A Survey On Intrusion Detection System (IDS) Using Machine Learning Algorithms

Abdulla Alali*, Maria Yousef**

**Department of Computer Science, Isra University, Jordan.*
***Department of Computer Science, Al-al Bayt University, Jordan.*

ABSTRACT:

Nowadays, the usage of the internet is growing rapidly which leads to different security problems in the network. Security threat indicates violating the integrity and confidentiality of the systems thereby the organizations may suffer a financial loss. Hackers get access to the system and bypass the authentication procedure to extract financial and personal data from their victims' databases. As a result, detection of security threats, also known as intrusion detection, has become an essential issue in network, data, and information security. An intrusion detection system (IDS) is designed to detect and classify various threats. It divides attacks into two categories: normal and abnormal. Generally, IDS are based on either a host or a network. A variety of data mining approaches and machine learning techniques are widely employed by IDS. in this study, a survey on intrusion detection systems is offered. The survey focused on the methodologies employed in IDS, in addition to a thorough understanding of the strengths and limits of detection methods, which serves as a basis for the development of effective IDS.

Keywords: *IDS, Data Mining, Network-Based, Host-Based, Machine Learning*.

1. INTRODUCTION:

The internet plays a critical role in today's society. It is used in all aspect of our life including: education, business, social networking , shopping, etc. Currently, the reliance of using the internet and computer systems in day-to-day life has led to serious problems related to privacy, security, and confidentiality due to the procedures involved in the electronic transformation of data. This increases the possibility of criminals accessing computer systems connected to the Internet **(Sharma et al., 2015).**

Because of the internet accessibility, a new type of criminal has emerged: cyber-crime **(Hunton, 2012)**. Cybercriminals attack systems and applications to obtain unauthorized access to data, misuse data, or decrease the information's availability to authorized users. As a consequence, Companies suffer huge financial losses, in addition to losing their customers' trust. According to **(Zanero et al, 2004)**, theft of information increased by 250 % between 1991 and 1996, with 99 % of all significant companies reporting at least one main security intrusion and 10 billion dollars lost in the United States due to Scams involving telecommunications and computers.

The term "security threat" refers to a system's integrity and confidentiality being breached, potentially resulting in financial loss for the company (Vinayakumar et al., 2019). Cybercriminals intrude into the system by circumventing the authentication mechanism to steal professional and personal information from their victims' databases. An intruder is "a system, program, or human that attempts and achieves in getting into an information system or performing an illegal conduct". Generally, there always will be an invisible hackable weakness in the system According to protocols, design, and programming mistakes in application programs, and software platforms. As a result, we require a way to identify intrusions as quickly as feasible and respond appropriately. Although much work has been made into improving the security and privacy of computer systems, these issues still remain; in fact, no system in the world is totally secure **(Dhanabal et al., 2015)**.

Various approaches have been developed for controlling unauthorized access to the system. One of the proposed solutions for detecting this incursion is the IDS (Intrusion Detection System). An IDS can monitor computer or network traffic and detect malicious behaviors that affect the confidentiality, availability, and integrity of information sources, as well as alert the system or network administrator from malicious attacks **(Almseidin et al., 2017)** . IDS can be a hardware or software appliance that monitors internet traffic and identifies threats. The aim of an IDS (Intrusion Detection System) is to identify any suspicious activity on the system. Based on the available resources, this system determines if the unauthorized user's activities are intrusive or regular. Anomaly detection and misuse strategies are the two most popular strategies used in IDS systems.

In this paper, we present a summary of the evolution of the research related to the IDS as well as a variety of machine learning algorithms suggested to detect different types of attacks. We studied a variety of intrusion detection methods employed by researchers. The paper addressed numerous studies on the use of machine learning algorithms in intrusion detection systems that were published between 2015 and 2020.

The remainder of the paper is laid out as follows: Part two covers attack types, a review of IDS, different types of detection, and how IDS works in general. The third part summarizes a number of previous studies and compares them. The comparisons were based on the classifier used, the performance of the methods and the dataset used to test the algorithms. The final part of this article explores the future of IDS development utilizing machine learning approaches.

