DDoS attacks. These properties are help to identify the D-DoS attack. Machine leaning algorithms are key elements for DDoS attack detection and presentation. In the survey discussed the different method which is based on ML algorithms.**

***Keywords*- Intrusion Detection Systems (IDS), Dempster-Belief theory (DBT),Host-based intrusion detection system (HIDS),Network primarily based Intrusion Detection (NIDS),artificial system (AIS),etc…**

I. INTRODUCTION

Computer security is a very important issue to any or all users of computer systems. Intrusion Detection Systems (IDS) technology is an efficient approach in handling the issues of network security. The main goal of Intrusion Detection System is to sight unauthorized use, misuse and abuse of computer systems by each systems insiders and external intruders. There are many ways wont to implement intrusion detection like applied mathematics analysis knowledgeable systems, and state transition approaches etc., and these many approaches relies on the system were projected in recent years[

Intrusion interference needs a well-selected combination of "baiting and trapping" aimed toward each investigations of attacker's. Abusive the intruder's attention from protected resource is another task of IDS. Knowledge generated by intrusion detection systems is fastidiously examined (this is that the main task of every IDS) for detection of potential attacks (intrusions) [2].

Intrusion detection is that the method of watching the events occurring during a automatic data processing system or network [2]. IDS will free form numerous tasks however identification of intruders is one among-st the foremost basic perform. It helps in gathering the proof in laptop crime.

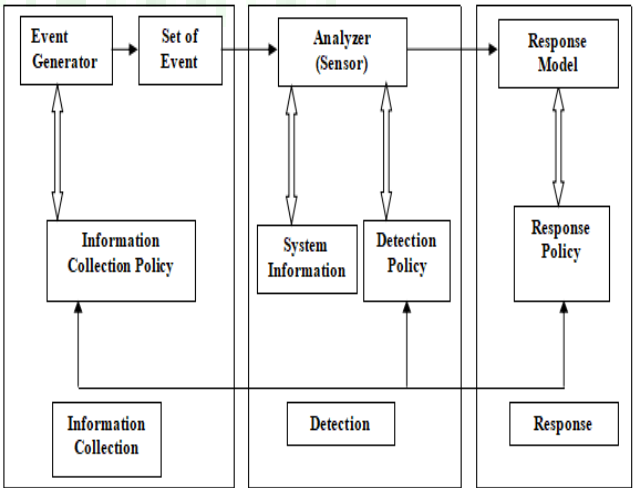

Figure 1: Components of IDS

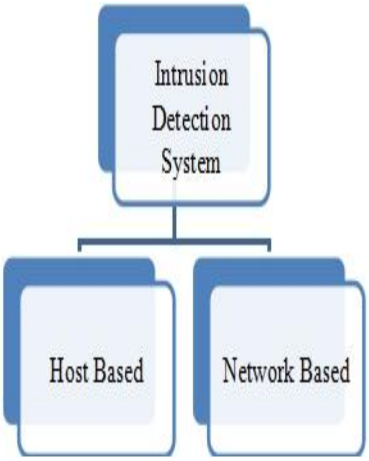

Figure 2: Classifications of IDS

.

A. Host-based intrusion detection system: HIDS value data found on a single or multiple host systems, together with contents of operational systems, system and application files.

B. Network primarily based Intrusion Detection: NIDS value data captured from network communications, analysing the stream of packets that travel across the network.

There are many completely different varieties of techniques wont to style Intrusion detection system. These embody applied mathematics anomaly techniques, mathematical logic techniques, rule-based anomaly techniques, rule-based penetration identification, state transition techniques, neural network primarily based, data processing techniques etc. [6].

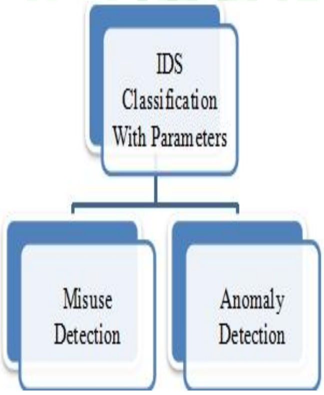

Figure 3. IDS classification with parameter

In the next section discuss the previous works that is presented by different researchers after that discuss the proposed method for multiple image super resolution in section III describe Section IV discusses the simulation and result parameters of the proposed method. Last but not least discuss the conclusion in section V

II. LITERATURE SURVEY

In this literature survey present on overview of existing intrusion detection techniques for detection DOS attacks. Intrusion detection system in a very popular and computationally expensive task.

