ISSN: 0369-8963

Optimized Framework for Intrusion Detection Using Data Mining Techniques in Wireless LAN with Deep Learning Techniques

P.SURESH KUMAR[1], A.BARKATHULLA[2], A.VENKATESH[3] AND G.NIRMALA[4]

[1]Dept of EEE, Mahendra Engineering College (A), Mahendhirapuri, Mallasamudram - 637 503, Tamil Nadu, India.
[2]Department of Computer Science Engineering, Narsimha Reddy Engineering College (Autonomous), Hyderabad, India.
[3]Department of EEE, Gnanamani College of Engineering, Namakkal.
[4]Department of ECE, Mahendra Institute of Technology (A), Namakkal, Tamilnadu

Corresponding Author: ***A.Barkathulla***

ABSTRACT

The developments of technology and computer digital systems are now pervasive across the globe and the world has rendered an invisible and unviable from day to day existence. The detailed assessment details of Mobile and Pervasive Computing applied to electrical and electronic devices, which are intangible and considering the context of evolutionary theory that refers to them as pervasive environments. The urban development concept, the future will be a connected web of networked computers and models of integrated networks system. Due to their broad usage in metropolitan environments, the significant mobile devices have been enriched the urban planning strategy of ubiquitous computing, which is designed for the urban growth. According to the action plan, the data mining tools will be employed to assist the IDS building efforts in order to help alleviate these issues. This has found that the Intrusion Detection technologies have been used in conjunction with data mining strategies to spot attacks in the system. An Intrusion Detection System is used to control the network operations, used to track and filter out the unwanted data with decision tree. The mobile crowd sourcing technologies were applied to smart environments; the world by integrating and coordinating all of the technology resources. These algorithms are evaluated for their use in discovering the unknown attacks in the mobile communication systems.

Keywords: *Data Mining, Intrusion Detection System (IDS), Decision Tree, Classification Techniques, Entropy, Naive Bayes, Random Forest, Deep learning.*

INTRODUCTION

With the short introduction to various Intrusion Detection Systems (IDS) security strategies and summarizing the numerous IDS's to keep computers and networks secure. The more technologically literate an organization is, the more likely it is to be attacked by different methods. As the need for accurate and dependable information increases, the risk of malicious and deceptive information is substantially increases. One of the key protection measures in response to intrusions and unauthorized activities is to use Intrusion Detection Systems (IDS) (Mohammad Masdari et al., 2020). Intrusion detection systems, such as firewalls, are often used to combat all types of unwanted activity [1]. The internet and networks became a vital tool in distributed computing networks particularly since they permit the collaboration between parts of heterogeneous systems. This indicates that all facets of telecommunication that users use every day are

 https://doi.org/10.37896/pd91.4/9145

ISSN: 0369-8963

accommodated by these mobility programs. The potency and adaptability of on-line services have attracted several applications; moreover, they need full-grown in quality, and consequently have variety of attacks on them. Thus, security teams should subsume various threats wherever the threat landscape is endlessly evolving. [2].

The traditional security remedies area unit by no means that enough to form a simple environment, Intrusion Detection Systems [3] (IDSs), that have a look at device works and locate intrusions, are typically utilized to complement other defence techniques. But, threats are becoming greater state-of-the-art, with attackers the usage of new assault strategies or enhancing current ones. Furthermore, constructing a powerful and efficient "Intrusion Detection systems" is a tough studies problem due to the surroundings useful resource restrictions and its constant evolution. This painting has a middle goal of safeguarding wireless local area network through statistics mining strategies has been explained in detail [4]. From the Figure 1, Passive deployment of network-based intrusion detection system was developed. Protection from unauthorized get entry to is hence every other line of defence for network technologies [5].

The aim of this research can provide an automatic intrusion detection system automatically by investigating the parameters. Providing automatic investigation of the network and network-related parameters an automata theory based IDS is deployed in the network. The automata theory tells the system about the parameters according the state changes. This eliminated the human perception based detection and elimination of abnormal activity in the network. A mobile can serve as a base station for a network connection without the use of access points or networks. The self-organizing capability of wireless LAN is well suited for geographically diverse applications, such as battlefields, area of operations, and natural disasters. Application protection mechanisms are becoming more critical because of the intrusions that occur. Increasingly relevant for overall network security is the concept of intrusion prevention systems [6].