2. BACKGROUND

2.1. TYPES OF ATTACK

Attacks can be classified into four kinds, according to the classification suggested by (Garnaev et al., 2014):

1. **Denial of Service (DoS):** DoS is an attack that aims to make a network resource or machine in which the hacker attempts to make a computer system too busy or overburdened to respond to its intended recipient. **(Jamal et al., 2018)**. Teardrop, Smurf, Ping of Death, Back, Land, Neptune, and others are examples of DoS attack.
2. **User to Root(U2R):** U2R attack attempts to obtain superuser accessibility to a computer system. This type is an exploit in which the hacker logs in as a normal user and then tries to gain superuser privileges by taking use of vulnerabilities in the application software or operating system. Before beginning an assault, the purpose of this form of attack is to get access to all network data **(Bahl et al., 2015)**. A buffer overflow attack is the most common type of attack in this category. Examples include: Perl , Loadmodule, Ps, Xterm and other attacks.
3. **Remote to User:** this attack occurs when an attacker attempts to obtain unauthorized authentication to the target system's superuser account from a remote machine. In this approach, the attacker transmits packets over a network to a system, then uses a vulnerability to earn local access as a user of that machine **(Paliwal et al., 2012)**. Dictionary, Guest, Ftp write, Phf, Imap, and other remote to user attacks are examples.

4. **Probing**: An attacker explores a network of computers for data or known flaws in this form of assault. An attacker who knows which devices and services are on the network can use this information to look for flaws. This information will be used to plan future assaults (Wang et al., 2017). There are numerous probing attack tools available that can be employed by even the most inexperienced attacker. Ipsweep, Nmap, Mscan, Satan, Saint, and other probing attacks are examples..

2.2. INTRUSION DETECTION SYSTEM

An intrusion is described as an attempt to effects the availability, confidentiality, integrity, or illegal employment of resources of a network or computer system by bypassing its mechanisms of security. IDS (intrusion detection system) is a type of software that checks for malicious activity and illegal activities on a computer system. The database administrator is notified of any such action that occurs. An IDS operates by tracking system activity via observing the system vulnerabilities, and the integrity of files and analyzing patterns. It constantly monitors the Internet for new threats that could lead to an assault.

The following are the objectives of IDS:

- monitored and analyzed both system and user activities.
- Detect unusually activities.
- Ability to identify patterns of attacks.
- Analyzed vulnerabilities and configurations of the system.
- Checked for security policy violations.
- Correcting system configuration errors.

2.3. TYPE OF IDS

The classification of intrusion detection systems depends on two main parameters, as shown in the figure-1:

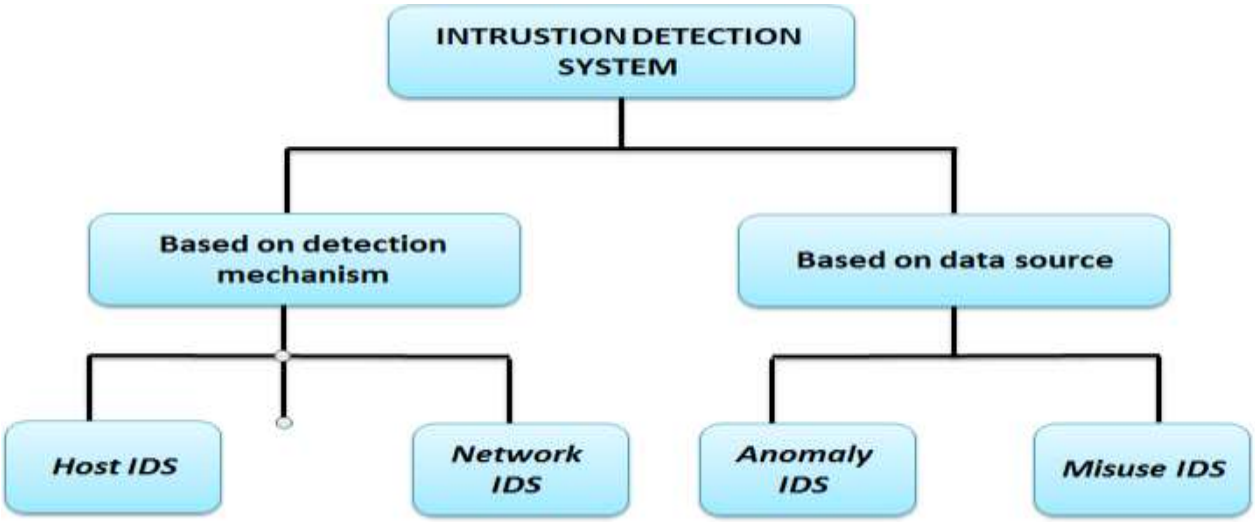

Figure - 1. Type of IDS

1. Based on detection mechanism:

A. Anomaly IDS: In an anomaly-based intrusion detection approach, the system first learns the system's or network's typical behavior or activities before detecting the intrusion. According to this strategy, behaviors differing from behaviors considered "normal" are assumed to be attacks, and anomaly detectors calculate the deviation to detect these attacks **(Gupta, 2015).** Anomaly detectors use normal behaviors to create profiles of individuals, servers, and network connections. These profiles are created from data that is considered normal. Following the profile construction, detectors track fresh event data, compare it to the profile, and look for deviations.