Akgun, et.al. (2022). In this paper, we provide a new intrusion detection system that is based on deep learning models for DDoS attacks. We used CIC- DDoS 2019 dataset, which contains 12 classes, including a benign class. We tested various deep learning models such as DNN, CNN, and LSTM for various units per layer. We also improved the system using pre processing techniques such as feature elimination and selsection where we selected 40 important features out of 88. We obtained a new homogeneous data set by selecting an equal number of samples from each attack type with random subset selection. Afterward, we removed duplicate records to obtain a clean, non-repetitive data set which most relevant studies ignored. In this respect, this study presents two new data sets to the literature that directly affect the performance of the training processes produced from the CIC-DDoS 2019 data set. Finally, we applied min- max normalization processes to examine their effect on the performance. Therefore we produced applicable data by obtaining a normalized set containing an equal number of pre-processed samples from each attack type without duplicates [1].

Ullah, S., et.al. (2022).The extensive growth of smart vehicularnetworks has opened up several doors for cyber criminals. Attacks on intra-vehicle networks can cause deaths and severe accidents. This research proposes a hybrid DL-based model for intrusion detection in IoV. The presented scheme contains a hybrid combination of LSTM and GRU that reduces the training and response time. The performance of the proposed approach was evaluated by conducting extensive experiments on a combined dataset of CIC DoS 2016, CICIDS 2017, and CSE-CIC-IDS 2018, and car-hacking datasets. The experimental results demonstrate thatthe proposed model achieves 99.5% accuracy for the combined DDoS dataset and 99.9% for the car hacking dataset, respectively [2].

Saghezchi, et.al. (2022). In this paper, we applied ML for detecting DDoS attacks in Industry 4.0 CPPSs. Authors exported network traffic traces (PCAP files) from a real-world large-scale semiconductor production factory and employed 11 different semi-supervised, unsupervised, and supervised ML algorithms for anomaly detection in network traffic flows. The simulation results showed that supervised learning algorithms outperformed both unsupervised and semisupervised ones. In particular, DT, RF, and K-NN detected DDoS attacks with Accuracy =Recall = 0.999, Precision = 0.999, and FPR = 0.001.However, the two applied unsupervised algorithms (K-Means and EM) also showeda very good performance (Accuracy = 0.95, Recall > 0.9, Precision > 0.9, and FPR < 0.09),although their performance decreased significantly when the PCA algorithm was applied(even with 95% variance retain). This is an interesting finding, since unlike supervised learning, unsupervised learning does not require data labelling which is a tedious task in practice and needs a significant amount of human effort and intervention [3].

Mighan, et.al (2021)-In this researcher work, the literature reveals that as use of internet increases, intrusion detection is considered as an important security issue. Therefore, the main goal of this paper is to address scalable network intrusion detection in big data framework. Besides, one has to keep in mind that detection accuracy, time and cost are of importance, as well. Thus, the present study tried to use deep learning methods to improve diagnostic accuracy, decrease the error rate, improve prediction speed and save time and cost. This presented work a hybrid SAE–SVM scheme for a fast and efficient cyber security intrusion detection system. In the proposed system, a stacked auto encoder network was used as a feature extraction method and SVM as the classifier. The deep network platform outperformed other feature extraction methods. Also, the performance of the proposed framework was evaluated using the big data processing tool of Apache Spark and machine learning algorithms. We examined the performance of the proposed SAE–SVM scheme by reducing the 42-dimensional ISCX dataset to approximately 75% of its original size and then classified the reduced data by SVM in Spark **[4].**

