International Journal of Information Processing and Communication (IJIPC) Vol. 11 No. 2 [December, 2021], pp. 61-74
Online: ISSN 2645-2960; Print ISSN: 2141-3959

Supervised Machine Learning Algorithms for Cyber-Threats Detection in the Perception Phase of a Situation Awareness Model

[1]Olofintuyi, Sunday Samuel and [2]Olajubu Emmanuel Ajayi
[1]Department of Mathematical Sciences, Achievers University Owo, Nigeria
[2]Department of Computer Science and Engineering, Obafemi Awolowo University, Ile -Ife, Nigeria
Olofintuyi.sundaysamuel@gmail.com

Abstract

Advent of the Internet of Things (IoTs) has technically increased the tremendous growth of computer networks and a number of applications are now used by individuals, groups, companies and governments. With this growth, cyber security poses a big challenge as cyber-attack are on the verge of collapsing some businesses. Thus, a data driven Intrusion Detection System (IDS) is needed to detect all the inconsistencies, structures and patterns of potential cyber-attacks on the computer network. The aim of this research is to propose the best supervised Machine Learning (ML) algorithm to be adopted in the perception phase of Situation Awareness (SA) model for threats detection. This paper employs ten various algorithms in the perception phase of a Situation Awareness (SA) model. The algorithms employed are; Artificial Neural Network (ANN), Support Vector Machine (SVM), Decision Tree (DT), ZeroR, ID3, Random Forest (RF), Baye Network (BN), NaiveBayes (NB), RepTree and J48 for threat detection on the computer network. All model's simulation were done in the WEKA environment using NSL-KDD 99 as the dataset. The efficiency, effectiveness and accuracy of each algorithm are compared with each other after model simulation. Final experimental results revealed that ANN gave 98.69% which is the highest accuracy and ZeroR gave 55.05% which is the least accuracy of the ten proposed algorithms.

Keywords: *Data driven Intrusion Detection System, Cyber Security, Cyber Attack, Supervised Machine Learning Algorithm, Situation Awareness*

1. Introduction

Cyber security defines the measures, defense, mechanism, technologies and structure designed to protect programs, data, networks and computers from unauthorized access, damages and cyber threats (Olofintuyi, 2021). One of the fast-growing aspects of Information Communication Technology (ICT) is the computer network and its applications, because of this prospect, cyber threats are also increasing and gaining ground in the cyber world (Olofintuyi and Omotehinwa, 2021). Cyber threats have caused a lot of damage and losses to individuals, research institutes, industries and governments. A lot of efforts have been put in place by industries, research institutes and governments to curb the activities of the intruders but all efforts seem not sufficient to handle the intruders (Olofintuyi, 2021). In year 2010, about 50 million malwares were recorded, in two years later, the number of the malwares has doubled to 100 million malwares and surprisingly in year 2019, the number of malwares has increased to 900 million malwares (Sarker *et al.,* 2020). According to Morgan (2021) the global cybercrime damage is predicted to cost about $ 6 trillion USD in 2021 and by 2025, it is expected to cost about $ 10.5 trillion USD annually. Hao *et al.,* (2020) stated that huge damages have been done by the attackers, the author identifies the action of intruders on American Medical Collection Agency (AMCA). The records of AMCA was hacked for almost a year and as a result of that, about 25 million hosts and 12 million records was hacked making the company to go bankrupt. The present mechanisms to curb cyber-threats such as user's authentication, hardware and software firewalls and data encryption seem not robust enough to handle the set of threats in the cyber world (Hamed *et al.,* 2020). Regrettably, all the conventional mechanisms are not efficient and effective enough as a guide against the

Online: ISSN 2645-2960; Print ISSN: 2141-3959

set of cyber- threats (Mohammadi *et al.,* 2019). For example, firewall does not indicate any signal when an internal attack takes place but only give a signal and prevent access when there is communication between two or more networks, because of this fact, a more accurate Machine Learning (ML) based Intrusion Detection System (IDS) will be needed for the security of the system. Generally, IDS is a system that detects abnormalities on a computer network. It also helps to check inconsistency, infectious activities and any attack pertaining to computer network securities such as probes, Denial of service (DoS), User to Root (U2R) and Root to Local (R2L). To guide against all these threats, IDS has been proposed (Sarker, 2019; Olofintuyi, 2021) IDS helps to monitor and also classify each threat to their respective classes for which both ML method and statistical method have been used. Statistical methods work on the assumption that certain distribution is either normal or abnormal communication, but with this assumption, the situation is not completely consistent and it becomes uneasy to completely determine the parameters (Zhao, 2020). For ML classifiers such as Artificial Neural Network (ANN) (Olofintuyi *et al.,* 2019; Kang and Kang, 2016), Decision Tree (DT) (Chen *et al.,* 2011), Support Vector Machine (SVM) (Shams and Rizaner, 2018) and Clustering (Lin and Ke, 2015) models, their performance is determined by False Negative (FN), False Positive (FP), True Negative (TN), True Positive (TP), Precision, Recall and accuracy. However, it is impossible for both ML method and statistical method to reach a satisfactory level based on their evaluation metrics because each of them is related to each other. For instance, if we want to reduce the FN in order to prevent the missing attacks, the FP by default may increase and vise-versa. Data driven IDS helps to identify the various classes of cyber threats, the patterns in the cyber threats are firstly analyzed which will help in predicting the classes of threats. To build data driven IDS, machine learning techniques are needed. However, there are different machine learning techniques for classifying security data, hence, each have different pattern of classifying threats on the computer network and produces different results based on their context for classifying cyber-threats (Olofintuyi and Omotehinwa, 2021; Sarker *et al.,* 2019). For these reasons, ten different machine learning algorithms which are; Artificial Neural Network (ANN), Support Vector Machine (SVM), Decision Tree (DT), ZeroR, ID3, Random Forest (RF), Baye Network (BN), NaiveBayes (NB), RepTree and J48 are examined at the perception phase of Situation Awareness (SA) model. Basically, the SA model has three phases which include the perception phase, comprehension phase and the projection phase. The perception detects threats on the network and the information is relayed to the comprehension phase. The comprehension phase is populated with instances (threats and non-threats) which also serves as a guide for the perception phase. The projection phase only gives out information to the administrator. (Olofintuyi, 2021; Olofintuyi *et al.,* 2019; Endsley, 1995). The focus of this research centers on the perception phase of SA model. The efficiency and effectiveness of each of the ten machine learning algorithms on the security dataset used are evaluated based on performance metrics such as; precision, recall and accuracy. The following sections discuss the literature reviewed, the methodology used, results obtained after the experimental results for each of the ten techniques used and the proposed future area of study.