B. Misuse IDS: In most cases, misuse (signature-based) detection is employed to detect known threats. All known dangers must first be defined, and information about these threats must then be given to the IDS. As a result, the IDS can compare all input and output activity to all possible attacks in its knowledge base and notify if any action matching data in the knowledge base. in this type, Signatures are the names given to the data recorded in this knowledge base **(Papamartzivanos et al., 2019)**. Simple string matching, which involves looking for unique key phrases in network traffic to identify attacks, to more complex ways such as rulebased matching, which defines an attack's behavior, are some of the methods for actually comparing a signature with an attack.

2. Based on data source:

C. Host IDS: Intrusion detection can be performed on the hosts which need to be protected, or it can be done on a network device that can monitor traffic from across all network hosts. IDS can be classified into two types based on their installation locations: host-based IDS and network-based IDS. The data collected by the HIDS (host-based intrusion detection and prevention system) is analyzed on the localhost or system software where it is implemented. It examines real system calls as well as system logs. NIDS (Network-based Intrusion Detection System) examines the network packets as they travel throughout the network **(Martins et al., 2022)**. In this traffic, it searches for known signs of informative action. Because NIDS analyzes network traffic, any assault signatures found may or may not be successful. NIDS typically have trouble distinguishing between successful and unsuccessful attacks, if not impossible.

D. Network IDS: At specific points in the network, NIDS (Network Intrusion Detection Systems) keep track of traffic to and from all connected devices. It examines the traffic of network and compares it to a database of known threats. An warning is provided to the administrator if an assault is detected or if any unusual activity is observed. On-line and off-line NIDS are the There are different type of NIDS. On-line NIDS works with network real time data, whereas off-line NIDS works with data that has been saved **(Koutsandria et al., 2014)**.

3. COMPARISON OF LITERATURE REVIEW:

Many researchers in the field of security intrusion detection have used machine learning methods such as Decision Tree, Support Vector Machine, Random Forest, etc. to classify activities on the system into normal or abnormal. This section provides a summary of a group of previous studies in this field. The comparison of related work is shown in Table 1.

(Lin et al., 2015) introduced a novel model, named the cluster center and nearest neighbor (CANN) strategy, Two distances are assessed in this study: the first is the distance between each data sample and its cluster center, and the second is the distance between the data set and its nearest neighbor in the same group. Then, for intrusion detection, a k-Nearest Neighbor (k-NN) algorithm employs this new one-dimensional distance-based feature to describe every sample data. The CANN classifier surpasses both SVM and KNN in classification performance, detecting, and error rates, according to experimental results based on the KDD-Cup 99 dataset.

In the paper presented **(Amira et al., 2017)**, The authors attempted to assess machine learning methods' abilities in the detection of network intrusion. In this study, six machine learning algorithms including BFTree, NBTree, J48, RFT, MLP, and NB are employed to determine the most suitable algorithem for providing additional knowledge about available attacks and predicting the type of attacks. The results of the experiments revealed that the DT classifier outperforms other classifiers.

(Farnaaz et al., 2016) attempt to detect and notify if the user's activities are abnormal (or normal) behavior. The authors of this study developed a new intrusion detection model utilizing a random forest method to detect four different types of attacks: probe, R2L, U2R, and DOS. To evaluate the ability of this model, the authors executed experiments based on the KDD-NSL dataset KDD-NSL is a new version of the KDD'99 data set that has 42 features and proposes solutions to some of the data set's inherent difficulties. This is a useful benchmark data set for academics to use when comparing different IDS.

(Zhou et al., 2020) addressed high-dimensional and unbalanced network traffic problems by suggesting a novel intrusion detection model, which is based on the feature selection approach and ensemble learning techniques. In the first stage of this study, a heuristic algorithm named CFS BA has employed to select the best subset of features based on the correlation between features. The authors then present an ensemble technique that combines the algorithms C4.5, Random Forest (RF), and Forest by Penalizing Attributes (Forest PA). Finally, for attack recognition, the voting mechanism is utilized to aggregate the probability distributions of the base learners. The experimental findings are promising, with a classification accuracy of 99.81 percent, 99.8 percent DR, and 0.08 percent FAR using a subset of 10 features for the NSL-KDD dataset, and an accuracy of 99.52 percent and 0.15 percent FAR with a subset of only 8 features for the AWID dataset. Surprisingly, our model obtains the greatest accuracy of 99.89% and DR of 99.9% on the CIC-IDS2017 dataset's subset of 13 features.

