PERFORMANCE ANALYSIS OF MACHINE LEARNING ALGORITHMS FOR IDS

[1]K.Priyanka, [2]Dr. R. Jegadeesan [3]V.Neelima, [4]S.Divya, [5]K.Sairamachari, [6]M.Ganesh

[2,3]Assoc.prof, [1,4,5,6]B.Tech Final Year Students-Computer Science and Engineering

[1,2,3,4,5,6]Jyothishmathi Institute of Technology and Science, karimnagar, India

Abstract : Any abnormal activity will be assumed to be anomalies intrusion. Intrusion could be a major issue that is to be addressed and should be detected. Intrusion detection could be a central a part of security tools, such as reconciling security appliances, intrusion detection systems, intrusion interference systems, and firewalls. Different techniques have been used for intrusion detection however their attainment is a problem. The performance of intrusion detection system primarily depends on accuracy that must produce less warning and high detection rate. To resolve the problems related to performance the techinques like support vector machine(SVM),Multi layer perceptron and different techniques are utilized in recent work. These techniques impose bound limitations and conjointly not applicable for big knowledge sets, like system and network knowledge. This downside is addressed during this paper by introducing well-known economical machine learning algorithms like SVM,random forest, and extreme learning machine(ELM). These techniques are well-known due to their ability in classification.

IndexTerms **-Detection rate, extreme learning machine, SVM, Warning**.

I. INTRODUCTION

Intrusion may be a severe issue in security and a chief drawback of security breach, as a result of one instance of intrusion will steal or delete information from laptop and network systems in a few seconds. Intrusion can even harm system hardware. Furthermore, intrusion will cause large losses financially and compromise the IT vital infrastructure, thereby leading to data inferiority in cyber war. Therefore, intrusion detection is very important. Different intrusion detection techniques are obtainable, but their accuracy remains associate issue; accuracy depends on detection and warning rate, the matter on accuracy desires to be self-addressed to cut back the false alarms rate and to increase the detection rate. This notion was the impetus for this analysis work. Thus, support vector machine (SVM), random forest (RF), and extreme learning machine (ELM) applied during this work; these ways are proved effective in their capability to deal with the classification. Intrusion detection mechanisms are valid on a standard dataset, KDD. This work used the NSL-knowledge discovery and data processing (KDD) dataset, that is associate degree improved type of the KDD and is taken into account a benchmark within the analysis of intrusion detection strategies. The remainder of the paper is organized as careful below. The connected work is given in Section II. The projected model of intrusion detection to that totally different machine learning techniques are applied is delineate in Section III. The implementation and results ar mentioned in Section IV. The paper is finished in Section V, that provides a summary and directions for future work.

II. RELATED WORK

Verifying pc and system data is imperative for associations and individuals because of traded off data will cause sizeable damage. To maintain a strategic distance from such conditions, interruption recognition frameworks zone unit essential. As of late, unique AI approaches are anticipated to improve the execution of interruption location frameworks. Wanget al arranged partner degree interruption location system dependent on SVM and substantial their strategy on the NSL-KDD dataset. They guaranteed that their procedure, that has 99.92% adequacy rate, was better than various methodologies; in any case, they neglected to make reference to utilized dataset measurements, scope of preparing, and testing tests. Yet in addition, the SVM execution diminishes once huge data zone unit concerned, partner degree and it is anything but a perfect option for dissecting huge system traffic for interruption identification.

Cortes C, Vapnik VN [1], exhibited SVM which utilizes the NSL-KDD informational index is a refined adaptation of its forerunner KDD‟99 informational collection with a sizable measure of value information which emulates the ongoing can just train and test an interruption location framework. The NSL-KDD dataset is utilized to assess the proposed strategy, and the exact outcomes demonstrate that it accomplishes a superior and more vigorous execution than existing strategies as far as exactness, location rate, false caution rate and preparing speed.

An epic help vector machine (SVM) show consolidating part essential segment investigation (KPCA) with hereditary calculation (GA) is proposed by J.H. Lee, J.H. Lee, S.G. Sohn, et al [2], for interruption recognition. In the proposed model, a multi-layer SVM classifier is received to appraise whether the activity is an assault, KPCA is utilized as a preprocessor of SVM to lessen the component of highlight vectors and abbreviate preparing time. So as to decrease the commotion brought about by highlight contrasts and improve the execution of SVM, an improved bit work (N-RBF) is proposed.

In AI, a blend of classifiers, known as a ensemble classifier, which is a model created by Nelcileno Virgílio de Souza Araújo [3], frequently beats singular ones. While numerous gathering approaches exist, it remains, be that as it may, a troublesome errand to locate a reasonable ensemble design for a specific dataset. This paper proposes a novel gathering development strategy that utilizes PSO produced loads to make troupe of classifiers with better exactness for interruption discovery.