Snehi, J., et.al (2021)- In this research work, The defense is the critical element of the computer system, and the most challenging issues are detecting the intrusion attacks. The IDS is the most critical cyber-security factor which can detect intrusion before, during, and after an attack. This works provides an overall IDS benchmarking which quantifies different IDS properties, types of anomaly-based IDS that are deployed in different environments or platforms, and comparison among them based on methods used, their details, and advantages of each method. In analyzed the different IDS techniques based on anomaly and various issues associated with anomaly-based IDSs. They addressed global environments for intrusion detection and framework for behavioral or anomaly-based intrusion detection systems and discussed the challenges facing anomaly-based IDSs. After reviewing the various anomaly-based IDS techniques, Then analyzed that successful detection rates could not be achieved by a single technique. To lower the false prediction rate and decreased the complexity of the process, an efficient automated hybrid technique is suggested for achieving accurate detection rates to enhance anomaly detection **[5].**

Liu, L., etr.al (2020)- In this presented work, As network intrusion continues to evolve, the pressure on network intrusion detection is also increasing. In particular, the problems caused by imbalanced network traf c make it difficult for intrusion detection systems to predict the distribution of malicious attacks, making cyberspace security face a considerable threat. This presented a novel Difcult Set Sampling Technique (DSSTE) algorithm, which enables the classification model to strengthen imbalanced network data learning. A targeted increase in the number of minority samples that need to be learned can reduce the imbalance of network trafc and strengthen the minority's learning under challenging samples to improve the classification accuracy. Then six classical classification methods in machine learning and deep learning and combined them with other sampling techniques. Experiments show that our method can accurately determine the samples that need to be expanded in the imbalanced network= trafc and improve the attack recognition more effectively **[6].**

Sarhan, et.al (2020)- In this researcher works, They community with four new NIDS datasets using Net Flow features. These datasets are to be used in ML-based NIDS training and evaluation stages. The datasets are showing positive results by achieving similar binary-class detection performance compared to the complete set of their respective original datasets. However, the NF-ToN-IoT and NF-CSE-CIC-IDS2018 datasets were inefficient when conducting multi-class detection experiments. Further feature analysis is required to identify the strength of each Net Flow feature, and how these datasets can be improved by adding key features from the original datasets to aid in the detection of missed attack types **[7].**

Kumar, V., et.al (2020)- In this research work, an integrated classification based IDS and evaluates its performance on offline traditional data set and on line real time data set. They evaluates the performance of presented model on a new data set (UNSWNB15) which covers the most recent attacks (DoS, Exploit, Normal, Probe, Generic) compared to KDD99 data set. It is observed that the value of several evaluation metrics (e.g. MFM = 84.5%, ADR = 90.32, FAR = 2.01% etc.) have higher performance compared to other existing traditional decision tree based models. Since the presented approach is based on the misuse-based technique so it is not able to detect any zero day attacks which are publicly unknown and hence there is no signature found for that attack. But once the attack is performed the signature is available to the proposed IDS model. Now our IDS model is updated with the signature to prevent the attacks of these categories. This works generates a real time data set at NIT Patna CSE lab (RTNITP18) and it acts as the testing data set to evaluate the performance of our proposed model. Accuracy of proposed model is 83.8%. It conclude that our proposed integrated model acts as the dog watcher in the network to prevent the systems of the organization from malicious attacks **[8].**

Gao, X., et.al (2019)- In this presented work, According to the theory that there is no free lunch, no learning algorithm is the best learner in any scenario. In the detection effect of single classification algorithm, the performance difference of each algorithm is not prominent. No matter what learning algorithm is adopted, a series of methods can be used to improve the detection effect. In this presented an adaptive ensemble learning model. The key idea of our model is to use ensemble learning to gather the advantages of different algorithms. The method of ensemble learning to improve the detection effect. Compared with other research papers, it is proved that our ensemble model effectively improves the detection accuracy. The accuracy of the adaptive voting algorithm we proposed is 85.2%, and the precision 86.5%, the recall 85.2%, the F1 84.9%, better than algorithms in Table 6. Compared with other algorithms of the same kind, the effect of the algorithm is obviously improved, and it has great practical value. Although deep neural network has some advantages in detection effect, it takes long time in our comparative experiment, which means it will lead to a long detection delay in the practical application scenario of broadband network which will affect the response time of attack detection. Although the effect of a decision tree is not as good as that of DNN, the result of our MultiTree algorithm is better than that of DNN algorithm. For imbalanced classification scenarios, adjusting the proportion of samples, setting different class-weights and choosing appropriate features can improve the accuracy of machine learning algorithm. In the subsequent practical applications in the field of intrusion detection, the primary goal is to improve the quality of training data as much as possible, optimize feature extraction and preprocessing methods, and make the data more separable. In addition, for a small number of types of attacks such as U2R, separate optimization methods should be considered to improve the detection capability of such high-level threat attacks. Ensemble machine learning has a good generalization effect, which is worthy of continuous promotion and optimization in the field of network security research and application **[9].**

