# Optimal Performance for Intrusion Detection in WirelessLan Network Using Data MiningTechniques

**K. Raja[a] and M. Lilly Florence[b]**

[a]Research Scholar, BharathiarUniversity, Coimbatore, Tamil Nadu
[b]Research Scholar, BharathiarUniversity, Coimbatore, Tamil Nadu

**Article History**: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

**Abstract:** The objective of this paper is to identify the intruder of the wireless local area network based on the network and transport layer while accessing the internet within organizations and industries. The Intrusion detection system is the security that attempts to identify anomalies attributes who are trying to misuse a network without authorization and those who have legitimate access to the system but are abusing their privileges. The fact of the existing system deals with a firewall to protect and detect the unauthorized person using Wireless Local Area Network. Since the administrator may block or unblock the intruder based on the priority. This paper presents an enhanced framework, to detect and monitor the anomalies in the wireless sensor networks in an organization or an institution. The proposed approach to detect and filter the intruder in the wireless local area networks. Hence optimize the intrusion detection system in the particular organization or industries. The proposed IDS results are compared with the existing Decision Tree, Naive Bayes, and Random Forest algorithms.

**Keywords***:* Intrusion Detection System (IDS), Wireless Local Area Networks, Decision Tree, Naïve Bayes, Random Forest Algorithm.

## 1. Introduction

### 1.1 Wireless Local Area Network

Mobile World has hooked up to a wi-fi nearby region interconnected community. A tiny low business enterprise, industries, a crew, or possibly at automobile is hooked up with wi-fi on the web. Wireless Local Area Network (AmjadMehmood, 2017) mainly centered on a disbursed wi-fi community device that linked with n variety of sensors at a decrease price for companion change or business enterprise or possibly a crew.Every node contains its own set of attributes like memory, capacity, the flow of information, and rate per second that is linked to unreliable and unknown networks. The amount of Usage of nodes had been speedily accumulated within the last 5 years, which created a revolution within the modern-day technologies. Since the variety of nodes and usage will grow quickly, protection threats emerge as one of the primary issues inside the Wireless Local Area Networks.

### 1.2 Intrusion Detection System:

Security issues are triumph over with new generation is known as an Intrusion Detection System. IDS (AbhisekhVerma, 2018) is that the key method of extracting the knowledge from an outsized vast quantity of data to observe and find the trespasser within inside the network. In some other word, the Intrusion Detection System commonly wont to monitor, decide the expertise, and expect the effects which is probably used for destiny actions. Classification is one in each of the maximum crucial key roles inside the Intrusion Detection System. IDS classed into 2 broad categories: (Zhihua Zhang, 2017). a) Network Intrusion Detection System, that is hired to study and discover the packet of records, this is moving into or going away the wi-fi community. b) Host-Based intrusion Detection this is offering the statistics through the OS or records gathers via way of means of a particular OS.

### 1.3 Network Intrusion Detection System (NIDS):

This NIDS (Ziwen Sun, 2017) is generally divided into 2 categories: i) Misuse detection, virtual signatures, or Associate in Nursing styles of Associate in Nursing present man or woman or consumer at the perfect community that examine and document the assaults of an unwelcome man or woman. ii) Anomaly Detection performing as a protection to the unauthorized profile from the real community site visitors and both blocked or document returned to authorised persons.

## 2. Literature Review

Kalyani Tukaram Bhandwalkar (2016) projected that normal bar techniques like user authentication, encoding, avoiding programming errors, and firewalls primarily type the primary line of defense for System security. These systems propose a security vulnerability analysis. However, the intruders have their approach to

these vulnerabilities and bypass the preventive security tools. Thus, there's a requirement for the second level of defense, which is deep-seated by tools like intrusion detection systems (IDS). In network security, an Intrusion Detection System performs an inexpensive supplementary position for the firewall. It improves the safety and dependability of the system and helps protect computers from network attacks. Here current intrusion detection system are discussed based on some pattern mining algorithms. Intrusion detection in wireless networks has become an important part of the wireless network security system. Currently, most devices square measure Wi-Fi capable and may access local area network. Here associate Intrusion Detection System, Wi-fi prospector is mentioned.