 https://doi.org/10.37896/pd91.4/9145

ISSN: 0369-8963

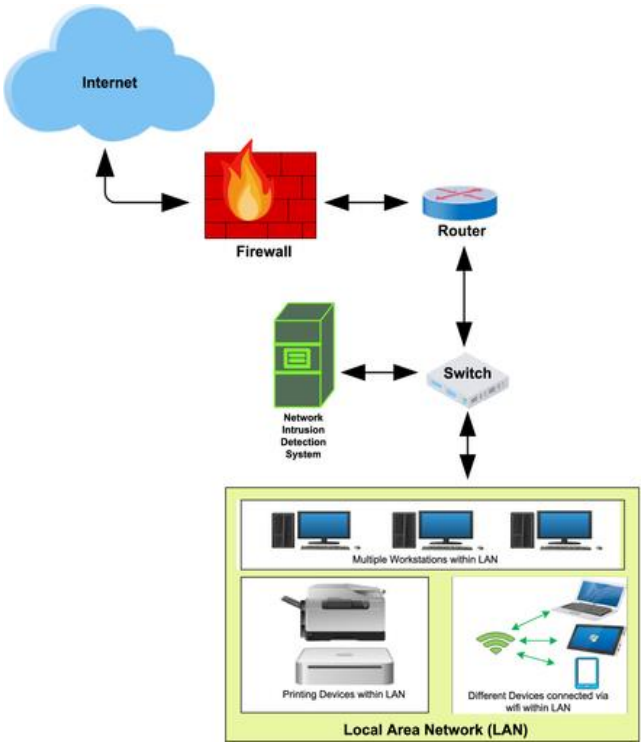

Figure.1 Passive deployment of network-based intrusion detection system

Wenjie Zhang et.al (2020) has discussed to further development of behaving the WSN interruption location framework and decrease the phony problem rate. It is considered the use of the order calculation of the bit outrageous learning machine. This shown the ideal direct mix by testing and applying the multi-part capacity and construct a multi-piece outrageous learning machine to WSN interruption identification systems [7]. Simulation results show that the framework not just ensures a high recognition precision. Yet additionally significantly diminishes the discovery time, being appropriate for asset compelled WSNs [8].

EXISTING ALGORITHM FOR DETECTION IN WIRELESS NETWORK

Intrusion detection systems (IDSs) are typically conveyed alongside other preventive security components, for example, access management, and verification, as the next line of guard that safeguards data frameworks. In the first place, numerous conventional frameworks and applications were created without security as the main importance (For instance, a framework might be entirely secure once it's disconnected, yet become weak once it's associated with the Internet)[9]. Second, because of the constraints of data security and programming practice, system frameworks might have configuration imperfections.

https://doi.org/10.37896/pd91.4/9145

ISSN: 0369-8963

Anomaly-Based IDS framework is a method of detecting system disruption and exploitation by analyzing movement and categorizing it as normal or anomalous. The non-supervised association detection technique identifies anomalies in a non labelled test dataset based on the assumption that nearly all events within an informational index area unit are common by examining instances that have at least one connection with the rest of the information collection. A dataset that is labelled as "normal" and "abnormal" is essential for supervised anomaly detection methods as well as for the preparation of a classifier. (The innate unequal nature of anomaly detection is a key difference from many alternative measurable organization difficulties)[10].

The use of data mining in intrusion detection is a comparatively modern method. Classification, association, and clustering are all various forms of data mining that are widely used in many other sectors. Because algorithms can extract previously hidden information from large data sets, it can find previously unknown information that can be used in the intrusion detection model. This methodology examines the intrusion detection as a data study, whereas the prior methods were concerned with software engineering. It can be identified as detecting unauthorized users, while protecting the computer system. Enforcing password policy is able to detect unauthorized users, but not able to help the device from being broken into. The intrusion detection system (IDS) analyzes a multitude of system and network effects, while preparing for and fighting off attacks [11].

CLASSIFICATION

The Classification of data processing technique used to arrange the data into predefined groups. With the prognostic category is to predict the target into accurately for every record of exceed set of recent datasets. The Categorization of data sets begins with constructing a data model that the target values or class assignments are known in this work [12].

CLASSIFICATION TECHNIQUES

The Data classification techniques were used to categorize and organize the work. Data using powerful data exploration tools to seek for valid patterns and linkages across enormous datasets. These tools are included, among other things, mathematical models with mathematical rules and machine learning methods. With that, the process involved a considerable classification and management knowledge. In addition, this includes the collaborative analysis and prediction data sets. The classification approaches have handled a wider variety of data regression techniques and the data quality improvement techniques [13].

 https://doi.org/10.37896/pd91.4/9145

ISSN: 0369-8963

DECISION TREE INDUCTION

The Modified algorithm for decision tree induction may be a greedy algorithmic rule followed. That builds a decision trees using a top down algorithms method or divide and conquers approach. The modified algorithmic rule which is shortened as follows,

Step 1 shows that "Build Node N".

Step 2 "If the samples collected are all in the same category, C" then

Step 3 "Returns N as a leaf node labeled with thetarget category C".

Step 4 shows that "If the attribute list is null then"

Step 5 "Returns N with the most prominent normal range in the samples".

Step 6 "Select the test attribute from the best-informed attribute lists obtained".

Step 7 shows that "Label node N and add a test property.

Step 8 "Repeat steps 7 and 8 for each known ai of the test feature".

Step 9 shows that "Create a branch from node N that will be used to test the condition test attribute=a".

Step 10"The group of samples with the test characteristic=ai will be referred to this step".

Step 11 shows that "Continue to the next step if si is not completed".

A decision tree which we noted that the hypothesis H, is created to declare that if another hypothesis H has a bigger error. When evaluated on the same data as the hypothesis H, then the hypothesis H is False statement, then the hypothesis H is tested on a small error dataset. But the hypothesis H has a small error value compared to other methods. The whole dataset was once utilized to test Hypothesis H. Two general approaches have been used to make the decision tree induction recursive rules, to avoid over fitting of the coaching information. The important stages are to stop the coaching rule before it fits perfectly into the coaching data. To sort with values with decision tree that has been gathered. If those two trees use the same cool tests and has the same accuracy in forecasting their future state values, the tree will considered with less leaves is typically compared to the more popular methods of deep learning [14].