Kaja, N., et.al (2019)- In this presented work, In initially provided a background in intrusion detection systems and their importance in the cyber security space. Then, a standardized dataset was analyzed and pre-processed using variance, correlation coefficients, Least Square Regression Error and Maximal Information Compression Index. Pre-processing the data was necessary to reduce the number of features and help with avoiding bias and over fitting. After such pre-processing, the data was used to build an intelligent, two-stage intrusion detection system. The first stage uses the K-means algorithm to detect an attack. The second stage tests four different supervised learning algorithms (J47, Random Forest, Na¨ıve Bayes, and Adaptive Boosting) to classify the attacks. After building and testing the two-stage model we achieved a high accuracy in performance results. In addition, the In IDS able to fully eliminate the number of false positives which are usually a syndrome of anomaly-based intrusion detection systems. Lastly, as compared the performance results from this proposed IDS with other state of the art research work. Based on the comparison it showed that results generated from this IDS are one of the best performance results achieved using the KDD dataset **[10].**

III. INTRUSION DETECTION SYSTEMS BACKGROUND

In this paper tend to offer the detail of theoretical background for planning intrusion detection systems (IDSs). This chapter starts with a classification of intrusion detection techniques. Next, it reviews the utilization of artificial immune systems, and explains however the desperate belief theory helps for the detection and interference in intrusion detection system.

A. MACHINE LEARNING (ML)

This is described as a type of machine learning. It is also the research of software projects to improve continuously using knowledge or the utilization of information. Algorithms build a model statistical inference, commonly called as “ "learning algorithm," in order to collect information and outcomes instead of being supervised machine learning. Algorithms were applied inside a variety of uses, like health, web filtering, natural language processing, as well as machine vision, because creating simple equations to be doing the necessary tasks is virtually impossible[30]**.** Learning is a form of analysis of data which it facilitates that construction for simulation solutions. It's just a subfield of AI based on the notion concept machines must study from material, understand trends, as well as decide with little or no user input.

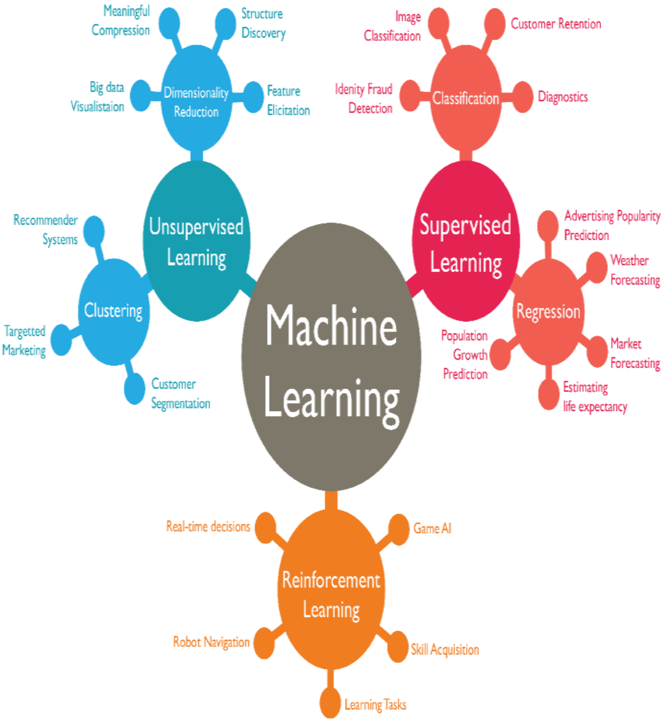

Fig.4 Machine Learning[31].