KamepalliSujatha (2013) explained concerning the item set or a rule whose support is a smaller amount than the minimum support threshold. The extraction of sporadic patterns is termed sporadic pattern mining. This work in the main concentrates on sporadic pattern mining. It provides a survey on ways for mining sporadic patterns from differing kinds of datasets. This paper reviews completely different analysis and presents the ways that they adopted to mine the sporadic patterns. It conjointly explains concerning completely different application areas wherever these sporadic patterns is used.

**3. Existing Methodologies**

The existing algorithm such as decision tree, naive bayes, and random forest algorithm is considered for analysis of the proposed algorithm.

Decision Trees are applied to the sphere of intrusion detection for over a decade. In general, the input dataset to classifiers is in an exceedingly high dimension feature area, however, not all the options are relevant to the categories to be classified. A genetic algorithmic program picks a set of input options for a call tree classifiers, with the goal of skyrocketing the detection rate and decreasing the alert rate in a network intrusion detection. The KDDCUP99 information set to a coach and takes a look at the choice tree classifiers. The experiments show that the ensuing call trees will have a higher performance than those engineered with all accessible options.

The increase of internet utilization elevated the requirement of safety withinside the network this is monitored with the aid of using the Intrusion Detection System (IDS). The machine learning algorithms are usual for implementing any IDS to any abnormal events that passed offwithin the system traffic whether it's traditional or attacks and conjointly to spot any. Its conjointly ends up in winning investigation device to spot, a combination of the decision tree and random forest algorithms deliberate to reserve any atypical behaviour withinside the system traffic. Naive bayes algorithm is one of all the popular supervised classification algorithms for a categorical dataset that is made on conditional independence of feature assumption.

In networktransmissions, network interruption is that the maximum vital problem presently. The growing occasion of the machine attacks will be a stunning trouble for machine administrations. The completely exceptional evaluation works location unit presently directed to discover a booming and efficient claim prevent interruption with inside the machine to make sure to arrange safety and protection.

**4. Proposed Methodologies**

The Communication among the Wireless gadgets through a cellular or a laboratory linked in a completely wi-fi community could be subjected to a criminal offense attacked with the aid of using unauthorized gadgets. The companion in a nursing entrant will get admission to the wi-fi LAN and plausible to transmit the content material from one tool to different.IDS is employed to observe or find the entrant from the device employed in the organization. The projected rule is employed to find the entrant with the assistance of their protocol kind, a service, a source, a destination, a file, a fragment, etc., that is entered as an associate in a nursing entrant.

The essential technique glide of the studies paintings is to reveal the intruder from the wi-fi nearby place network. Each device of the wireless area network are monitored by the proposed algorithm based on the several attributes such as protocol type, service, source, destination, file, etc., if anyone of the attributes mismatched or not applicable, the concerned user may be treated as unauthorized user otherwise user can access the service provided by the wireless local area network.

The main objective of this proposed work to determine the anomalies from the sample dataset of the wireless networks taken from the organization or institution. This proposed work consists of five phases such as Data Collection, Preprocessing, Training, Testing, Analysis, and Report.The data are collected from the sample server of an organization through wireless local area networks which are based on the intrusion detection simulation which consists of 42 attributes and the volume of the dataset is 22500 and preprocessing of data used to avoid the noise and redundancy of data.After the Data collection and preprocessing stage. The reduced data are being taken as the input for the training phase. The data are trained which includes the combination of the proposed intrusion detection algorithm based on Naive's Bayes algorithm and decision tree algorithm. Since the Naive Bayes algorithm mainly focused on conditional probability and the decision tree focused on the predictive analysis.