Random forest (RF) is a group classifier this model was presented by Ujwala Ravale, Nilesh Marathe, Puja Padiya [4], used to improve the precision. Random forest comprises of numerous choice trees. Random forest has low characterization error compared with other customary grouping calculations. Number of trees, least hub size and number of highlights utilized for part every hub. Points of interest of RF are recorded beneath. 1) Generated forests can be put something aside for future reference. 2) Random forest defeats the issue over fitting. 3) In RF exactness and variable significance is naturally produced. Highlight choice (FSS) is a pre preparing step usually utilized in information mining. It is viable in dimensionality decrease and evacuates irrelevant features along these lines builds exactness.

Intrusion Detection Systems provide police assistance, prevention and resistance to unauthorized access. Thus, Aburomman Reaz Reaz [5] planned a classification of the group, which could be a combination of PSO and SVM; this rating surpassed 92.90% on various roads. The data discovery and processing dataset was used in 1999 (KDD99), which has previously reported defects. What's more, SVM is not a good choice for massive analytics, as its performance deteriorates as the volume of information grows. Raman et al. Fellow planned in the detection mechanism of nursing penetration supported the base graph Algorithm Genetic Hyper (HG-GA) to prepare the parameter and have an option in SVM. They claimed that their methodology outperformed current approaches with a 97.14% detection rate on associates in the NSL-KDD nursing dataset. It was used to test and verify intrusion detection systems.

We consider the problem of intrusion detection in the computer network, investigate the use of maximum learning machines (ELMs) to classify and detect interventions. With increased communication between networks, the risk of information systems on external attacks or interventions has increased significantly. Chi cheng [6] Automated learning methods such as transmission support devices (SVMs) and neural networks have been used extensively to detect intrusion. These methods generally suffer from long training periods, requiring control of transactions, or not performing well in classifying multiple layers.We suggest a basic ELM method based on random features, the ELM-based method of the nucleus of the classification. We compare our methods with commonly used SVM techniques in both binary and multi-layered classifications. The simulation results show that the proposed ELM core proposal outperforms SVM in the speed of training and testing, while the kernel-matching ELM achieves higher detection accuracy than SVM in a multi-layer classification.

Farnaz and Jabbar [7] developed a model for the RF-assisted intrusion detection system. They tested the effectiveness of their model on associates in the NSL-KDD nursing dataset, and their results were non-tabular at 99.67% detection compared to J48. The most fundamental limitation of the RF algorithm is that many trees can create a slow mathematical base for time prediction. Elbasiony et al. Planned for the RF-supported intrusion detection model and k-weighted; it corrects its model on the KDD99 data set. The results of the system are indisputable with 98.3% accuracy. RF is not suitable for predicting real traffic due to its slowness, thanks to the formation of a large range of trees. To boot, the KDD99 data set refers to some restrictions as has been said.

III. PROPOSED MODEL

The key phases of the planned model embrace the dataset, preprocessing, classification, and evaluation analysis. Every part of the planned system is very important and adds valuable influence on its performance. The core focus of this work is to research the performance of various classifiers, namely, SVM,

RF, and ELM in intrusion detection. Figure one demonstrates the model of intrusion detection system planned during this work.The proposed model involves certain steps which are represented in the architecture of proposed model.The loaded data set is preprocessed and then it is subjected to classification and then evaluation is performed.