C. ARTIFICIAL INTELLIGENCE (AI)

Artificial intelligence (AI) AI, or artificial intelligence, is the ability of machines to learn to act and think like humans. Artificial intelligence can also be used to describe any computer that shows signs of intelligence like learning and problem solving.

AI's finest quality is the capacity to reason and take actions that are most likely to lead to the achievement of a certain objective. Software that can learn from as well as adapt to new information on its own, without human intervention, is considered a subset of artificial intelligence (AI). Because of the massive volumes of unstructured information that deep learning algorithms can process on the fly, this kind of autonomous learning is possible.

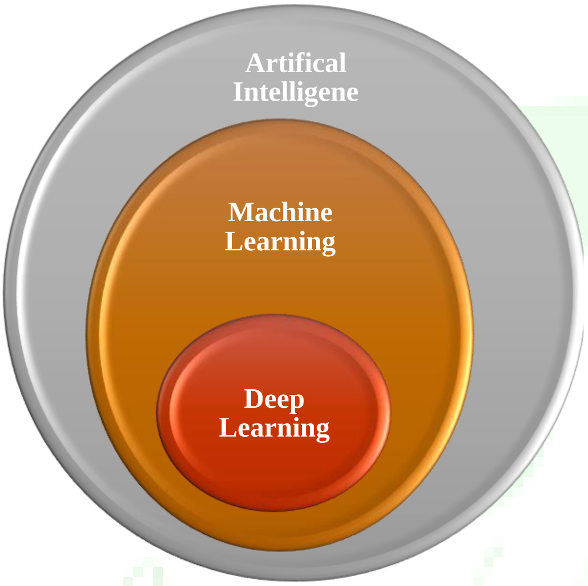

Fig. 5 Artificial intelligence, Machine learning and Deep learning.

IV. RESULT PARAMETERS

A. Designs Several Specification Modules

It must round the processing mechanism when the system works normally and access to the network bottom layer directly. First, set the working mode of network card as promiscuous mode to make it receive data packets on target MAC address not its own MAC address and then access to the data link layer directly to capture relevant data. There are many classification metrics for IDS, some of which are known by multiple names.

IDS are typically evaluated based on the following standard performance measures:

- True Positive Rate (TPR): It is calculated as the ratio between the number of correctly predicted attacks and the total number of attacks. If all intrusions are detected then the TPR is 1 which is extremely rare for an IDS. TPR is also called a Detection Rate (DR) or the Sensitivity. The TPR can be expressed mathematically as

$$TPR = \frac{TP}{TP + FN} \quad (1)$$

- False Positive Rate (FPR): It is calculated as the ratio between the number of normal instances incorrectly classified as an attack and the total number of normal instances.

$$FPR = \frac{FR}{FP + TN} \quad (2)$$

- False Negative Rate (FNR): False negative means when a detector fails to identify an anomaly and classifies it as normal. The FNR can be expressed mathematically as:
-

$$FNR = \frac{FN}{FN + TP} \quad (3)$$

- Accuracy (AC): The AC measures how accurate the IDS is in detecting normal or anomalous traffic behavior. It is described as the percentage of all those correctly predicted instances to all instances:
-

$$AC = \frac{TP + TN}{TP + TN + FP + FN} \quad (4)$$

V. IDS D-DOS ATTACK DETECTION TECHNIQUES

DDoS attacks have been studied for a long time and the types of threats to them are mostly known.5 However, SDN is a new architecture and the studies are at an early stage. In addition, SDN networks have distinct detection methods for different types of DDoS attacks.23 These methods include entropy-based,7,24-26 machine learning–based,10-13 traffic pattern analysis,27 connection rate,27,28 and techniques that combine the use of the IDS and OpenFlow.29-31

1. **Entropy** The ability to measure randomness in packets arriving on a network makes entropy-based methods good candidates for the DDoS detection. The greater the randomness, the greater the entropy, and vice versa. Entropy-based methods depend on network feature distributions to detect anomalous network activities.24 The presence of anomalies in an SDN network can be identified by adopting the use of predefined thresholds. In addition, probability distributions of various network features such as source IP address, destination IP address, and port numbers are used to calculate the entropy.32