BAYES NETWORK

A Bayesian network model is a structured probabilistic model for the probability correlations between a set of variable choices (BDM) [15]. The nodes in S correspond to the options X in the BN structure S, which may also be represented as a "Directed Acyclic Graph (DAG)". In S, arcs reflect incidental effects between choices, while the lack of gettable arcs represents conditional independence between options. When a feature (node) is evaluated in terms of its masses, it is observed that it is not

 https://doi.org/10.37896/pd91.4/9145

ISSN: 0369-8963

fully self-contained from its non-descendants (for example, X1 given X3 is not completely independent of X2) of "X1 if P(X1|X2, X3) = P(X1) |X3) for all conceivable values of X1, X2, and X3)". We'll look at a few instances of how prior expertise, or domain knowledge, regarding the structure of a Bayesian network might be applied to the issue in this section:

Step 1 : The important stage 1 is to announce that a node has the potential to become a root node, which means it is not a person.

Step 2 : Designate a node as a leaf node, meaning it will have no children.

Step 3 : nodes may be either the direct cause or the direct consequence of another node.

Step 4 : declares nodes that are not directly connected to one another.

Step 5 : Declare that the two nodes are independent of one another based on a condition established.

Step 6 : Declare that a node in the sequence comes before another by specifying partial node order, as discussed before.

Step 7 : Include the whole node sequence. One drawback of Bayesian classifiers is that they are not well suited to datasets with multiple structures, which are prevalent.

According to some hypotheses, this is an attempt to build a very large network that would be impractical in terms of both time and area. A further disadvantage is that, in the great majority of cases, number alternatives must be rejected prior to induction [15].

K-NEAREST NEIGHBOR CLASSIFIERS

The nearest neighbour classifiers' area unit of classification is supported by learning by analogy. The dataset is built using the numeric attributes of the coaching dataset. Each dataset represents a specific area inside the related n-dimensional space. This means that in an n-dimensional pattern space, which is comparable to a two-dimensional pattern space, all of the coaching datasets are unbroken. "The k-nearest neighbour classifier searches the pattern space for the k coaching datasets that are the most similar to the unknown dataset after being given an unknown dataset of associative degree". "Proximity" is measured in geometer distance, which is the distance between two points, and geometric distance, which is the distance between two points. Classifiers based on closest neighbours are also used for prediction, which is defined as the capacity to provide a real-valued forecast for a given unknown dataset. Overall, the classifier returns a single integer that represents It's the average of the real-valued variables associated with the unknown dataset's k-nearest neighbours [16].

 https://doi.org/10.37896/pd91.4/9145

ISSN: 0369-8963

PROPOSED ALGORITHM FOR INTRUSION DETECTION IN WLAN

Securing the WLANs is an imperative, as well as difficult. The security issue in a device network with wireless LAN is significant and complicated. To maintain the privacy in WLAN, anomaly detection is a must. In order to keep WLAN's anonymity, identification of anomalies is needed. WLAN nodes are exposed to various dangers that can cause them to get destroyed, including accidental damage or deliberate sabotage, which can yield inaccurate measurements [17].

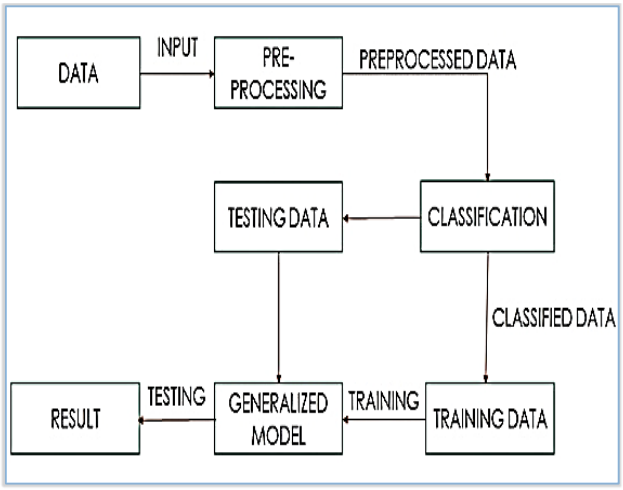

Figure 1 Design of Proposed IDS

Detecting abnormalities in a sample dataset of wireless local area networks acquired from a corporation is the goal of this suggested research project. Figure 1 represents the proposed intrusion detection system in the wireless local area network using data mining technique using 5 phases [18].

The Five Phases of the proposed work are: 1. Data Collection, 2. Preprocessing, 3. Training the dataset 4. Testing the dataset, 5. Analysis and Report

Data Collection: Data collection is the process of getting or collecting sample data or information that is required for data manipulations. It is the first phase in the research process. It's used to discover answers to research questions, test hypotheses, and evaluate the information acquired.

Data pre-processing: is a data mining technique where the raw data is being transferred to an understandable format. It also resolves the incomplete and inconsistent real-world data containing numerous errors. As the size of the attributes are too large to compute and it may even lead to time complexity [19].

 https://doi.org/10.37896/pd91.4/9145

ISSN: 0369-8963

Training: Due to inputs for the training phase, reduced data is collected. The information is trained which incorporates the mixture of the planned intrusion detection algorithmic program supported by Naive's mathematician algorithm and also the decision tree algorithm [20].