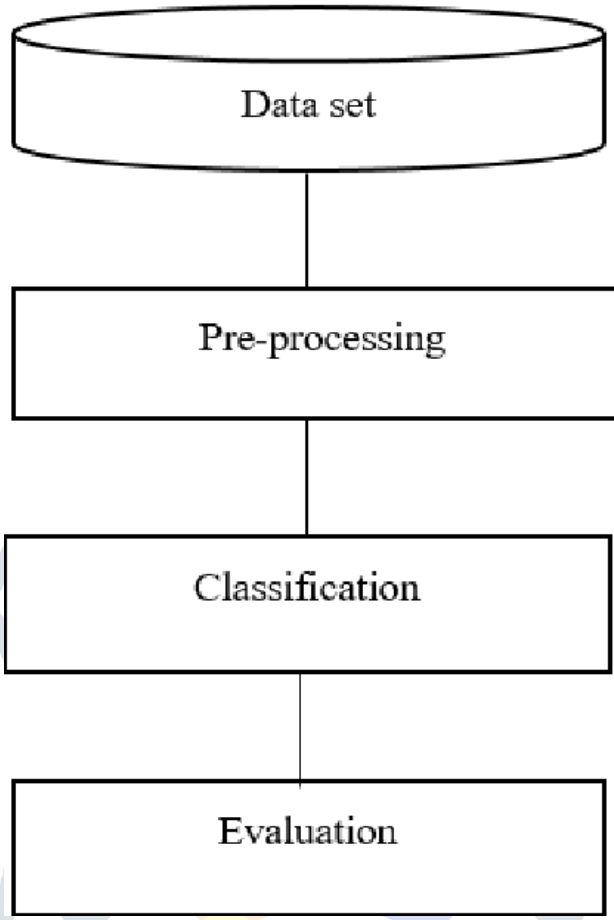

Figure 1. Proposed model for intrusion detection system

A. Dataset

Dataset choice for experimentation may be a vital task, as a result of the performance of the system is predicated on the correctness of a dataset. The more accurate the information, the bigger the effectiveness of the system. The dataset will be collected by various suggests that, like 1) change dataset, 2) simulated dataset, 3) testbed dataset, and 4) normal dataset. However, complications occur within the application of the primary three methodologies. A true traffic methodology is dear, whereas the change methodology is unsafe. The event of a simulation system is additionally complicated and difficult to boot. Differing kinds of traffic square measure required to model numerous network attacks, that is complicated and expensive. To beat these difficulties, the NSL–KDD dataset is employed to validate the projected system for intrusion detection.

B. Preprocessing

The classifier is unable to method the raw dataset as a result of a number of its symbolic options. Thus, preprocessing is essential, during which non-numeric or symbolic options are eliminated or replaced, as a result of they are doing not indicate important participation in intrusion detection. However, this method generates overhead as well as a lot of coaching time; the classifier's design becomes advanced and wastes memory and computing resources. Therefore, the non-numeric options are excluded from the raw dataset for improved performance of intrusion detection systems.

C. Classification

Placing an activity into traditional and intrusive classes is the core activity of intrusion detection system, which is known as the intrusive analysis engine. Thus, different classifiers are applied as intrusive analysis engines in intrusion detection within the literature, like multilayer perceptron, SVM, naive Thomas Bayes, self-organizing map, and DT. However, during this study, the 3 completely different classifiers of

SVM, RF, and ELM area unit applied supported their proved ability in classification issues. Details of every classification approach area unit provided

1) Support Vector Machine

SVMs were at the start projected by Vapnik (1995) for determination problems of classification and multivariate analysis. SVM is a supervised learning technique that's trained to classify different classes of information from numerous disciplines. These have been used for two-class classification issues and area unit applicable on each linear and non-linear information classification tasks. SVM creates a hyperplane or multiple hyperplanes in a high-dimensional house, and also the best hyperplane in them is that the one that optimally divides information into completely different classes with the biggest separation between the categories. A non-linear classifier uses numerous kernel functions to estimate the margins. The most objective of those kernel functions (i.e., linear, polynomial, radial basis, and sigmoid) is to maximize margins between hyper-planes. Recently, several extremely promising applications are developed by researchers because of the increasing interest in SVMs.

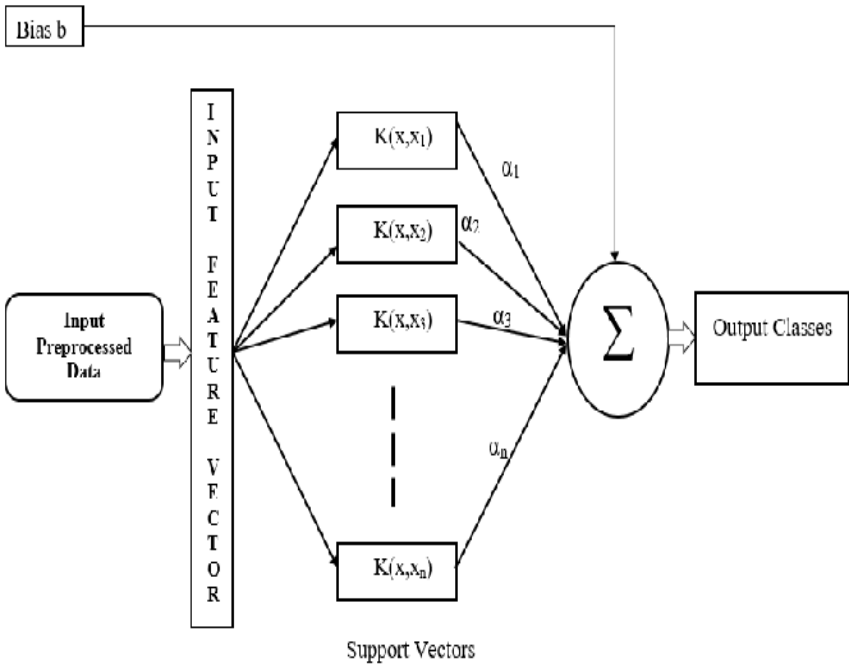

Figure 2. Architecture of the SVM for intrusion detection

The figure 2 illustrates the design of the SVM classification model within the projected intrusion detection system. We have used the radial basis perform (RBF) kernel for the implementation of the SVM model within the projected system. The kernel perform uses square geometrician distance between 2 numeric vectors and maps information|input , file|computer file} to a high dimensional area to optimally separate the given data into their various attack categories. Therefore, kernel RBF is especially effective in separating sets of information that share complicated boundaries. In our study, all the simulations are conducted victimization the freely accessible LibSVM package.