2. Related Works

Cybersecurity threat is defined as a malicious program that gains access without the knowledge of the user where vital data has been stolen. The threats put the integrity of information and its confidentiality to stake. Various approaches such as cryptography, firewall and access control are the primary mechanism used for internal threats detection (Olofintuyi, 2021). However, both internal and external attacks are also detected by IDS. IDS helps to detect malicious events on the network and personal computer. Threat detection is done based on the assumption that the pattern of normal events is different from attack on the network (Stallings, 2003). IDS analyzes all the events that come to the network and classifies them based on their patterns and the feedback is reverted to the network administrator. IDS also helps the network administrator to handle auditing, monitoring and also accesses to the network (Olofintuyi *et al.,* 2019). Basically, IDS are classified into various types based on the perspective of users. We can have a Network based Intrusion Detection System (NIDS) and Host based Intrusion Detection System (HIDS) (Hamed *et al.,* 2020). In HIDS, its operation lies within a single system where an abnormality is checked for. Also, inconsistencies are also checked for in the operating system in HIDS while in NIDS, unwanted traffic such as malicious packets are checked between networks (Hamed *et al.,* 2020). Signature based Intrusion

Online: ISSN 2645-2960; Print ISSN: 2141-3959

Detection System (SIDS) or Anomaly based Intrusion Detection System (AIDS) is another approach to IDS based on the user's perspective. SIDS cannot detect attacks without the prior pattern available in the database of the administrator. From the name SIDS, a pattern must exist for the SIDS to effectively classify all the various groups of threats. A good example of SIDS is an expert system developed in the mid 1960 (Hao *et al.,* 2020) which uses a set of rules for its classification. SIDS is very effective and efficient in detecting known attacks but becomes inefficient and ineffective for detecting any variant of known attacks and any unknown attacks (Hamed *et al.,* 2020). Keeping the update of the signature and pattern of SIDS is a major setback. AIDS studies the pattern on the network and then develops its own pattern which is used for detection of novel threats on the network (Sarker *et al.,* 2020). Various techniques have been used for threat detection in AIDS and these techniques are classified either as ML and statistical technique (Olofintuyi and Omotehinwa, 2021). In statistical technique, the captured network traffic data is created along with the profile representing its behavior and this is based on the number of packets from different protocols, the traffic rate and the IP address distribution and so on. Machine learning can be supervised, unsupervised and semi supervised ML. The most common types of supervised ML are regression method and classification method (Sarker *et al.,* 2019). Future security problems have been predicted by the two aforementioned methods. For instance, classification techniques such as DT (Sarker *et al.,* 2019), SVM (Halim and Suryadibrata, 2021) Naïve Bayes (Sentuna *et al.,* 2021), OneR (Neeraj 2018) Logistic regression (Prokofiev *et al.,* 2018) and adaptive learning (Farhan *et al.,* 2019). All these algorithms have been used for classification of threats into their respective classes. Recently, Sarker *et al.,* (2020) proposed IntruTree and Olofintuyi (2021) presented ANN based DT which are used for threat classification on the network. For regression, it has been used to predict network parameters. It has also been used to detect the prevalence of cyber threats and fraud related to cybercrime (Hamed *et al.,* 2020). Linear regression (Alexander, 2020). Support Vector Regression (Halim and Suryadibrata, 2021) are two good examples of regression methods. The output of both regression and classification differs from each other. The output variable of regression is numerical or continuous while the output of classification methods is discrete. For the unsupervised ML, structures and patterns are detected in an unlabeled dataset (Sarker *et al.,* 2019). Clustering algorithm which is a good example of unsupervised ML can be used to detect the hidden patterns and structure in an unlabeled dataset. Unwanted instances can be eliminated by clustering algorithm in a given dataset, clustering algorithm can also be used for policy violation and also used to identify anomalies. Examples of clustering algorithms include K-mean (Virendra *et al.,* 2021) and K-medoids (Thomas *et al.,* 2020). Semi-supervised ML lies between supervised and unsupervised ML. For a labeled dataset in semi-supervised ML, less amount of time is needed in order to handle the dataset (Olofintuyi and Omotehinwa, 2021).

3. Methodology

In this section, ten (10) different ML algorithms were simulated in the perception phase of SA. Also, NSL-KDD 99 dataset which is an online security dataset was used during model building and training. The result of the model that gives the highest classification out of the 10 models is fed into the classification phase, and then into the comprehension phase and the final result is sent to the network administrator via the projection phase.

3.1 Dataset

The research work deploys NSL KDD 99 dataset for model training and simulation. The NSL KDD dataset is an online dataset which does not contain any redundant and irrelevant attributes, the dataset is an extract from KDD 99 dataset. The dataset has 41 features which is depicted in Table 1. The dataset has 59,277 instances, all the instances are numeric in nature and it ranges from different numbers. For threats classification, all the numeric values were converted to 0's and 1's. All the threats in the dataset are in four categories as explained below:

(a) **Denial of Service (DOS):** This is the first category of threats in NSL-KDD 99 dataset. The classes of threats engage the memory so as to be busy so that they are unable to attend to legitimate requests. Examples of DOS are: process table, ping of death, land, SYN flood, Back, mail bomb and land.