The proposed algorithm is combined to get efficient and effective results. In the proposed algorithms a training module is being generated where the test data is fed.The testing phase includes the validation of the outcome to predict the actual result. Here, in this system, 30% of the pre-processed data is fed for testing towards the accuracy in predicting the anomaly-based IDS, Where the testing is made based on the training results. Testing is finished for the proposed set of rules on the idea of the skilled data. Parameters such as recall, precision, and accuracy are considered for analysis of the proposed algorithm along with existing algorithms such as decision tree, naive bayes, and random forest. The results generated based on the parameter of various anomalies attributes and also compared with existing algorithms.

## 5. Experimental Results

There are three parameters that are implemented to track and monitor the performance of the Proposed Algorithm using a confusion matrix.

| | |
|---|---|
| **Accuracy** | Accuracy will be Calculated as Assessment Divided by Total Vareity of Assessments<br>**Ay = Correct Assessment/Total Assessment** |
| **Precision** | Precision Termed because the method of scheming the quantitative relation of true positive divided by an actuality positive and false positive. |
| **Recall** | A recall could be a method of crucial the quantitative relation of true positive from the total of true positive and false negative |

The performance of results are measured for the proposed IDS along with existing IDS as follows:

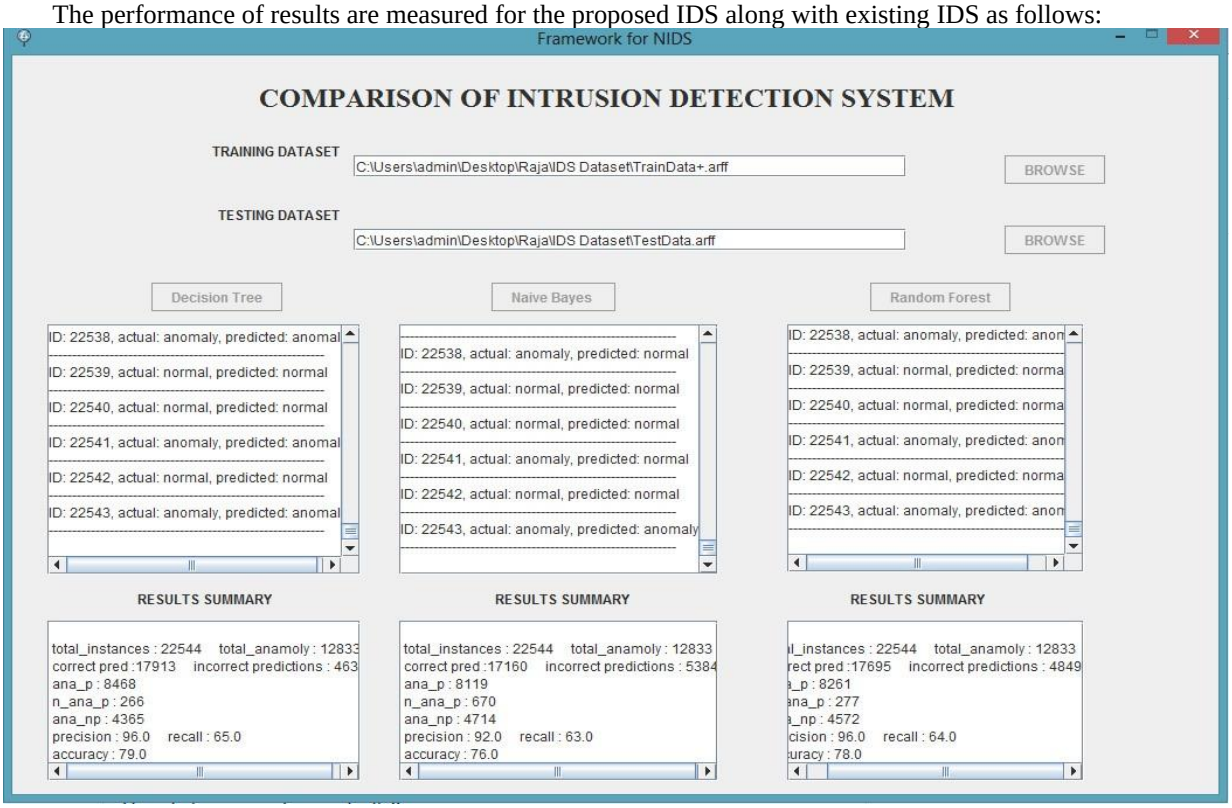


Figure 1: Results of existing IDS

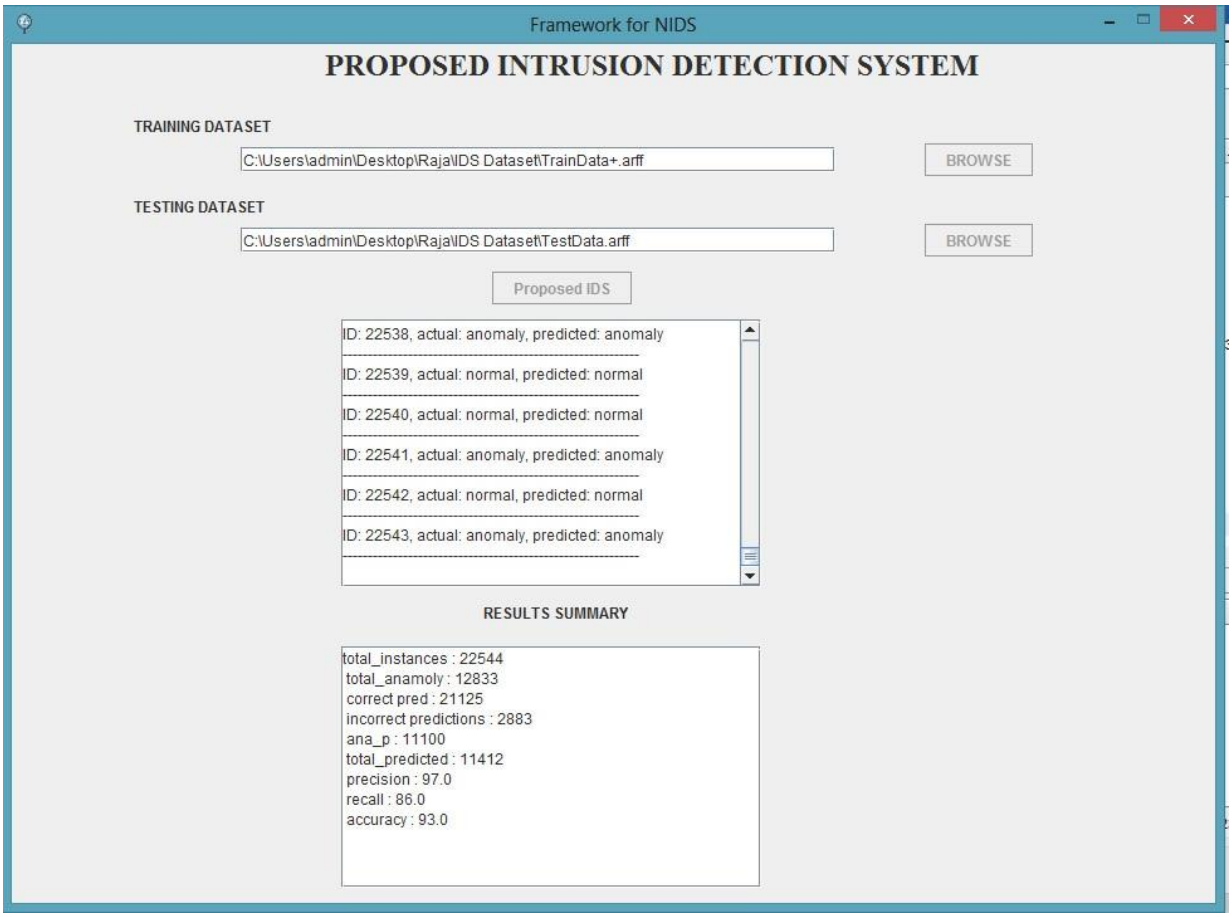


Figure 2: Results of Proposed IDS

The proposed algorithm results are compared with an existing algorithm with the parameter of Precision, Recall, and Accuracy are shown in the following table.