Given that the chosen drawback may be a multiclass classification drawback, it uses the notion of 1 vs all for attack classification. during this notion, the multiclass drawback is split into a two-class drawback. The radial basis operate (RBF) kernel is employed during this study, that is diagrammatical as follows:

$K(x,y)=e^{-y\|x-y\|2}$, $\gamma>0$

For given coaching samples (**xi** , y i), i = 1, 2, . . . n, where i is the maximum range of samples within the coaching knowledge, x i ∈ R^n and y i ∈ , wherever one shows samples from a positive class and −1 represents sequences from the negative category. When exploitation SVM, the answer of the subsequent downside is provided.

$$\underset{w,b,\xi}{\text{Min}} 1/2w^Tw+C\sum^{n}_{i=1}\xi i$$

$$\text{subject to } yi(w^T W\varphi(xi)+b)\geq 1-\xi i$$

Here, φ transforms the coaching vector x i to the upper dimensional area. Following this, the SVM shows a hyper-plane having most margin to separate totally different categories of knowledge.

The determined results via the SVM model aren't considerably convincing compared with those from the opposite classifiers. The advantage of SVM is that stripped-down parameter adjustment is needed. The disadvantages of it embody the necessities of a mathematician perform for every instance of the coaching set, thereby increasing coaching time and performance degradation on terribly giant datasets with thousands

of instances, as within the case classification. Just in case most margin classifier fails to search out any separating hyperplane, soft margin is employed to beat this downside. Soft margin uses positive slack variables ξ i , i = 1, 2, . . . , N within the constraints as follows:

$(w.x_i-b)\geq +1-\xi_i$ for $y_i=+1$

$(w.x_i-b)\geq -1+\xi_i$ for $y_i=-1$

$\xi>0$

When a slip happens, ξ i need to exceed unity. Then, i ξ i is associate edge on the coaching error. The Lagrange during this situation is as follows

$LP=1/2\|W^2\| + C\sum^n_{i=1}\xi i$

$-\sum_i\alpha i \{yi(xi.w-b)-1+\xi i\}-\sum_i\mu i\xi i$

where, μ i represents Lagrange multipliers wont to acquire the positive worth of ξ i .

2) Random Forest

RFs are ensemble classifiers, that are used for classification and regression analysis on the intrusion detection knowledge. RF works by making numerous call trees within the coaching section and output category labels those have the majority vote. RF attains high classification accuracy and might handle outliers and noise within the knowledge. RF is employed during this work as a result of it's less prone to over-fitting and it's antecedently shown smart classification results.

Figure 3 shows the implementation of the random forest classification model within the information classification within the projected system. A preprocessed sample of n samples is fed to the random forest classifier. RF creates n totally different trees by employing a range of feature subsets. Every tree produces a classification result, and also the results of the classification model depends on the bulk ballot. The sample is appointed to the category that obtains highest ballot scores. The antecedently earned classification results indicate that RF is fairly suitable within the classification of such information as a result of in some cases, it's obtained higher results than produce other classifiers. Alternative advantages of the RF embody its higher accuracy than Adaboost and fewer probabilities of overfitting. The architecture of the random forest for intrusion detection is given in Figure 3.

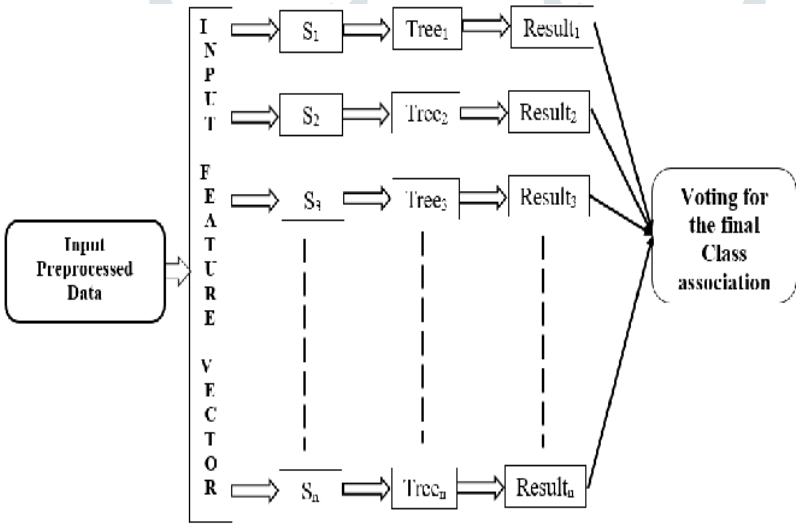

Figure 3. Architecture of RandomForest for intrusion detection

3)Extreme Learning Machine

ELM is sometimes referred as single or multiple hidden layer feedforward neural networks. ELM will be wont to solve numerous classification, clustering, regression, and have engineering issues. This learning rule involves input layer, one or multiple hidden layers and therefore the output layer. Within the ancient neural networks, the tasks of adjustment of the input and hidden layer weights square measure terribly computationally high-ticket and long as a result of it needs multiple rounds to converge.