(b) **Root to local (R2L):** Packets of data are sent by these categories of threats to the end users, once the end user accepts such data, their system becomes vulnerable which gives the attackers access to their system. Examples of

Online: ISSN 2645-2960; Print ISSN: 2141-3959

R2L are; Guest, Dictionary, Xlock, Imap, FTP and write. Figure 1 depicts the proposed SA model and a suitable simulating tool WEKA was used.

(c) **User to root (U2R**): These sets of threats work as a legitimate user and as a result gain access to the computer system and then explore the system because they are now vulnerable. Examples of U2R are; Fdformat, Loadmodule, Xterm and Perl.

(d) **Probe:** This is the last category of attacks, the attackers approach the system and when he is able to access the system, the vulnerabilities of such system are then explored. Examples of probes are; Ipsweep, Satan, Saint, Nmap and Mscan.

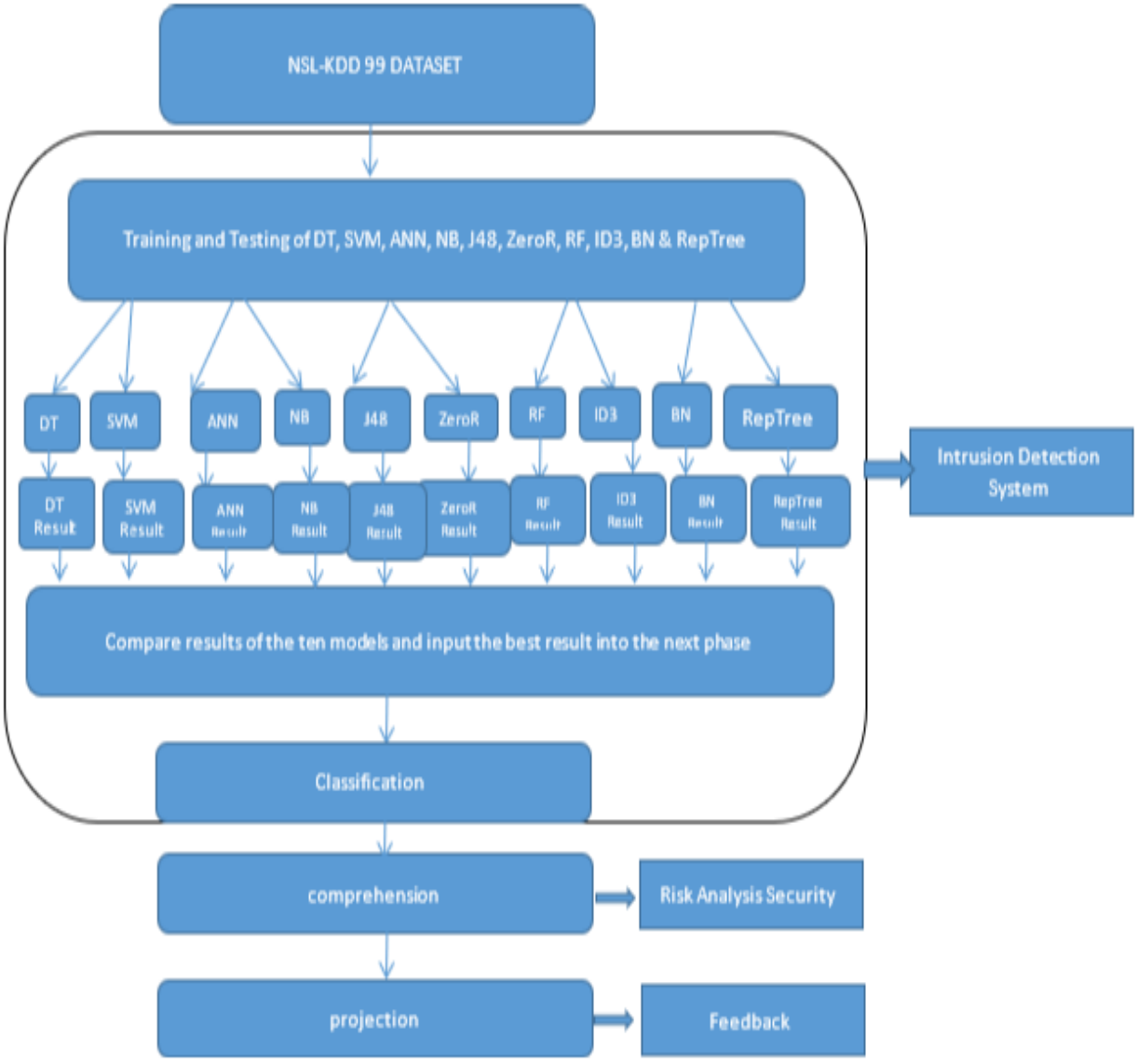

Figure 1: Proposed Situation Awareness Model

Table 1: 41 Features of NSL-KDD 99 used

Online: ISSN 2645-2960; Print ISSN: 2141-3959

No	Feature name	Types	NO	Feature Name	Types	NO	Feature name	Types
1	Duration	continuous	15	Su_attempted	Continuous	29	Same_srv_rate	Continuous
2	Protocol type	Symbolic	16	Num_root	Continuous	30	Diff_srv_rate	Continuous
3	service	Symbolic	17	Num_file creation	Continuous	31	Srv_diff_host_rate	Continuous
4	Flag	Symbolic	18	Num_shell	Continuous	32	Dst_host_count	Continuous
5	Scr_bytes	continuous	19	Num_access file	Continuous	33	Dst_host_srv_count	Continuous
6	Dst_bytes	Continuous	20	Num_outbound_cmds	Continuous	34	Dst_host_same_srv_rate	Continuous
7	Land	Symbolic	21	Is_host_login	symbolic	35	Dst_host_diff_srv_rate	Continuous
8	Wrong fragment	Continuous	22	Is_guest_login	symbolic	36	Dst_host_same_src_port_rate	Continuous
9	Urgent	Continuous	23	count	Continuous	37	Dst_host_srv_diff_host_rate	Continuous
10	Hot	Continuous	24	Srv_count	Continuous	38	Dst_host_serror_rate	Continuous
11	Num_failed login	continuous	25	Serror_rate	Continuous	39	Dst_host_srv_rate	Continuous
12	Logged_in	Symbolic	26	Srv_serror_rate	Continuous	40	Dst_host_srv_serror_rate	symbolic
13	Num_compromised	Continuous	27	Rerror_rate	Continuous	41	Dst_host_serror_rate	symbolic
14	Root_shell	Continuous	28	Srv_rerror_rate	Continuous			

3.2 Model 1 Decision Tree (DT) Is the first algorithm used in the perception phase of SA model for threats detection. DT has a tree like structures that has branches, leaves and internal nodes. As used in this algorithm, the branches are used to represent the outcome while the leaves are used to represent the class label. The internal nodes are used to represent the attributes used in the NSL-KDD 99 dataset. DT uses historical dataset for threats detection and classifies each group of threat into their respective categories. Each of the groups of threats are categorized into various groups by the leaf. If the output gives 1000, it is classified as DOS, if the output is 0100, it is classified as R2L, if the output is 0010 it is classified as U2R and if the output is 0001, it will be classified as a probe. Table 2 below depicts the various classes as being categorized by DT

Table 2: Threats classification based on their group