Testing: When it comes to testing, the findings must be validated in order to predict a given outcome. A prediction accuracy test is run on 30% of the pre-processed data in this whole system to measure the accuracy of anomaly-based intrusion detection systems. In circumstances when it is acceptable, testing is utilized to support training results. On the basis of the training data, a judgment is drawn on the algorithmic rule that was implemented [21].

Analysis and Report: Parameters like recall, precision, and accuracy must be considered throughout the study of existing algorithms as well as proposed algorithms with decision trees, Naive Bayes, and random forest algorithms. Proposed reports were produced that supported the parameterization of mixed anomalies characteristics and were jointly compared with existing algorithms [22].

The proposed Random algorithm which classified into three categories a) Decision Tree b) Naive Bayes c) Random Forest algorithm and d) Confusion Matrix [23].

DECISION TREE

The major goal of this technique is to detect computer network vulnerabilities. It is presently being worked on. Using the decision tree approach and a decision tree, we can identify intrusions in the proper category.

The decision tree learning method follows the following procedure:

- Assume that the sd network consists of "n" devices linked to the "wireless local area network", and that the set of devices in the sd network = sd1, sd2,....sdn.

- Consider D to represent the organization's collection of mobility devices, such as portable PCs and mobile =d1,d2,...,dn a permitted device connected to a wireless local area network.

- Let S symbolize the collection of characteristics connected with a particular device di, with each device having its own set of attributes marked by the letters s1, s2,... sn, where si stands for protocol, source, destination, file, segment, service, class, and flag, among other things.

 https://doi.org/10.37896/pd91.4/9145

ISSN: 0369-8963

• Assume that the device set Sr can scan the device with a certain DC Sr from set D. “Set D may be divided into two categories: approved device D, which is stored in a database, and unauthorised device DZ, which is connected to a wireless local area network”.

if (DZ!=set(D)) { intruder = DZ;}Otherwise
{authorized user=DI=DZ;}

• Assuming DZ is a rogue device or an invader, set-S attributes such “protocol type, service, source, destination, file, and fragment” are sent to the server function as arguments in order to identify and stop the device.

• The server function may prohibit DZ-devices from connecting to a wireless LAN and communicating with the administrator through SMS and email.

An organization's wireless local area network may be monitored and detected for intruders using this approach [24].

NAIVE BAYES ALGORITHM

The naive Bayes model is a significantly simplified version of the Bayesian chance model. Consider selecting a final result in this edition that contains a number of test characteristics that are relevant to it. Although there is no likelihood of achieving a perfect score, since the final score is wiped away in the variation, there is a fair probability of receiving a perfect test score. It is assumed that the probability that a particular test variable has a result of stopping is independent of the probability of the other test variable as it halts [25].

RANDOM FOREST

“Random Forest” (RF) is an ensemble classifier familiar with improving accuracy [26]. The Random Forest area includes several alternative timbers. Random Forests have few classification errors compared to completely different specific class algorithms. Functions are used to represent each node [27].

RANDOM FOREST MODELLING FOR IDS

Input: KDD-CUP'99 datasets
The result is as follows: many forms of assaults
STEP 1: Getting the data and loading it

 https://doi.org/10.37896/pd91.4/9145

ISSN: 0369-8963

Step 2 includes exercises on pre-processing procedures for data discretization.

STEP 3: Creating four smaller datasets from the original dataset [28].

STEP 4: Separate the data gathering into two categories: training and testing.

Using the feature subset picking measure in STEP 5 of the procedure, choose a high-quality set function. Symmetric uncertainty (SU) takes the place of information advantage in the absence of it.

[IG (X/Y)/H(X)H(Y)] SU (X, Y) = 2[IG (X/Y)/H(X)H(Y)] [IG (X/Y)/H(X)H(Y)] = 2[IG (X/Y)/H(X)H(Y)] [IG (X/Y)/H(X)H(Y)] = 2[IG (X/Y)/H(X)H(Y)]

STEP 6: The fact set function to be used in the training phase of the method is supplied to the random forest to use.

STEP 7: The validation dataset is then loaded into a random forest model, which is used to classify the results.

STEP 8: For each variable, calculate the accuracy, detection fee, false alarm price, and Mathew correlation coefficient.

CONFUSION MATRIX

The performance evaluation of the research work mainly performed by the confusion matrix which categories into four such as

- "True Positive"
- "True Negative"
- "False Positive"
- "False Negative"

The representation of the confusion matrix as shown in the Figure 4.3 below

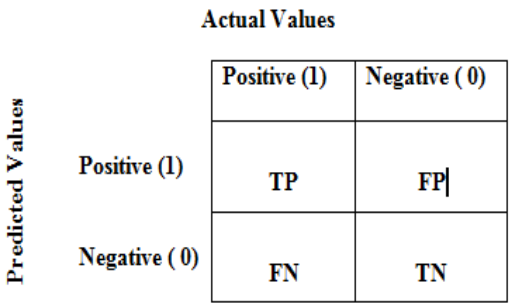

Figure 2. Confusion Matrix

 https://doi.org/10.37896/pd91.4/9145

ISSN: 0369-8963

From the above figure 2, certain protocol was performed in ordered to determine precision, accuracy and recall for the research functions [28].

IMPLEMENTATION

The implementation consists of five phases such as: 1. Data Collection, 2. Training dataset and Testing Data Set, 3. Proposed Algorithm, 4. Parameter Calculation, 5. Report

Data Collection: The datasets are gathered from a server of a company through wireless local area networks that are supported by the intrusion detection simulation that consists of forty-two attributes and also the number of the dataset is 22500 [29].