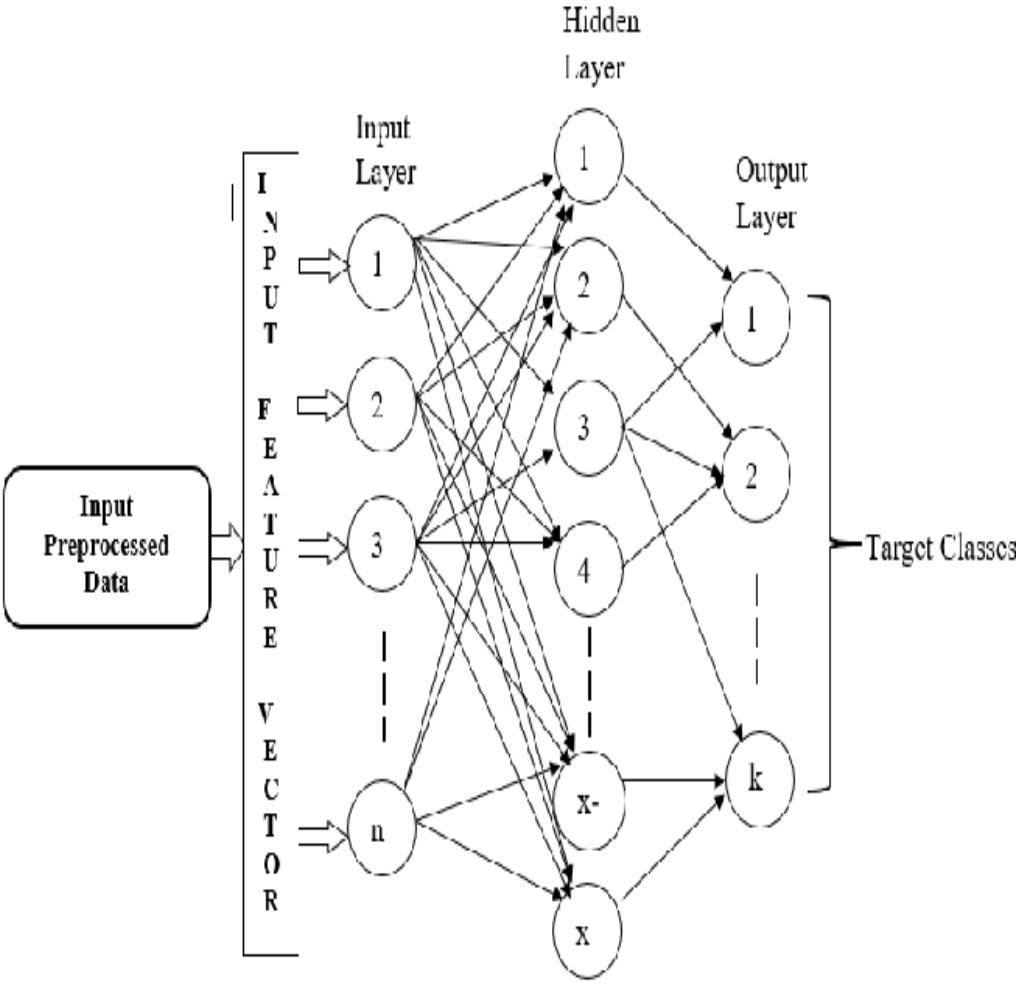

Figure 4. Architecture of Extreme learning machine for intrusion detection

To overcome this drawback, Huang et al.planned an SLFN by indiscriminately choosing input weights and hidden layer biases to attenuate the coaching time. The excellent detail of ELM is accessible in Huang et al. and Qayyum et al. The authors claim that these models learn quicker and attain higher generalization capability as compared with different feedforward network models. ELM performance is comparable SVM or different progressive machine learning classifiers. ELM has the best ability to perform higher in extremely complicated datasets. The design of the planned system is shown in Figure 4.

N input samples (z i , y i) are gift, wherever z i = [x i1 , x i2 , ..., x in] T is that the ith sample with n completely different options and y i = [y i1 , y i2 , ..., y im] T describes the particular labels of x i with ancient SLFN with K hidden neurons that is outlined as follows:

$$\sum^{K}_{n=1} \beta_j h(w_n.a_j + c_n)= \alpha_j \qquad j=1,2,.....,N$$

Where $w = [w_{n1},w_{n2},.....,w_{nx}]^T$is the chosen weight vector associate degree indicates an jth hidden somatic cell reference to the input nodes. $\beta_j=[\ \beta_{j1},\beta_{j2},.....\ ,\beta_{jn}]^T$shows the burden vector with affiliation of jth hidden neuron and alsothe output nodes and cm is that the threshold of the jth hidden neuron $\alpha_k=[\ \alpha_{k1},\ \alpha_{k2},....., \alpha_{kn}]^T$ is the kth output neuron. h(.) represents the activation operate and SLFN used for Mhidden neurons and activation operate will approach these N coaching samples with zero error. Numerous alternative techniques are applied to find and classify intrusion of wiredand wireless atmosphere.