Online: ISSN 2645-2960; Print ISSN: 2141-3959

S/N	Attack Group	Different attacks	Output
1	Denial of service attack	Process table, Ping of death, Land, SYN, Flood, Back, Mail bomb and Land.	1000
2	Root to local	Guest, Dictionary, Xlock, Imap, FTP and write.	0100
3	User to root	Fdformat, Loadmodule, Xterm and Perl.	0010
4	Probes	Ipsweep, Satan, Saint, Nmap and Mscan	0001

3.3 Model 2 Support Vector Machine (SVM): SVM is a supervised ML algorithm which uses hyperplane to classify the various points in space into various categories. The threats are classified into four categories and the result is optimum when Equation 1 is at maximum which depends directly on Equation 2 and Equation 3 respectively.

$$\min \frac{1}{2} \parallel W_t \parallel^2 \ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{Equation 1}$$

$X_\alpha Y_\alpha \ldots\ldots (X_\beta Y_\beta)\ \gamma \epsilon (1,0)\ where\ X_\alpha Y_\alpha \ldots\ldots (X_\beta Y_\beta)$ are trained data, Y falls between the category of (0 and 1) and β is used to depict the number of samples. The weight of the input is depicted by W_t while the bias is depicted by b_t, the input features are depicted by χ. The various categories are being represented by the formula below

$$(W_t.X) + b_t \geq Y_i\ if\ Y_i = 1 \qquad Equation\ 2$$
$$(W_t.X) + b_t \leq Y_i\ if\ Y_i = 0 \qquad Equation\ 3$$

Each of the groups of threats are categorized into various groups by the hyperplane. If the output gives 1000, it is classified as DOS, if the output is 0100, it is classified as R2L, if the output is 0010 it is classified as U2R and if the out is 0001, it will be classified as probe as shown in Table 2 above

3.4 Model 3 Artificial Neural Network (ANN): Is a supervised ML which has three segments. The input layer, hidden layer and the outer layer. The hidden layer uses sigmoid activation function for its operation. The online NSL-KDD 99 dataset serves as an input into the input layer of ANN. The categories of threats in the dataset are then categorized into their respective classes as shown in Table 2. If the output gives 1000, it is classified as DOS, if the output is 0100, it is classified as R2L, if the output is 0010 it is classified as U2R and if the output is 0001, it will be classified as a probe. The feature of each threat is used as an input variable into the input layer and it is determined by:

$$\delta_a = (\delta_1 \delta_2 \delta_3 \ldots\ldots\ldots\ldots \delta_n) \qquad Equation\ 4$$

The number of variables is depicted by a . At layer X the synaptic weight on the input neuron is shown in equation below:

$$M_x = W_{1X}\delta_1 + W_{2X}\delta_2 + \cdots \ldots\ldots\ldots\ldots + W_{nx}\delta_n + b \qquad Equation\ 5$$

The sigmoid function limits the output of a threshold [+1, 0]. The difference between the actual output and expected output is measured with square error measure (E)

$$E = (P - Q)^2 \qquad \text{Equation 6}$$

The network weight needs to be calculated with respect to square error function. To redefine the square error function, ½ is used to cancel Exponential 2 when differentiating.

$$E = \frac{1}{2}\ (P - Q)^2 \ldots\ldots\ldots\ldots Equation\ 7$$

Output β_x defines each neuron X.