(Kumar et al., 2020) proposed system introduces a miss-behavior analytical system that is abnormal detection using various base algorithms such as Bayes method, decision tree, random forest, RNN, and LSTM, which are all combined to represent as ensemble-based voting algorithm. When comparing our proposed approach to Multi-tree algorithm, the accuracy of our proposed work is 85 percent, whereas the existing approach yields 79.2 percent. The results suggest that our proposed system outperforms the current system.

The role of an IDS is to defend a network from potential intrusions. Feed Pattern Recognition and Feed Forward Neural Networks are developed and evaluated for the identification of multiple threats in this research paper **(Iqbal et al., 2019)** the authors used a modified KDD Cup99 dataset. The Artificial Neural Networks are trained using Scaled Conjugate Gradient training functions and Bayesian Regularization. Accuracy, Rsquared, MCC, MSE, AROC, FAR, and DR are some of the performance indicators used to evaluate the recommended Neural Network Models. According to the findings, both systems surpassed others in evaluation metrics on various attack detections.

Based on Artificial Bee Colony (ABC) and Artificial Fish Swarm (AFS) algorithms, **(Hajisalem et al., 2018)** developed a novel hybrid ABC-AFS detection model. The Correlation-based Feature Selection (CFS) and Fuzzy C-Means Clustering (FCM) techniques are utilized in this work to partition the training set and eliminate unneeded characteristics. Moreover, If-Then instructions are constructed using the CART method based on the chosen features differentiate between normal and abnormality records. Likewise, the generated rules have been used to train the hybrid technique that has been proposed. In terms of detection rate and false-positive rate, two well-known datasets, UNSW-NB15 and KDD-NSL, were utilized to validate the suggested technique.

Another attempt to compare machine learning algorithms in detection network attacks is done by **(Raviteja, 2020)**. A comprehensive survey of important techniques used in detection the type of intrusion is offered in this work. Techniques based on the Random Forest algorithm have been created, as well as classification methods include Logistic Regression, Decision Tree, and Support Vector Machine. According to the findings of the experiments, the Random Forest classifier is the most acceptable method because it has d achived highest accuracy of classification. When comparing execution times, the Random forest classifier chooses the one with the shortest execution time.

There are several machine learning algorithms used to prevent and detect the different types of protection attacks. **(Lee et al., 2017)** provide a study in which they use various machine learning approaches with information entropy computation to the Kyoto 2006+ data set and assess their effectiveness. According to the findings, many machine learning methods produce higher than 90% precision, recall, and accuracy for this data set. However, we find that the Radial Basis Function (RBF) beats the other seven methods in this study when using the area under the Receiver Operating Curve (ROC) measure.

(Gharaee et al., 2016) present and construct an IDS by using genetic algorithm to detect various forms of network intrusions quickly. The author employed the standard KDD99 benchmark dataset to develop and measure the performance of this system, and they were able to get a satisfactory detection rate. The author utilized the standard deviation equation with distance to determine chromosomal fitness. GA parameters and evolution mechanisms are thoroughly discussed and implemented. This method applies evolutionary hypothesis to information transition to filter traffic data and thereby minimize complexness.

(Gaikwad et al., 2015) proposed a novel IDS based on machine learning ensemble methods. This system is implemented using the Ensemble Bagging approach and REPTree as the foundation class. GA algorithm used in the feature selection step to select the optimal features from the NSL_KDD dataset is selected by using the GA algorithm to enhance the accuracy and decrease the false positive rate. The suggested ensemble model performance is measured in terms of False Positives rate, classification accuracy, and model construction time. The Bagging ensemble using the REPTree base class has the best classification accuracy, according to the results. The Bagging method has the advantage of taking less time to construct the model. The proposed ensemble method has a reduced false-positive rate in comparison to existing machine learning techniques.

Table : 1 Comparison of the related works.