D. Evaluation

The designed system is evaluated supported the quality dataset NSL–KDD, that is irregular and divided into 3 elements, namely, the total dataset, and therefore the 1/4 dataset. the total dataset consists of 65,535 samples, the includes 32,767 samples, and therefore the 1/4 th dataset consists of 18,383 samples. Accuracy, precision, and recall are used as analysis metrics.

Accuracy: Accuracy is computed as ‘‘the total variety of correct prediction, True Positive (TP) + True Negative (TN) divided by the whole variety of a dataset Positive (P) + Negative (N)’’.

Accuracy =(TP + TN)/(P + N)

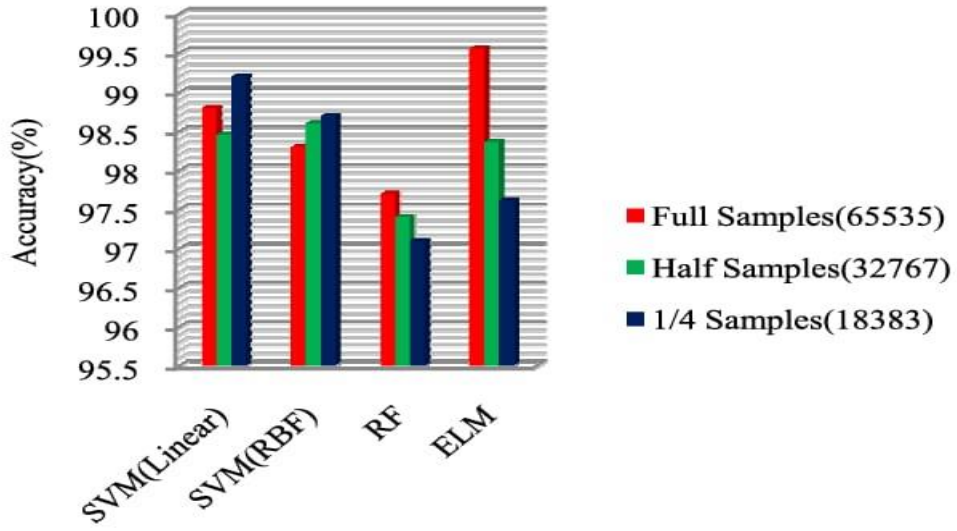

Figure 5. Accuracy of the SVM, RF and ELM(80% training and 20% testing)

Precision: preciseness is computed as ‘‘the variety of correct positive predictions (TP) divided by the whole variety of positive predictions (TP + FP)’’.Preciseness is additionally called a positive prognostic worth.

Precision =TP/(TP + FP)

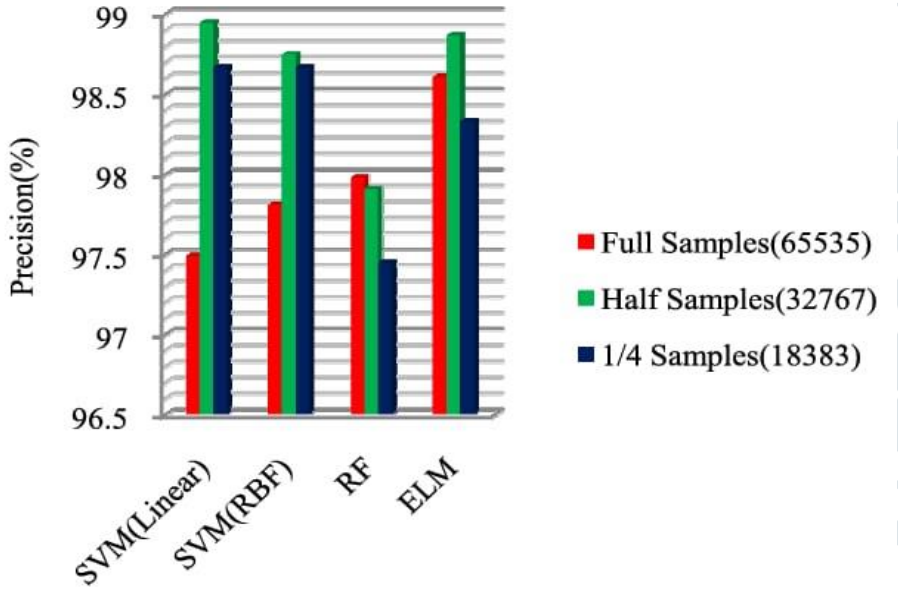

Figure 6. Precision of the SVM, RF and ELM(80% training and 20% testing)

Recall: Recall is computed as ‘‘the variety of correct positive predictions (TP) divided by the whole variety of positives (P)’’. Recall is additionally called verity positive rate or sensitivity.