Table: Comparison of Proposed with Existing Algorithms

| **ALGORITHM** | **DECISION TREE** | **NAVIE'S BAYES** | **RANDOM FOREST** | **PIDS** |
|---|---|---|---|---|
| PRECISION | 96 | 92 | 96 | 97 |
| RECALL | 65 | 63 | 64 | 86 |
| ACCURACY | 79 | 76 | 78 | 93 |

The Following graph is generated from the above table as follows.

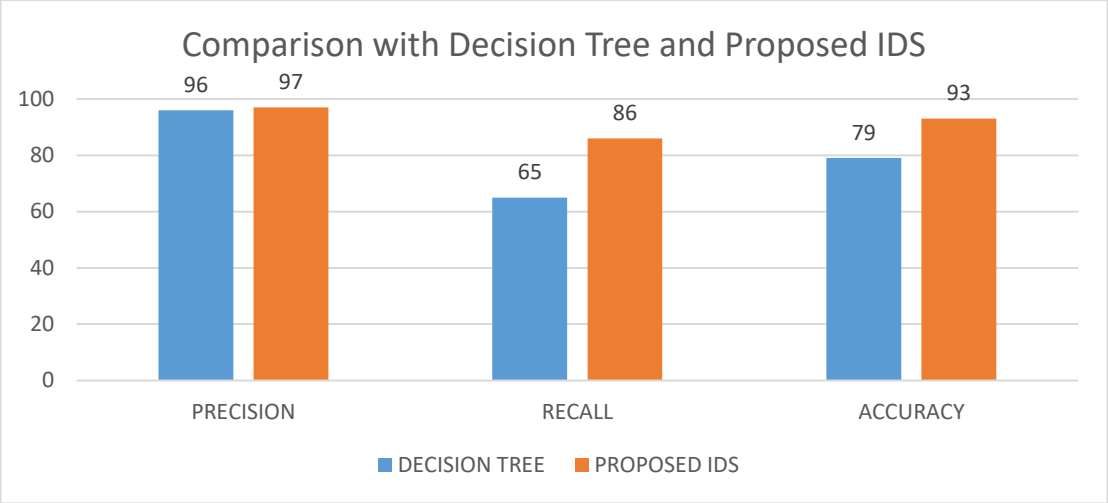


Figure 3: Comparison with Decision Tree and Proposed IDS

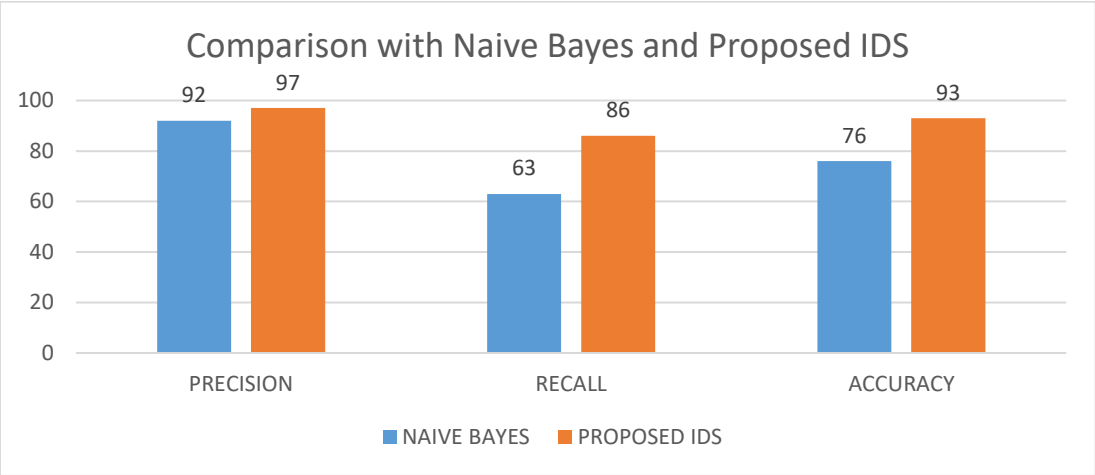


Figure 4: Comparison with Naïve Bayes and Proposed IDS

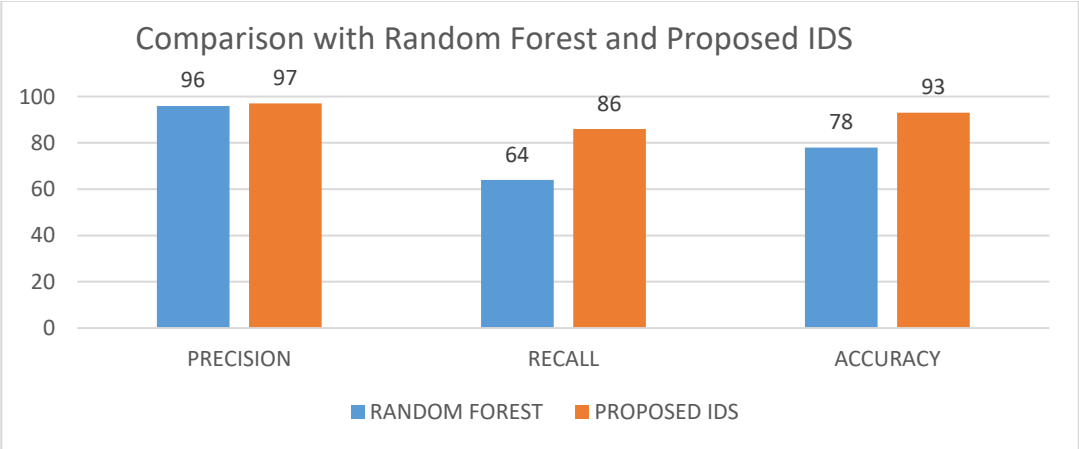


Figure 5: Comparison with Random Forest and Proposed IDS

## 6. Conclusion

In the proposed application to observe and discover the intruder in phrases of a cmobile device which includes laptops or mobile linked to the wireless LAN additional effectively and with efficiency. This proposed

enhanced framework is used to detect the anomalies of various attacks of the intrusion detection system using wireless networks. The Proposed Algorithm proved to be an effective process in determining performance evaluation using the confusion matrix along with the existing algorithm. This proposed research work concludes that the parameter used to determine the anomalies of various attacks is efficient and effective with good accuracy in the Wireless LAN.