Online: ISSN 2645-2960; Print ISSN: 2141-3959

$$\beta_x = Q(net_x) = Q\sum_{k=1}^{n} W_{ax}\delta_a \qquad Equation\ 8$$

Whenever the activation function θ is differentiated, derivative of Equation 2 is:

$$\frac{d\theta}{dz} = \theta(1-\theta) \qquad Equation\ 9$$

The partial derivative of error (E) was derived by using chain rule with respect to the weight W_{ax}

$$\frac{dE}{dw_{ax}} = \frac{dE}{d_{\beta x}}\frac{d\beta_x}{dnet_x}\frac{dnet_x}{dW_{ax}} \qquad Equation\ 10$$

From Equation 8, terms on the left-hand side can be calculated as:

$$\frac{dnet_x}{dW_{ax}} = \frac{d}{dW_{ax}}\left(\sum_{k=1}^{n} W_{ax}\delta_a\right) = \delta_a \qquad Equation\ 11$$

$$\frac{d\beta_x}{dnet_x} = \frac{d}{dnet_x}\beta(net_x) = \beta(net_x)\big(1-\beta(net_x)\big) \qquad Equation\ 12$$

Let Q be the outer layer such that $Q = \beta_x$, the first term is obtained by differencing error function in Equation 7

$$\frac{dE}{d\beta_x} = \frac{dE}{d\beta} = \frac{d\,1}{\frac{dx}{2(P-Q)}} = Q - P \qquad Equation\ 13$$

When E is given as a function of all the input neuron, the recursive expression for the derivative is derived as follows:

$$\frac{dE}{d\beta_x} = \sum_{aEL}\left(\frac{dE}{dnet_a}\frac{dnet_a}{d\beta_x}\right) = \sum_{aEl}\frac{dnet_a}{dnet_\beta}\frac{d\beta_a}{dnet_a}W_{ax}) \qquad Equation\ 14$$

3.5 Model 4 Naïve Bayes (NB) Model: NB is another supervised ML used at the perception phase of SA model. NB uses probability technique to estimate the probability and then classify the cyber-threats in a given dataset into their respective classes. NB considers each feature of the dataset as independent and it also considers the correlation that exists between the features. NB uses both class probability and conditional probability. To obtain the class probability, the total instances is used to divide the frequency of each class instance while for a given class, the occurrence of each attribute and occurrence of sample for the same class determines the conditional probability. Each threat in the dataset is classified into four respective classes as shown in Table 2.

3.6 Model 5 J48 Model: J48 is an implementation of C4.5 algorithm, it is also an extension of ID3. J48 accounts for missing values, continuous attribute value range, decision trees pruning and derivative of rules. J48 calculates the values of a new sample from the available dataset. The attributes are being denoted by the internal node while the final output is determined by the terminal nodes. Each classes of threats are classified into their respective class as shown in Table 2

3.7 Model 6 ZeroR Model: ZeroR is one of the simplest ML algorithm classifiers. ZeroR ignores all predictors and relies on the targeted values. Majority of the class in terms of category are predicted by ZeroR. ZeroR algorithm does not have the predictability power, it is most suitable to be used as a baseline for other classifiers. It uses frequency table for threats classification and then the most frequent value is selected and grouped to their respective classes as depicted in Table 2

3.8 Model 7 Random Forest (RF) Model: RF is another ML algorithm used in the perception phase of SA model for threat detection. This algorithm adopts both regression and classification methods in its operation. RF uses DT on the NSL-KDD 99 dataset by random sampling from the dataset and predictions are made from the DT of each sample. Voting method is performed on the predicted results, results with the highest votes are predicted and classified to their classes as shown in Table 2.

3.9 Model 8 Iteration Dichotomiser 3 (ID3) Model: another algorithm used in the perception phase of SA model is the ID3 algorithm. Top-down greedy approach is being used by the ID3 algorithm. The algorithm starts building

Online: ISSN 2645-2960; Print ISSN: 2141-3959

its tree from the top and the best feature is selected at each iteration and a node is established. The node classifies the threats into their respective classes as depicted in Table 2

3.10 Model 9 Baye Network (BN) Model: BN is a supervised ML algorithm used in the perception phase of SA. For prediction of threats, BN adopts probability theory. The probability theory is a derivative from the Bayes theory as follows:

$$P\left(\frac{a}{b}\right) = \frac{P\left(\frac{a}{b}\right) * P(a)}{P(b)} \qquad Equation\ 15$$

The input variables of the dataset are being represented by a while the attack group is represented by b. Equation 15 can be re-written as:

$$P\left(\frac{a}{b}\right) = P\left(\frac{a_1}{b}\right) * P\left(\frac{a_2}{b}\right) * \ldots\ldots\ldots P\left(\frac{a_n}{b}\right) \qquad Equation\ 16$$

Since the attack group (b) is the focus, and the input features are constant, a which is the input variable can be removed from the Equation and introduce proportionality. The Equation then gives:

$$P\left(\frac{b}{a}\right) \alpha P\left(\frac{a}{b}\right) * P(S) \qquad Equation\ 17$$

$$\text{Or } P\left(\frac{b}{a}\right) \alpha P(b) * \prod_{i=1}^{n} P\left(\frac{a_i}{b}\right) \qquad Equation\ 18$$

Maximum value is obtained from the targeted group when Argmax is introduced into Equation 15. BN classifies the attack group as depicted in Table 2

$$b = argmax_b\{P(a) * \prod_{i=1}^{n} P\left(\frac{a_1}{b}\right) \qquad \text{Equation 19}$$

3.11 Model 10 Reduced Error Pruning Tree (RepTree) Model: RepTree is the last model used for threats detection and classification in the perception phase of SA model. The algorithm adopts regression tree logic and multiple trees are created in different iterations. From the multiple trees created, the best one is selected which is used to represent others. The prediction made by the tree is being pruned by using mean square error. The best tree is used to classify threats in the NSL-KDD 99 dataset into their respective classes as depicted in Table 2.

3.12 Performance Evaluation: The following metrics were used to evaluate the 10 different supervised ML algorithms in the perception phase of SA model.