2. **Machine learning** Machine learning–based methods employ techniques to detect anomalies in a network environment, these can be based on models, based on statistic and math, based on unsupervised machine learning algorithms, and based on supervised machine learning algorithms.33 These algorithms take into account various network features and traffic characteristics to detect the presence of anomalies. In fact, any system that is built to detect any anomalies in the network catch the traffic on it and extract some kind of information from them, and the approach that uses machine learning is trying to catch the pattern of normal and abnormal traffic on the network, without the need to know the pattern itself

3. **Traffic pattern** analysis These techniques work on the assumptions that the infected hosts exhibit similar behavioral patterns that are different from benign hosts.34 Therefore, it analyzes the traffic relating to the metrics of the attack pattern networks in order to identify the attacker or the target under attack. Patterns are observed as a result of a command that is sent to many members of the same botnet causing a similar behavior (eg, sending illegitimate packets, starting to scan).

Connection rate Bawany et al32 define connection rate techniques as ‘‘the probability of a connection attempt being successful should be much higher for a benign host than a malicious host.’’ Whenever the likelihood ratio for a host to exceed a certain threshold, it is declared as infected. These techniques are classified into two types: connection success ratio and connection rate, which refers to the number of connections instantiated within a certain window of time.

VI. CONCLUSION

In this research work researcher presented different method used on IDS DDOS attack detection using different machine learning approach. In the last decade there are different methods are presented in the area of IDS DODS detection in terms of cyber attacks. There are different cyber attacks are happened in on line portal and IaaS discussed in this paper. Also discussed the properties of IDS DDoS attacks. These properties are help to identify the D-DoS attack. Machine leaning algorithms are key elements for DDoS attack detection and presentation. In the survey discussed the different method which is based on ML algorithms.

REFERENCES

1. Akgun, Devrim, Selman Hizal, and Unal Cavusoglu. "A new DDoS attacks intrusion detection model based on deep learning for cybersecurity." Computers & Security 118 (2022): 102748.
2. Ullah, Safi, Muazzam A. Khan, Jawad Ahmad, Sajjad Shaukat Jamal, Zil e Huma, Muhammad Tahir Hassan, Nikolaos Pitropakis, and William J. Buchanan. "HDL-IDS: a hybrid deep learning architecture for intrusion detection in the Internet of Vehicles." Sensors 22, no. 4 (2022): 1340.
3. Saghezchi, Firooz B., Georgios Mantas, Manuel A. Violas, A. Manuel de Oliveira Duarte, and Jonathan Rodriguez. "Machine learning for DDoS attack detection in industry 4.0 CPPSs." Electronics 11, no. 4 (2022): 602.
4. Mighan, Soosan Naderi, and Mohsen Kahani. "A novel scalable intrusion detection system based on deep learning." International Journal of Information Security 20, no. 3 (2021): 387-403.
5. Snehi, Jyoti, Abhinav Bhandari, Manish Snehi, Urvashi Tandon, and Vidhu Baggan. "Global intrusion detection environments and platform for anomaly-based intrusion detection systems." In Proceedings of Second International Conference on Computing, Communications, and Cyber-Security, pp. 817-831. Springer, Singapore, 2021.
6. Liu, Lan, Pengcheng Wang, Jun Lin, and Langzhou Liu. "Intrusion detection of imbalanced network traffic based on machine learning and deep learning." IEEE Access 9 (2020): 7550-7563.
7. Sarhan, Mohanad, Siamak Layeghy, Nour Moustafa, and Marius Portmann. "Netflow datasets for machine learning-based network intrusion detection systems." In Big Data Technologies and Applications, pp. 117-135. Springer, Cham, 2020.
8. Kumar, Vikash, Ditipriya Sinha, Ayan Kumar Das, Subhash Chandra Pandey, and Radha Tamal Goswami. "An integrated rule based intrusion detection system: analysis on UNSW-NB15 data set and the real time online dataset." Cluster Computing 23, no. 2 (2020): 1397-1418.
9. Gao, Xianwei, Chun Shan, Changzhen Hu, Zequn Niu, and Zhen Liu. "An adaptive ensemble machine learning model for intrusion detection." IEEE Access 7 (2019): 82512-82521.
10. Kaja, Nevrus, Adnan Shaout, and Di Ma. "An intelligent intrusion detection system." Applied Intelligence 49, no. 9 (2019): 3235-3247.
11. Chawla, Ashima, Brian Lee, Sheila Fallon, and Paul Jacob. "Host based intrusion detection system with combined CNN/RNN model." In Joint European Conference on Machine Learning and Knowledge Discovery in Databases, pp. 149-158. Springer, Cham, 2018.
12. Dias, L. P., Jés de Jesus Fiais Cerqueira, Karcius DR Assis, and Raul C. Almeida. "Using artificial neural network in intrusion detection systems to computer networks." In 2017 9th Computer Science and Electronic Engineering (CEEC), pp. 145-150. IEEE, 2017.
13. Rodda, Sireesha, and Uma Shankar Rao Erothi. "Class imbalance problem in the network intrusion detection systems." In 2016 international conference on electrical, electronics, and optimization techniques (ICEEOT), pp. 2685-2688. Ieee**,** 2016.
14. Farhoud Hosseinpour, Kamal rulnizam Abu Bakar, Amir Hatami Hardoroudi, Nazaninsadat Kazazi, “Survey on Artificial Immune System as a Bio-inspired Technique for Anomaly Based Intrusion Detection Systems” International Conference on Intelligent Networking and Collaborative Systems, IEEE , pp 323-324,Nov-2010.