Studies	Algorithms used	Dataset used	Accuracy	Finding of the study	Limitations
(Lin et al., 2015)	CANN KNN SVM	KDD-Cup 99	SVM:80% KNN:93% CANN:99%	Introduce a new method of theme selection to improve classification accuracy for intrusions and regular traffic	A few malicious traffic managed to get through the cracks.
(Aziz et al., 2017)	NBTree BFTree RFT J48 NB MLP	KDD-NSL	NBTree: 98% BFTree: 98% RFT: 98% J48: 97% NB: 84% MLP: 98%	A significant drop in FP (folse positive alarms)	To assess the work, new datasets should be used.

(Farnaaz et al., 2016)	RF	KDD-NSL	99%	Achived a high rate of detection for different types of attack	To decrease the complexity experienced throughout execution, attribute selection methods must be used.
(Zhou et al., 2020)	Combination of Forest PA, RF, and C4.5	KDD-NSL AWID CIC-IDS2017	KDD-NSL:99.8% AWID: 99.5% CICDS2017: 99%	The work was evaluated using a variety of datasets, therefore it was highly effective.	In one of the datasets used, FPR is observed.
(Kumar et al., 2020)	RNN-LSTM DT RF BC	KDD-NSL	85%	Handel the high dimensionality problem	The model must be evaluated with recent datasets.
(Iqbal et al., 2019)	FFANN PRANN	KDD-NSL	FFANN=98.0792% PRANN=96.6225%	Hybridization of multiple ML classifiers often aids in achieving high accuracy.	The model must be evaluated with recent datasets.
(Hajisalem et al., 2018)	Hybrid ABC-AFS	KDD-NSL	99%	The results of this study show that the hybrid strategy outperforms similar techniques previously used.	High execution time
(Raviteja, 2020)	DT LR RF SVM	KDD-NSL	RF=73% DT=72% SVM=71% LR=68%	The RF classifier aids in the reduction of execution time.	When alternative classifiers are applied, The model is unable to replicate its results.
(Lee et al., 2017)	KNN K-Means SVM FCM RBF NB	Kyoto2006+	KNN: 97.5% K-Means:83.6% SVM:94.2% FCM:83.6% RBF: 97.5% NB:96.7% Ensemble: 96.7%	kyoto2006+ was used to assess the job.	Low Recall

(Gharaee et al., 2016)	GA	KDD‟99	99%	Achieved high detection accuracy	More recent datasets should be used to test the strategy.
(Gaikwad et al., 2015)	(GA), Bagged Classifier with partial decision tree	KDD-NSL	99%	Achieved high detection accuracy	High execution time

4. DISCUSSION AND FUTURE WORKS

Table 1 shows that hybrid models outperform single models in terms of predicted accuracy and detection rates. In order to increase the performance of IDSs, the following challenges have been identified for future research and must be addressed:

1. Single machine learning algorithms act well but when more than one machine learning algorithms are mixed in a certain way, the classification accuracy and detection rate increase significantly, hence the combination and hybrid ML classification methods should be adopted frequently in future studies.
2. More models must be constructed in the future so that they can successfully operate on a variety of databases. Certain algorithms perform better on specific datasets only.
3. Some studies looked at did not use feature extraction before the categorization process, whereas others did. To enhance the reliability and accuracy of IDS, all redundant, irrelevant and unnecessary features must be deleted; feature selection must be recommended for future study.
4. The majority of the previous strategy is based on a two-class classification system (normal and attack) (to the best of our knowledge). Multiple class categorization (five-class, four assault classes, and one normal class) as shown in [26][27] has received very little attention. As a result, future studies on the classification of multiple classes can be expanded.

Most of the studies reviewed between 2015 and 2020 used the KDD-NSL
database in building the model. The most current and edited databases should be utilized to assess the methods used to deal with current incursions and risks.

Conclusion:

In this study, we present an summary of the concept of IDS and the types that are used to identify different types of attacks in networks and systems. The protection of data in systems is a main problem to authors. IDS and methodology work has been a prominent focus of research in the field of information security. In this study, we describe how research on intrusion detection systems has progressed, as well as numerous approaches and machine learning algorithms that have been presented for detecting different threats. However, there are major gaps in the existing intrusion detection system. As a result, the survey's future work must focus on developing a system that can effectively and accurately distinguish unexpected threats. We wish that this study will supply useful insights, a broad summary, and new research trends in this field to the readers.

References:

Almseidin, M., Alzubi, M., Kovacs, S., & Alkasassbeh, M. (2017, September). "Evaluation of machine learning algorithms for intrusion detection system", In 2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY),000277-000282.