False Positive: This wrongly defines events that are negative as positive

False Negative: Events which are positive are wrongly predicted to the network administrator as negative

True Positive: Positive events on the network are correctly predicted to the network administrator

True Negative: This also correctly predict negative event to the network administrator as negative events

Recall: Describe the completeness and quantity of the models

$$Recall = \frac{TP}{TP + FN} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (20)$$

Precision: The exactness and quality of the models are being described by this metric

$$Precision = \frac{TP}{TP + FP} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (21)$$

Accuracy: Accuracy describes how effective models are for threats classification.

$$Accuracy = \frac{TP + TN}{TP + FN + FP + TN} \ldots\ldots\ldots\ldots\ldots \quad (22)$$

Online: ISSN 2645-2960; Print ISSN: 2141-3959

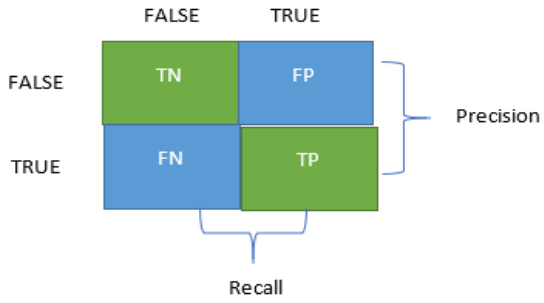

Figure 2: Confusion Matrix for Evaluation

3.13 Experimental Setup

10 different ML models were built and evaluated in Waikato Environment for Knowledge Analysis (WEKA). WEKA has gained popularity among researchers for model simulation because of its flexibility, accessibility and ease of usage. The dataset used in this experiment is an online dataset. It is an extract from KDD 99 dataset and because of this, all the redundant and irrelevant features have been removed. For WEKA to recognize the dataset, it must be in arff format. The dataset was firstly saved in CSV format and later converted to arff format so that WEKA can recognize it. 10-fold cross validation was adopted where the dataset was divided into 10 samples, 9 out of the 10 samples was used for training of the models and the testing was done with the last one sample. The performance evaluation of the models was determined by the number of instances they were able to correctly classify. After the whole experiment, all the models were compared against each other.

4. Results and Discussion

The efficiency and effectiveness of all the models were determined based on how they were able to correctly classify instances. Evaluation results of all the models in the perception phase of SA model is discussed as follows; BN Model (Model 1) classified 50,588 instances correctly and 8689 instances were wrongly classified. Model 1 gave a Recall of 0.790, Precision 0.871 and 0.8534 accuracy. NB Model (Model 2) correctly classified 50,393 instances and wrongly classified 8881 instances. Model 2 gave a Recall of 0.7898, Precision 0.865 and 0.8501 accuracy. ANN Model (Model 3) classified 58,502 instances correctly and 772 instances incorrectly. Model 3 gave a Recall of 0.993, Precision: 0.979 and 0.9869 accuracy. SVM Model (Model 4) classified 58116 instances correctly and 1158 were wrongly classified. Model 4 also gave the following results; Recall: 0.978, Precision: 0.978 and Accuracy: 0.9804. DT Model (Model 5) correctly classified 58309 instances and wrongly classified 965 instances. Model 5 also gave the following results; Recall: 0.986, Precision: 0.978 and Accuracy: 0.9836. ZeroR Model (Model 6) classifies 32630 instances correctly and 26644 were wrongly classified. Model 6 gave the following results; Recall: 0.021, Precision: 0.61 and Accuracy: 0.5505. ID3 Model (Model 7) classifies 57344 instances correctly and 1930 instances incorrectly. Model 7 gave the following results; Recall: 0.957, Precision: 0.971 and Accuracy: 0.9674. RF Model (Model 8) classified 57923 instances correctly and 1351 instances incorrectly. Also, Model 8 gave the following results; Recall: 0.971, Precision: 0.978 and Accuracy: 0.9772. Model 9 which is RepTree correctly classifies 58502 instances and wrongly classifies 772 instances. Also, Model 9 gave a Recall of 0.993; Precision: 0.979 and Accuracy of 0.9869. Finally, J48 Model (Model 10) classifies 58309 correctly and 965 instances were wrongly classified. Model 10 also gave the following results; Recall: 0.986, Precision: 0.978 and Accuracy: 0.984. Figure 3, 4, 5, 6, 7, 8, 9, 10, 11 and 12 depicts the confusion matrix for all the models.

Online: ISSN 2645-2960; Print ISSN: 2141-3959

Figure 3: Confusion matrix for BN (Model 1)

Figure 4: Confusion matrix for NB (Model 2)

Figure 5: Confusion matrix for ANN (Model 3)

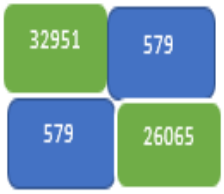

Figure 6: Confusion matrix for SVM (Model 4)

Figure 7: Confusion matrix for DT (Model 5)

Figure 8: Confusion matrix for ZeroR (Model 6)

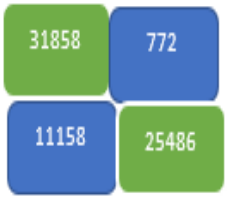

Figure 9: Confusion matrix for ID3 (Model 7)

Figure 10: Confusion matrix for RF (Model 8)

Figure 11: Confusion matrix for RepTree (Model 9)

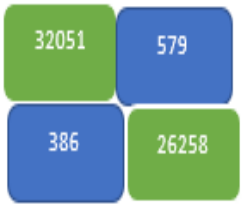

Figure 12: Confusion matrix for J48 (Model 10)

4.1 Performance Comparison of all Models

Table 3 depicts the results of all the models showing the TP, TN, FP and FN. After the simulation, it was observed that the ZeroR model gave the least accuracy for threats detection while the ANN model gave the highest detection of threats. Figure 13 depicts the performance bar chart for all the models used. The best ML algorithm (ANN) is