15. D. Barbara, N. Wu, and S. Jajodia, “Detecting novel network intrusions using bayes estimators,” Proceedings of the First SIAM International Conference on Data Mining (SDM 2001), Chicago, USA, Apr. 2001.
16. Chung-Ming Ou, Yao-Tien Wang C.R. Ou , “Intrusion Detection Systems Adapted from Agent-based Artificial Immune Systems”, International Conference on Fuzzy Systems , IEEE, pp 115 -122,2011.
17. SazzadulHoque, Md. Abdul Mukit and Md. Abu Naserbikas, “An implementation of intrusion detection System using genetic algorithm”, International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, pp 109-120, March 2012.
18. Mattew A. Bishop, “Computer Security: Art and Science”, Addison Wesley Longman Publishing co., pp: 1120, New York, NY, USA, 2002.
19. William Stallings, “Cryptography&Network Security Principles & Practices”, Intrusion Detection (pp.571) (3rd Edition, 2003).
20. Eshghi Shargh, “Using Artificial Immune System on Implementation of Intrusion Detection Systems”, Third UK-Sim European Symposium on Computer Modelling and Simulation, IEEE, pp164-168, Nov-2009.
21. Xuanwu, Zhou, “Evolutionary Algorithm and its Application in Artificial Immune System”, Second International Symposium on Intelligent Information Technology Application (IITA-08), Vol: 3, pp.32-36, Dec- 2008.
22. H. Debar, A. Wespi, “Aggregation and Correlation of Intrusion-Detection Alerts”, the Fourth workshop on the Recent Advances in Intrusion Detection(RAID), LNCS 2212, pp 85-103,2001.
23. Julie Green smith, Jamie Twycross and UweAickelin, “Dendritic Cells for Anomaly Detection”, IEEE Congress on evolutionary Computation, IEEE, pp664-671,July-2006.
24. Emma Hart, Jon Timmis, “Application areas of AIS: The past, the present and the future”, Applied soft computing science direct, Vol: 8,Issue: 1, pp 191-201,2008.
25. Lu Hong, "Immune Mechanism Based Intrusion Detection Systems”, International Conference on Networks Security, Wireless Communications and Trusted Computing, vol.2,pp.568-571April-2009.
26. Wei Hu, Jianhua Li QiangGao, “Intrusion Detection Engine Based on Dempster-Shafer's Theory of Evidence”, International Conference on Communication, Circuit and System Proceedings, Vol: 3, IEEE, pp1627-1631, June-2006.
27. D. Dasgupta, “Immunity-based intrusion detection system: a general framework”, Proceeding of the 22nd National Information Systems Security Conference (NISSC), pp.147-160, 1999.
28. Matzinger. P, “Tolerance, Danger and the Extended Family”, Annual Review in Immunology, vol.12, pp. 991-1045,April-1994.