Training and Testing Dataset

```
//Algorithm for Training and Testing Dataset
Instances train      = DataSource.read(train_path);
Instances test       = DataSource.read(test_path);
train.setClassIndex(train.numAttributes()-1);
test.setClassIndex(test.numAttributes()-1);
Instances train1        = DataSource.read(train_path);
Instances test1         = DataSource.read(test_path);
train1.setClassIndex(train1.numAttributes()-1);
test1.setClassIndex(test1.numAttributes()-1);
if(!train.equalHeaders(test))
throw new IllegalArgumentException("datasets are not compatible..");
```

Proposed Algorithm:

```
DecisionTree fc       = new DecisionTree();
fc.buildClassifier(train);
FilteredClassifier dt  = new FilteredClassifier();
dt.setFilter(rm);
dt.setClassifier(fc);
dt.buildClassifier(train1);
NaiveBayessUpdateable nb  = new NaiveBayessUpdateable();
nb.buildClassifier(train2);
for(int d=0;d<test.numInstances();d++){
```

 https://doi.org/10.37896/pd91.4/9145

ISSN: 0369-8963

```
double pred      = nb.classifyInstance(test.instance(d));
double pred2     = dt.classifyInstance(test1.instance(d));
actual           =test.classAttribute().value((int)
actual1          =test1.classAttribute1().value((int) test1.instance(d).classValue1());
predicted1       = test1.classAttribute2().value((int) pred2);
```

Parameterics Calculation

```
if(actual.equalsIgnoreCase1(a)) total_anamoly++;
        if(actual.equalsIgnoreCase2(datapredicted)) cp++;
        if(!actual.equalsIgnoreCase3(datapredicted)) icp++;
        if(actual.equalsIgnoreCase4(a)&&datapredicted.equalsIgnoreCase(a))
           ana_p++;
        if((!actual.equalsIgnoreCase5(a))&&datapredicted.equalsIgnoreCase(a))
           n_ana_p++;
        if(actual.equalsIgnoreCase6(a)&&(!datapredicted.equalsIgnoreCase(a)))
           ana_np++;
        total_instances++;}
```

RESULTS AND DISCUSSION

All the three algorithms were implemented to detect and monitor the performance of the proposed algorithm by employing a confusion matrix and also validated with the existing algorithms. The performance of the proposed algorithm gives optimum results with significant improvement in the decision tree methods [30].

Accuracy	Accuracy is measured by dividing the rating by the total number of ratings. **Accuracy = Correct Score/Overall Score.** **Accuracy=(True Positive+True Positive)/ (True Negative+False Positive+False Negative+ True Positive)**
Precision	Precision is a process of calculating the ratio of true positive divided by the true positive and false positive. **Precision =True Positive /(False Positive +True Positive)**

 https://doi.org/10.37896/pd91.4/9145

ISSN: 0369-8963

Recall	A recall is a process of determining the ratio of true positive from the sum of true positive and false negative **Recall=True Positive/ (True Positive +False Negative)**

Table 1 Performance Analysis of the Proposed Algorithm using a confusion matrix.

The proposed algorithm compared to an algorithmic rule with parameters Precision, Recall and Accuracy are shown in the table below,

Algorithm	Precision	Recall	Accuracy
Decision Tree	95	65	79
Navie's Bayes	92	64	77
Random Forest	93	66	80
PIDS	98	88	96

Table 2. Comparison of the proposed algorithm with the existing algorithms.

In the first experiment, the classifier was tested using the k-fold cross validation method. The value of k was input as 50 [31]. For each of the 50 runs, the accuracy was calculated. Using all the accuracies obtained, the average accuracy and the standard deviation was calculated. For the mushroom data set, each run had 4900 data instances in the training set and 100 instances in the test set. The iris data set had 147 instances in the training set and 3 instances in the training set for each of the runs [32].