Online: ISSN 2645-2960; Print ISSN: 2141-3959

compared with Aslahi-Shahri, (2016) and Mustapha and Sulaiman (2016) in terms of accuracy. Aslahi-Shahri, (2016) gave 97.31% accuracy while Mustapha and Sulaiman (2016) gave 89.28% accuracy. But the proposed algorithm gave 98.69 accuracy

Table 3: Evaluation table for the 10 models

Classifiers	**No of instances**	**TN**	**TP**	**FN**	**FP**	**Precision**	**Recall**	**Accuracy**
BN (Model 1)	59,277	29543	21045	5599	21045	0.872	0.790	0.8534
NB (Model 2)	59,277	29348	21045	5599	3282	0.8650	0. 7898	0.8501
ANN (Model 3)	59277	32051	26451	193	579	0.9785	0.9928	0.9869
SVM (Model 4)	59,277	32051	26065	579	579	0.9783	0.9783	0.9804
DT (Model 5)	59,277	32051	26258	386	579	0.9784	0.9855	0.9836
ZeroR (Model 6)	59,277	32051	579	26258	386	0.6014	0.02163	0.5505
ID3 (Model 7)	59,277	31858	25486	1158	772	0.9706	0.9565	0.9674
RF (Model 8)	59,277	32051	25872	772	579	0.9781	0.9710	0.9772
RepTree (Model 9)	59,277	32051	26451	193	579	0.9786	0.9928	0.9862
J48 (Model 10)	59,277	32051	26258	386	579	0.9784	0.9855	0.9837

Online: ISSN 2645-2960; Print ISSN: 2141-3959

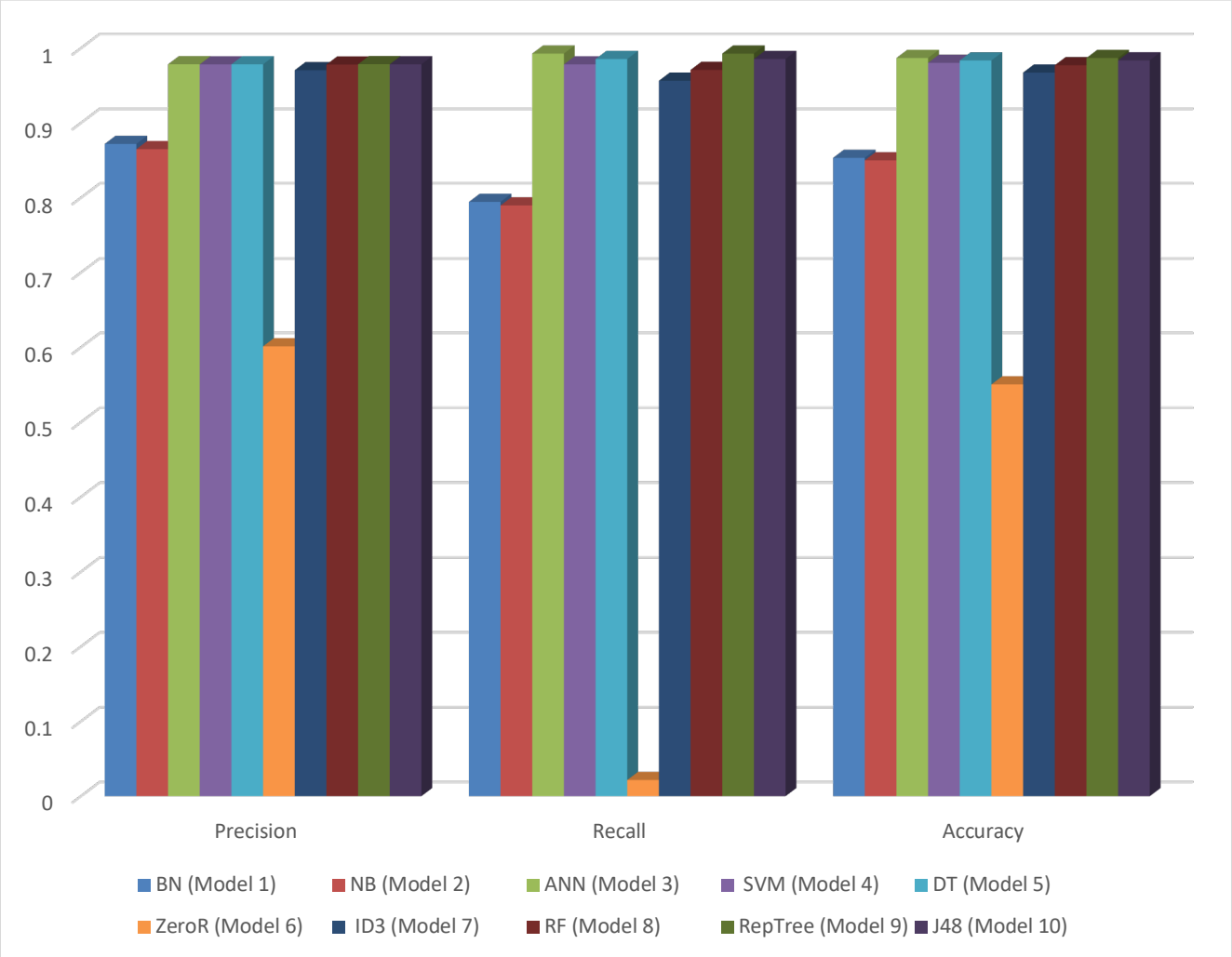

Figure 13: Evaluation of 10 machine learning algorithms based on Precision, Recall and Accuracy

5. Conclusion

Due to the damages caused by cyber threats to companies, groups, individuals and governments, the effectiveness and efficiency of ML based IDS is a great concern to all these bodies. Largely speaking, there are different categories of cyber-attacks in a given cyber security dataset with different relevant features. Hence, the performance of some of the classifiers may not be the same because the prediction rate is based on the different features of the cyber-security dataset used. This research took into account by considering the effectiveness and efficiency of some of the popular ML techniques used for prediction. Also, each model was evaluated based on Recall, Precision and Accuracy. The research work shows that ANN gave the highest accuracy and ZeroR gave the least accuracy in the perception phase of the SA model. Future work will focus on the usage of other cyber-security dataset and also to design an automated data driven IDS so as to give notification to the cyber security community.