Aziz, A. S. A., Sanaa, E. L., & Hassanien, A. E. (2017). "Comparison of classification techniques applied for network intrusion detection and classification", Journal of Applied Logic, 24, 109-118.

Bahl, S., & Sharma, S. K. (2015, May). "Detection rate analysis for user to root attack class using correlation feature selection", In International Conference on Computing, Communication & Automation, 66-71.

Dhanabal, L., & Shantharajah, S. P. (2015). "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), 446-452.

Farnaaz, N., & Jabbar, M. A. (2016). Random forest modeling for network intrusion detection system. Procedia Computer Science, 89, 213-217.

Gaikwad, D. P., & Thool, R. C. (2015). Intrusion detection system using bagging with partial decision treebase classifier. Procedia Computer Science, 49, 92-98.

Garnaev, A., Baykal-Gursoy, M., & Poor, H. V. (2014). "Incorporating attack-type uncertainty into network protection", IEEE Transactions on Information Forensics and Security,

9(8), 1278-1287.

Gharaee, H., & Hosseinvand, H. (2016, September). A new feature selection IDS based on genetic algorithm and SVM. In 2016 8th International Symposium on Telecommunications (IST) (pp. 139-144). IEEE.

Gupta, S. (2015, October). "An effective model for anomaly IDS to improve the efficiency", In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT) (pp. 190-194). IEEE.

Hajisalem, V., & Babaie, S. (2018). A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection. Computer Networks, 136, 37-50.

Hunton, P. (2012). "Data attack of the cybercriminal: Investigating the digital currency of cybercrime", Computer Law & Security Review, 28(2), 201-207.

Iqbal, A., & Aftab, S. (2019). A Feed-Forward and Pattern Recognition ANN Model for Network Intrusion Detection. International Journal of Computer Network & Information Security, 11(4).

Jamal, T., Haider, Z., Butt, S. A., & Chohan, A. (2018). "Denial of Service Attack in Cooperative Networks", arXiv preprint arXiv:1810.11070.

Koutsandria, G., Muthukumar, V., Parvania, M., Peisert, S., McParland, C., & Scaglione, A. (2014, November). "A hybrid network IDS for protective digital relays in the power transmission grid", In 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm) (pp. 908-913). IEEE.

Kumar, Y. V., & Kamatchi, K. (2020). Anomaly Based Network Intrusion Detection Using Ensemble Machine Learning Technique. en. In: International Journal of Research in Engineering, Science and Management, 3, 290-297.

Lee, C. H., Su, Y. Y., Lin, Y. C., & Lee, S. J. (2017, September). Machine learning based network intrusion detection. In 2017 2nd IEEE International conference on computational intelligence and applications (ICCIA) (pp. 79-83). IEEE.

Lin, W. C., Ke, S. W., & Tsai, C. F. (2015). CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. Knowledge-based systems, 78, 13-21.

Martins, I., Resende, J. S., Sousa, P. R., Silva, S., Antunes, L., & Gama, J. (2022). "Host-based IDS: A review and open issues of an anomaly detection system in IoT", Future Generation Computer Systems.

Paliwal, S., & Gupta, R. (2012). "Denial-of-service, probing & remote to user (R2L) attack

detection using genetic algorithm", International Journal of Computer Applications, 60(19), 57-62.

Papamartzivanos, D., Mármol, F. G., & Kambourakis, G. (2019). "Introducing deep learning self-adaptive misuse network intrusion detection systems", IEEE Access, 7, 13546-13560.

Raviteja, P., Devi, M. S. V. S., Gowri, M., Krishna, M. V. S., & Prabhakar, P. V. S. (2020). Implementation Of Machine Learning Algorithms For Detection Of Network Intrusion. vol, 8, 163-169.

Sharma, S., & Gupta, R. K. (2015)." Intrusion detection system: A review", International Journal of Security and Its Applications, 9(5), 69-76.

Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). "Deep learning approach for intelligent intrusion detection system", IEEE Access, 7, 41525-41550.

Wang, H., Forte, D., Tehranipoor, M. M., & Shi, Q. (2017). "Probing attacks on integrated circuits: Challenges and research opportunities", IEEE Design & Test, 34(5), 63-71.

Zanero, S., & Savaresi, S. M. (2004, March). Unsupervised learning techniques for an intrusion detection system. In Proceedings of the 2004 ACM symposium on Applied computing (pp. 412-419).

Zhou, Y., Cheng, G., Jiang, S., & Dai, M. (2020). Building an efficient intrusion detection system based on feature selection and ensemble classifier. Computer networks, 174, 107247.