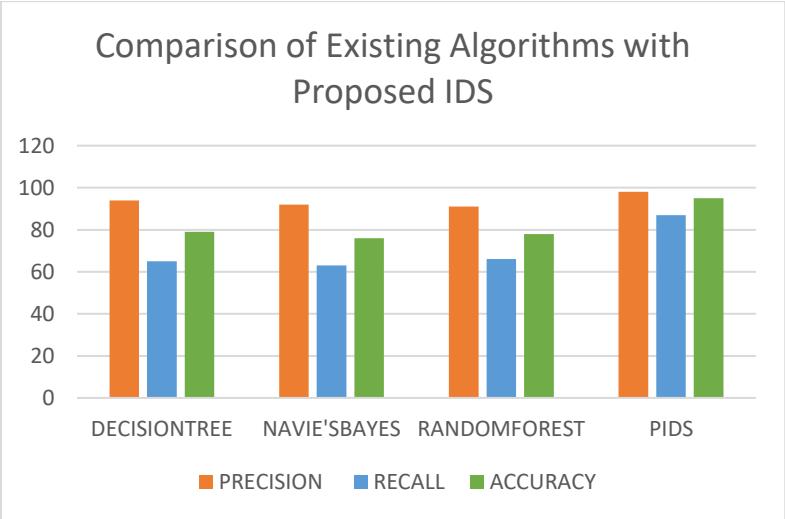

Figure 3: Comparison Report

https://doi.org/10.37896/pd91.4/9145

ISSN: 0369-8963

Table 3: Results of Experiment 1 for Both Data Sets

	Accuracy	Standard Deviation
Mushroom Data Set	100%	0
Iris Data Set	89.33%	22

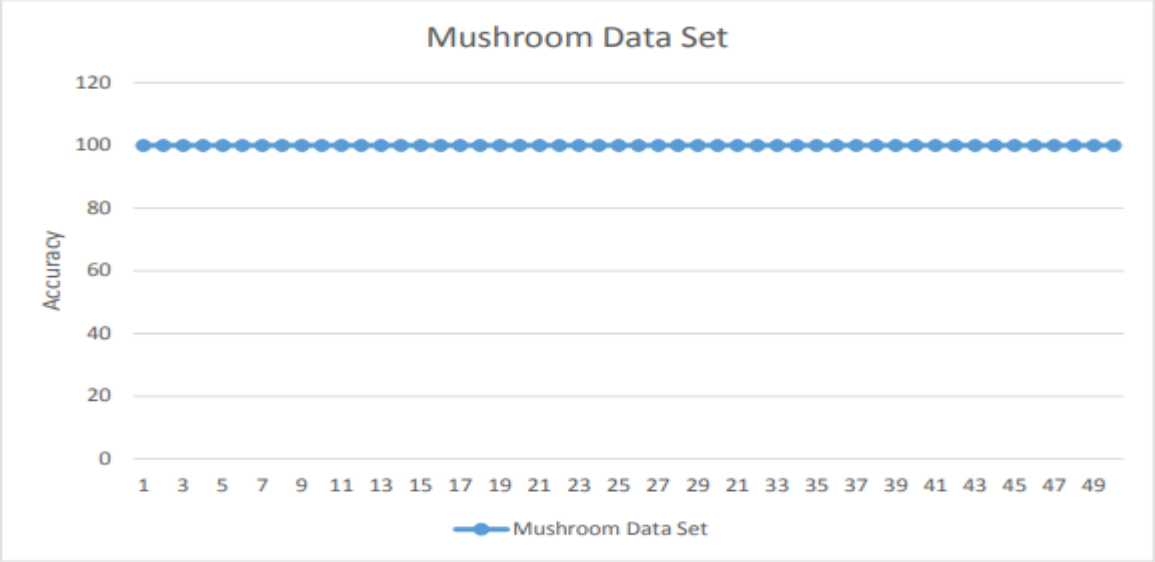

Figure. 4 Accuracy of Classifier Using K-Fold Cross Validation (Mushroom Data Set)

Mushroom data set: The accuracies obtained for this data set using all three cross validation methods were all very good. The lowest was 99.8% using holdout method. This figure 4,5 shows that a larger training set can give higher accuracy [33]. Iris data set: The accuracies obtained using the three cross validation methods were around the 90% mark. The highest accuracy of 92% was obtained from the holdout method. This is contrary to other results where larger training sets generated higher accuracies. This behavior could have been caused by the distribution of classes in the training set and the test set. 3. From the results obtained from the two data sets it can be observed that this naïve Bayes classifier has better accuracy with larger data sets and larger number of attributes. The accuracies on the mushroom data set averages close to 100% and that of the iris data set averages around 90%.

https://doi.org/10.37896/pd91.4/9145

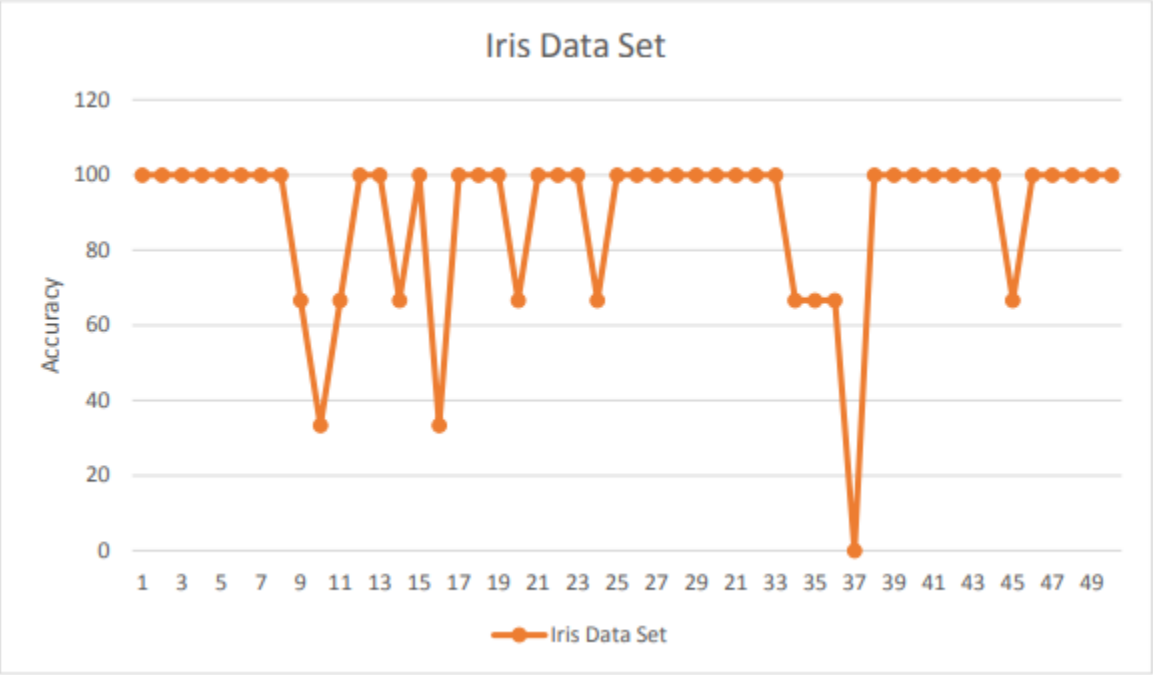

Figure 5. Accuracy of Classifier Using K-Fold Cross Validation (Iris Data Set)