Reference

Online: ISSN 2645-2960; Print ISSN: 2141-3959

[1] Halim, L. and Suryadibrata, A. (2021). Cyberbullying Sentiment Analysis with Word2Vec and One-Against-All Support Vector Machine. *International journal of new media technology*, 8(1), 57-64.

[2] Olofintuyi, S.S. (2021). Cyber Situation Awareness Perception Model for Computer Network. *International journal of advanced computer science and application.* 12(1), pp. 392-397.

[3] Olofintuyi, S.S. and Omotehinwa, T.O. (2021). Performance Evaluation of Supervised Ensemble Cyber Situation Perception Models for Computer Network. *Computing, Information Systems, Development Informatics & Allied Research Journal.* 11(2), pp. 1-.14.

[4] Sentuna, A., Alsadoon, A. and Prasad, P. (2021). A Novel Enhanced Naïve Bayes Posterior Probability (ENBPP) Using Machine Learning: Cyber Threat Analysis. Neural Process Lett, 177–209.

[5] Virendra, K., Asha, A. and Suman, K. (2021). Big data security enhancement based intrusion detection system using k-mean clustering of decomposited features, *Information Technology in Industry*, 9(1), pp. 36-48

[6] Morgan, S. Cyberwarfare in the suite (2021). Cyber security magazine. Publish by cybersecurity ventures

[7] Alexander, R. (2020) Using Linear Regression Analysis and Defense in Depth to Protect Networks during the Global Corona Pandemic. *Journal of Information Security*, 11, 261-291. doi: 10.4236/jis.2020.114017.

[8] Thomas T., P. Vijayaraghavan A. and Emmanuel S. (2020) Machine Learning and Cybersecurity. In: Machine Learning Approaches in Cyber Security Analytics. *Springer,* Singapore. https://doi.org/10.1007/978-981-15-1706-8_3

[9] Hao, Z., Feng, Y., Koide, H. and Sakurai, K. (2020). A sequential detection method for intrusion detection system based on artificial neural networks. *International Journal of Networking and Computing*, 10, pp. 213-226

[10] Hamed, A., Igbal, H.S., Asra, K., Syed, M. H., Sheikh, I. and Sohrab, H. (2020). Cyber Intrusion Detection using Machine Learning Classification Techniques. *Springer Nature Singapore*. pp. 121–131

[11] Sarker, H., Kayes, A., Badsha, S., Alqahtani, H., Waters, P. and Alex, N. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big data*.

[12] Sarker, H. Abushark. Y., Alsolami, F. and Khan, A. (2020). Intrudtree: a machine learning-based cyber security intrusion detection model. *Symmetry*, 12, pp.754-761.

[13] Zhao, H., Feng, Y., Koide, H. and Sakurai, K. (2020). A sequential detection method for intrusion detection system based on artificial neural networks. *International Journal of Networking and Computing*, 10, pp.213-226

[14] Farhan, U., Hamad, N., Sohail, J., Shehzad, K., Muhammad A., Fadi Al-turjman, L. (2019). Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach, in *IEEE Access*, vol. 7, pp. 124379-124389.

[15] Mohammadi, S., Mirvaziri H., Ghazizadeh-Ahsaee, M. and Karimipour, H. (2019). Cyber intrusion detection by combined feature selection algorithm. *Journal of Information Security and Application*, 44, pp. 80-88

[16] Olofintuyi, S.S., Omotehinwa, T. O., Odukoya, O.H. and Olajubu, E. A. (2019). Performance comparison of threat classification models for cyber-situation awareness. Proceedings of the OAU Faculty of Technology Conference, 305-309.

[17] Sarker, H., Kayes, A. and Watters, P. (2019). Effectiveness analysis of machine learning classification models for predicting personalized context-aware smartphone usage. *Journal of Big Data*

[18] Sarker, H. (2019). A machine learning based robust prediction model for real-life mobile phone data. *Internet of Things*, 5, pp.180-193

[19] Prokofiev, A., Smirnova, Y. and Surov, V. (2018). A method to detect Internet of Things botnets, 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pp. 105-108.

Online: ISSN 2645-2960; Print ISSN: 2141-3959

[20] Shams, E. A., and Rizaner, A. A. (2018). A novel support vector machine-based intrusion detection system for mobile ad hoc networks. *Wireless Networks*.

[21] Mustapha, M. and Sulaiman, M. (2016). Improving anomalous rare attack detection rate for intrusion detection system using support vector machine and genetic programming. *Neural Processing Letters*.

[22] Kang, M., and Kang, J. W. (2016). Intrusion detection system using deep neural network for in-vehicle network security. PLoS one

[23] Aslahi-Shahri, B. (2016). A hybrid method consisting of ga and svm for intrusion detection system. *Neural computing and applications,* 27(6), 1669-1676.

[24] Lin, W. C. and Ke, S. W. (2015). An intrusion detection system based on combining cluster centers and nearest neighbors. Knowledge-based system.

[25] Stallings W. (2003). Cryptography and network security: principles and practices

[26] Endsley M. (1995). Toward a theory of situation awareness in dynamic systems. *In Human Factors Journal*, 37, pp.32-64.