Recall =TP/P

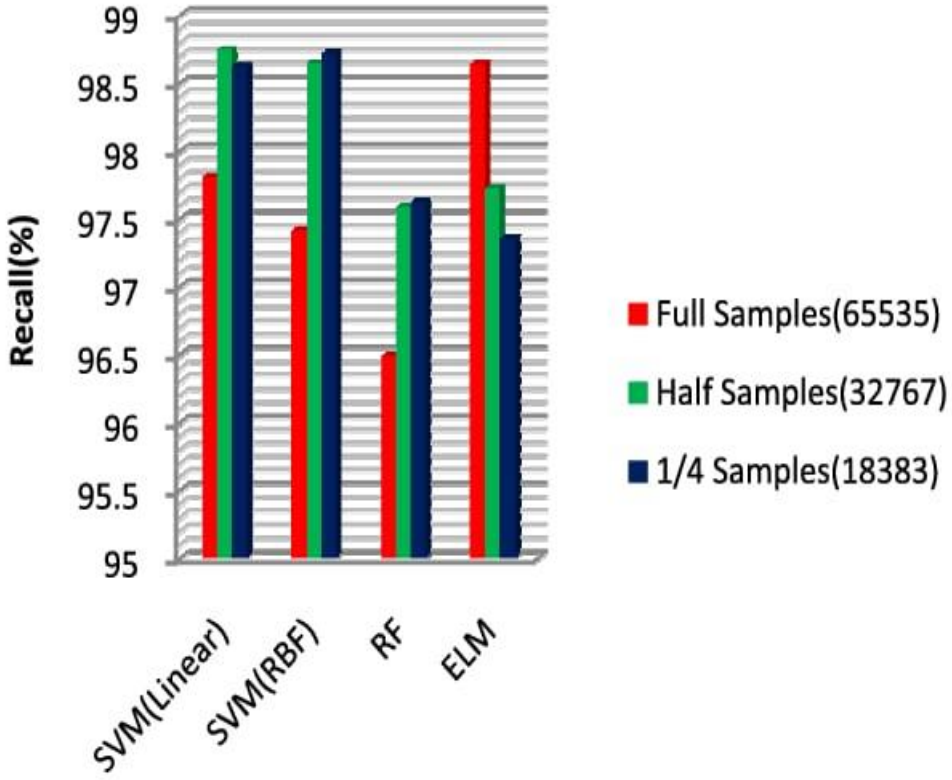

Figure 7. Recall of the SVM, RF and ELM(80% training and 20% testing)

IV. RESULTS

The exactness/accuracy of SVM (Linear), SVM (RBF), RF, and ELM on 20% testing and 80% training information tests is appeared in Figure 5. ELM performs better than SVM (Linear), SVM (RBF) and RF on full information tests, while SVM (RBF) shows improved exactness over RF and ELM on half information tests. SVM (Linear) beats different procedures on 1/4 information tests, as delineated in Figure 5.

The precision of SVM (Linear), SVM (RBF), RF, and ELM on 20% testing and 80% preparing information tests is appeared in Figure 6. The precision of ELM is superior to that of SVM Linear and RBF on the full information tests, and it moreover outflanks that of RF. On half information tests, the precision of SVM (Linear) is higher than that of SVM (RBF), ELM, and RF. On 1/4 information tests, the precision of SVM (Linear) is equivalent to that of SVM (RBF). Besides, the SVM performs superior to ELM and RF in the 1/4 dataset.

The recall of SVM (Linear), SVM (RBF), RF, and ELM on 20% testing and 80% preparing information tests is appeared in Figure 7. On full information tests, the recall of ELM performs superior to those of SVM (Linear), SVM (RBF), and RF. The recall of SVM (Linear) is more prominent than those of SVM (RBF), ELM, and RF. The positioning of review on 1/4 of information tests is as per the following: first for SVM (RBF), second for SVM (Straight), third for RF, and fourth for ELM. The above mentioned dialog demonstrates that SVM performs better on a little dataset, though EML beats others approaches on huge datasets.

The exactness/accuracy of SVM (Linear), SVM (RBF), RF, and ELM on 10% testing and 90% preparing information tests is appeared in Figure 8. On the full information tests, the exactness of ELM is superior to that of SVM (direct), SVM (RBF), and RF. The SVM (RBF) beats SVM (Linear), ELM, and RF on the half information tests. The SVM (straight) demonstrates better execution on 1/fourth information tests as contrasted and SVM (RBF), RF, and ELM.