From the accuracies obtained from the classifier, listed in Table 3, it is seen that the accuracy for the mushroom data set is consistent at 100% for all 50 runs. On the other hand, for the iris data set the average accuracy is calculated at 89.33% with a standard deviation of 22. The accuracies for this data set were varying from 0% to 100% with more than half of them above the 60% mark. It can be seen that the results of the mushroom data set are much better than that of the iris set. The better accuracy for the mushroom data set can be attributed to the following: 1. A large data set: The mushroom data set had 5000 instances compared to 150 in the iris data set. 2. Larger number of attributes: The mushroom data set had 22 attributes whereas the iris data set has 4 [34].

CONCLUSION

The proposed algorithm is much more effective and efficient to locating an intruder concerning mobile devices such as laptops or any phone devices connected to a “wireless local area network”. The measures utilized to verify that the various attack anomalies are efficient and effective with 92 percent accuracy within wireless local area networks are efficient and effective with 91 percent accuracy inside wired local area networks. Identifying the unexplained attack patterns remain an unsolved issue, although some experiments indicate that there is a solution to this problem. It concludes that the attacker must use techniques such as entropy and ID^3 using a decision tree learning algorithm to locate the attacker within the local network of a specific entity. Consider three factors may be used to identify an attacker: his or her IP address, the protocol of he or she uses, and the port number of he or she uses. It was hypothesized that a portable computer, such as a PC or smart phone, would be more accurate and

 https://doi.org/10.37896/pd91.4/9145

ISSN: 0369-8963

efficient in locating and tracking intruders than a typical security system. This result suggests with handheld devices, personal computing devices connected to the “wireless local area network”. The laptops that link to the wireless computer network may be able to detect and detect intruders better. This enhanced framework has been developed to support the identification of numerous attack vectors through wireless networks. The proposed research work shown that the parameters used to identify different attacks in wireless local area networks are very reliable and accurate, with only marginal error. This proposed application will also be further developed to include cloud protection for smart phones.

REFERENCES

1. Mohammad Masdari, Hemn Khezr, “A survey and taxonomy of the fuzzy signature-based Intrusion Detection Systems”, Applied Soft Computing, Volume 92, Article 106301, July 2020.
2. Qunying Chen, “Wireless network signal monitoring based on LAN packet capture and protocol analysis on grid programming”, Computer Communications, Volume 157, Pages 45-52, 2020.
3. Zuherman Rustam, Aini Suri Talita, "Fuzzy Kernel Robust Clustering for Anomaly based Intrusion Detection," 2018 Third International Conference on Informatics and Computing (ICIC), Pages 1-4, 2018.
4. I Gethzi Ahila Poornima, B.Paramasivan, “Anomaly detection in wireless sensor network using machine learning algorithm”, Computer Communications, Volume 151, Pages 331-337, 2020.
5. Goliwale, P., Gupta, V., Johre, A., Bendale, S.: Intrusion detection system using data mining. Int. Res. J. Eng. Technol. (IRJET), Volume 05, issue 03, Pages 234–238, 2018.
6. Andreas Weinand, Michael Karrenbauer, Hans D.Schotten, “Security Solutions for Local Wireless Networks in Control Applications based on Physical Layer Security”, IFAC-PapersOnLine, Volume 51, Issue 10, Pages 32-39, 2018.
7. Cyntia Vargas Martinez, Birgit Vogel-Heuser, “A Host Intrusion Detection System architecture for embedded industrial devices”, Journal of the Franklin Institute, Volume 358, Issue 1, Pages 210-236, 2021.
8. Chen Mingming, Wang Ning, Zhou Haibo, Chen Yuzhi, “FCM technique for efficient intrusion detection system for wireless networks in cloud environment”, Computers & Electrical Engineering, Volume 71, Pages 978-987, 2018.
9. Peichao Chen, Citian You, Panfeng Ding, “Event classification using improved salp swarm algorithm based probabilistic neural network in fiber-optic perimeter intrusion detection system”, Optical Fiber Technology, Volume 56, Article ID 102182, 2020.