**References**

1. Ameern Sultana, a. M. (2016). *Intelligent network Intrusion Detection System using Data Mining Techniques. IEEE Publication.*
2. AmjadMehmood, A. K. (2017). *Secure Knowledge & Cluster-based Intrusion Detection Mechanism for Smart Wireless Sensor Networks. IEEE Publication, 2169-3536.*
3. A.M. Barani, R.Latha, R.Manikandan, *"Implementation of Artificial Fish Swarm Optimization for Cardiovascular Heart Disease" International Journal of Recent Technology and Engineering (IJRTE), Vol. 08, No. 4S5, 134-136, 2019.*
4. Arunkarthikeyan, K. and Balamurugan, K., 2020, July. Performance improvement of Cryo treated insert on turning studies of AISI 1018 steel using Multi objective optimization. In 2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE) (pp. 1-4). IEEE.
5. Aroulanandam, V.V., Latchoumi, T.P., Bhavya, B., Sultana, S.S. (2019). Object detection in convolution neural networks using iterative refinements. Revue d'Intelligence Artificielle, Vol. 33, No. 5, pp. 367-372. https://doi.org/10.18280/ria.330506
6. Bhasha, A.C. and Balamurugan, K., 2020, July. Multi-objective optimization of high-speed end milling on Al6061/3% RHA/6% TiC reinforced hybrid composite using Taguchi coupled GRA. In 2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE) (pp. 1-6). IEEE.
7. Chinnamahammad Bhasha, A., Balamurugan, K. Fabrication and property evaluation of Al 6061 + x% (RHA + TiC) hybrid metal matrix composite. SN Appl. Sci. **1,** 977 (2019). https://doi.org/10.1007/s42452-019-1016-0
8. Deepthi, T. and Balamurugan, K., 2019. Effect of Yttrium (20%) doping on mechanical properties of rare earth nano lanthanum phosphate (LaPO4) synthesized by aqueous sol-gel process. Ceramics International, 45(15), pp.18229-18235.
9. Garikipati P., Balamurugan K. (2021) Abrasive Water Jet Machining Studies on $AlSi_7$+63%SiC Hybrid Composite. In: Arockiarajan A., Duraiselvam M., Raju R. (eds) Advances in Industrial Automation and Smart Manufacturing. Lecture Notes in Mechanical Engineering. Springer, Singapore. https://doi.org/10.1007/978-981-15-4739-3_66
10. Gowthaman, S., Balamurugan, K., Kumar, P.M., Ali, S.A., Kumar, K.M. and Gopal, N.V.R., 2018. Electrical discharge machining studies on monel-super alloy. Procedia Manufacturing, 20, pp.386-391.
11. K. Raja and Dr. M. Lilly Florence *"Implementation of IDS within a Crew Using ID3Algorithm in Wireless Sensor Local Area Network, Part of the Lecture Notes in Networks and Systems book series (LNNS),* ***Springer,*** *Volume 98, ISSN 2367 3370, Inventive Computation Technologies pp 467-475, August 2019*
12. K. Raja, and. M. Lilly Florence (2017*). Tracking of Intruder in Local Area Network Using Decision Tree Learning Algorithms. Asian Journal of Applied Sciences.*
13. Karthikeyan, G. M. (2018). *Intrusion Detection Using Data Mining Techniques. International Journal of Engineering Science Invention (IJESI).*
14. R. Manikandan, Dr Senthilkumar A. Dr Lekashri S. AbhayChaturvedi. *"Data Traffic Trust Model for Clustered Wireless Sensor Network." INFORMATION TECHNOLOGY IN INDUSTRY 9.1 (2021): 1225–1229. Print.*

*15.* PareshGoliwale, V. G. (2018). *Intrusion Detection System using Data Mining. International Research Journal of Engineering and Technology(IRJET).*

16. Ranjeeth, S., Latchoumi, T.P., Sivaram, M., Jayanthiladevi, A. and Kumar, T.S., 2019, December. Predicting Student Performance with ANNQ3H: A Case Study in Secondary Education. In 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE) (pp. 603-607). IEEE.

*17.* Vaddella., S. G. (2020). *A Study on Intrusion Detection System in Wireless Sensor Networks. International Journal of Communication Networks and Information Security, 127-141.*

*18.* Wenjie Zhang, D. H.-C. (2020). *Wireless sensor network intrusion detection system based on MK-ELM. Soft Computing , 1-14.*

19. Zhihua Zhang, H. Z. (2017). *Intrusion Detection Based on State Context and Hierarchical Trust in Wireless Sensor Networks. IEEE Publication.*

*20.* Ziwen Sun, Y. X. (2017). *An Intrusion Detection Model for Wireless Sensor Networks with an Improved V-Detector Algorithm. IEEE Publication.*