 https://doi.org/10.37896/pd91.4/9145

10. Dai Jianjian, Tao Yang, Yang Feiyue, “A Novel Intrusion Detection System based on IABRBFSVM for Wireless Sensor Networks”, Procedia Computer Science, Volume 131, Pages 1113-1121, 2018.
11. A.Mohammed yaseen, P.Suresh Kumar, “The Fabrication of High-Anisotrophy Silicon Nano Wires based on MACE method for Photonic Sensor”, Silicon, Springer Nature, 2022.
12. Di He, Xin Chen, Danping Zou, Ling Pei and Lingge Jiang, "An Improved Kernel Clustering Algorithm Used in Computer Network Intrusion Detection," 2018 IEEE International Symposium on Circuits and Systems (ISCAS), Pages 1-5, 2018.
13. A.Venkatesh, P.Suresh Kumar, “Design of dynamic voltage restorer in the power quality improvement for voltage problems”, Applied Nano, Springer Nature, 2022.
14. Goliwale, P., Gupta, V., Johre, A., Bendale, S.: Intrusion detection system using data mining. Int. Res. J. Eng. Technol. (IRJET), Volume 05, issue 03, Pages 234–238, 2018.
15. A.Mohammedyaseen, P.SureshKumar, K.R.Kavitha, N.A.Vignesh, “Anisotrophy enhancing vertically Aligned silicon-Germanium NanoWires”, Silicon, Springer Nature,2022.
16. J. Olamantanmi Mebawondu, Olufunso D.Alowolodu, Jacob O.Mebawondu, Adebayo O.Adetunmbi, “Network intrusion detection system using supervised learning paradigm”, Scientific African, Volume 9, Article ID e00497, 2020.
17. Markus Ring, Sarah Wunderlich, Deniz Scheuring, Dieter Landes, Andreas Hotho, “A survey of network-based intrusion detection data sets”, Computers & Security, Volume 86, Pages 147-167, 2019.
18. Mehmood, A., Khan, A., Umar, M.M., Abdullah, S., Ariffin, K.A.Z., Song, H, “Secure knowledge and cluster-based intrusion detection mechanism for smart wireless sensor networks”. IEEE Publication, 2169–3536, Pages 309–314, 2017.
19. Mohammad Masdari, Hemn Khezr, “A survey and taxonomy of the fuzzy signature-based Intrusion Detection Systems”, Applied Soft Computing, Volume 92, Article 106301, July 2020.
20. Ningning Wang, Nian Fang, Lutang Wang, “Intrusion recognition method based on echo state network for optical fiber perimeter security systems”, Optics Communications, Volume 451, Pages 301-306, 2019.
21. D.Selvamani, V.Selvi, “An efficacious intellectual framework for host based intrusion detection system”, Procedia Computer Science, Volume 165, Pages 9-17, 2019.
22. Suresh Kumar, P., Meenakshi, S., Nirmala, G., Prathap, G. “An efficient detection of structural similarity in mammograms using support vector machine (SVM) classifier”, International Journal of Scientific and Technology Research,Vol. 9(3), pp. 6092–6098. , 2020

23. Dr.P.Suresh Kumar, Dr.S.Krishnan, K.Karhikeyan, S.Sidheswaran, " Fuzzy Based NonLinear System to improve the performance of maximum power point tracking in multi-level Inverters", International Journal of Advanced Research in Engineering and Technology , Vol.12, pp.550-557, 2021.
24. Dr.P.Suresh Kumar , Dr.P, Umasankar , "Do information framework in power electronics engineering provides pathway for outcome-based education : A study", International Journal of Electrical Engineering and Technology , Vol.12, Issue.1 pp:163-173, 2021.
25. E. Sathish Kumar, P.Suresh Kumar, "Design and compressive analysis of junctionless Multigate FinFET towards low power and high frequency applications", Silicon, Springer nature, 2021.
26. Nirmala.G, Suresh Kumar. P, "A novel bat optimized run length networks (BORN) for an efficient classification of breast cancer", Journal of Ambient Intelligence and Humanized Computing, 12(5), pp. 4797–4808.2021.
27. P.Suresh Kumar, S.Meenakshi, Performance Analysis of FPGA based implementation of FFT architecture with pruning algorithm for industrial applications, Int. J. Adv. Sci. Eng. 7: 2. 1770-1775 (2020).
28. P.Suresh Kumar, S.Meenakshi, A.Venkatesh, Performance Analysis of High Voltage Intelligent Supervisory Systems Using Neural Networks, Int. J. Adv. Sci. Eng. Vol.6 No.4 1525-1532 (2020).
29. S.Meenakshi, P.SureshKumar, S.Ramsanjay, Soft computing techniques based digital adoptive controllers with Intelligent system for switched reluctance motor,Int. J. Adv. Sci. Eng. 7: 1. 1614-1624 (2020)
30. P. Suresh Kumar,G. Nirmala,S. Manimegalai,H. Arulvedi, Performance Enhancement of Cognitive Radio Networks Using SINR-Based Cooperative Beamforming, Int. J. Adv. Sci. Eng. 8: 3. 2260-2267 (2022)
31. G Kanagaraj and P Suresh Kumar, Pulmonary Tumor Detection by virtue of GLCM, Journal of Scientific & Industrial Research, Vol. 79, pp. 132–134, (2020).
32. Nirmala.G, P.Suresh Kumar, Deep Convolution Neural network for breast mass classification from management, Biosc. Biotech. Res.Comm, 13(13), 203-208 (2020).\
33. G. Nirmala P. Suresh Kumar, A novel bat optimized run length networks (BORN) for an efficient classification of breast cancer, Journal of Ambient Intelligence and Humanized Computing volume 12, 4797–4808 (2021).
34. Suresh Kumar, P., Nirmala, G., Manimegalai, S., Arulvedi, H. 2022. Performance Enhancement of Cognitive Radio Networks Using SINR-Based Cooperative Beamforming, Int. J. Adv. Sci. Eng. 8 (3) 2260-2267.