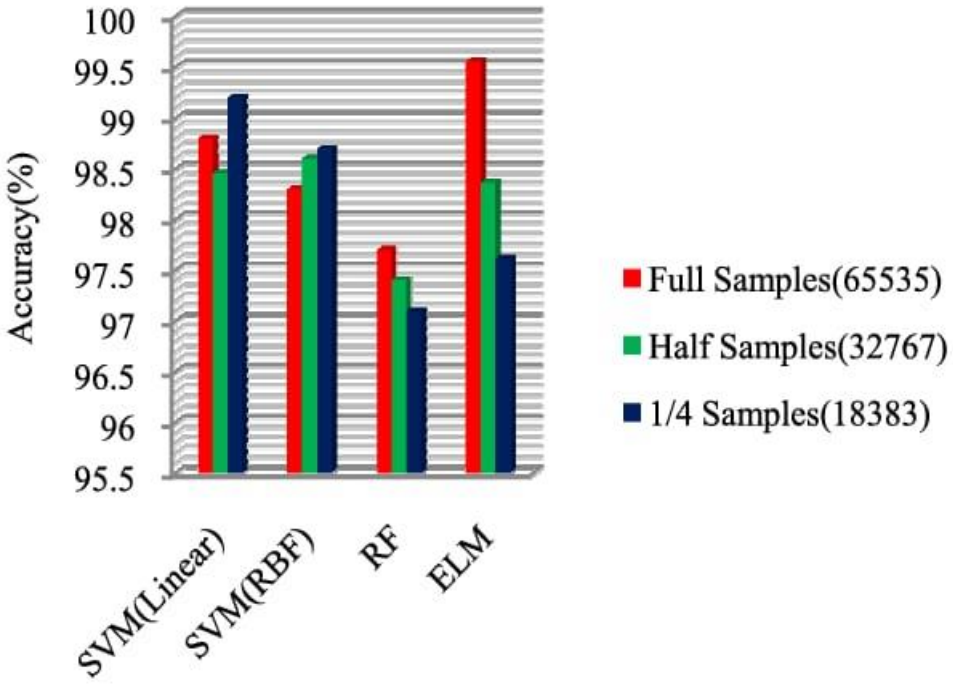

Figure 8. Accuracy of the SVM, RF and ELM(90% training and 10% testing)

The precision of SVM (Linear), SVM (RBF), RF, and ELM on 10 % testing and 90% preparing information tests is appeared in Figure 9. The outcomes demonstrate that the ELM shows better precision than RF, SVM (RBF), and SVM (Linear) on full information tests, while SVM (Linear) demonstrates better precision on the half information tests. Besides, SVM (Linear) performs superior to ELM and RF on 1/4 dataset.

The recall of SVM (Linear), SVM (RBF), RF, and RLM on 10% testing and 90% preparing information tests is appeared in Figure 10. On full information tests, the recall of ELM out per frames those of SVM (direct), SVM (RBF), and RF, while the recall of SVM (straight) is superior to those of SVM (RBF), ELM, and RF on half information tests. On the 1/fourth information tests, SVM (RBF) is practically equivalent to SVM (Linear), while it demonstrates better outcomes over RF and ELM, as appeared in Figure 10.

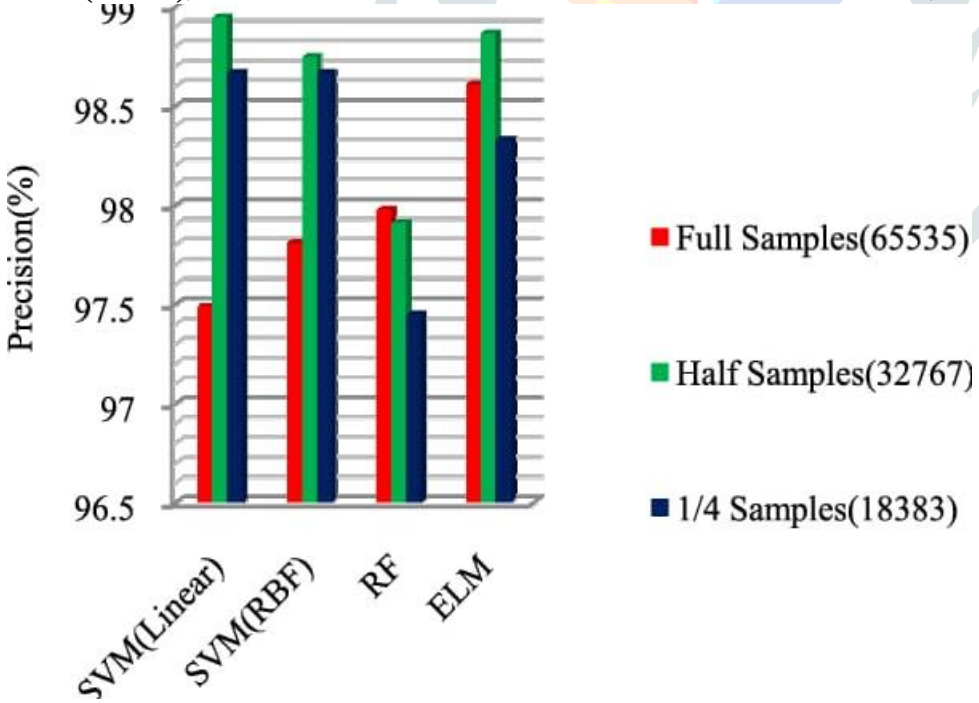

Figure 9. Precision of the SVM, RF and ELM(90% training and 10% testing)

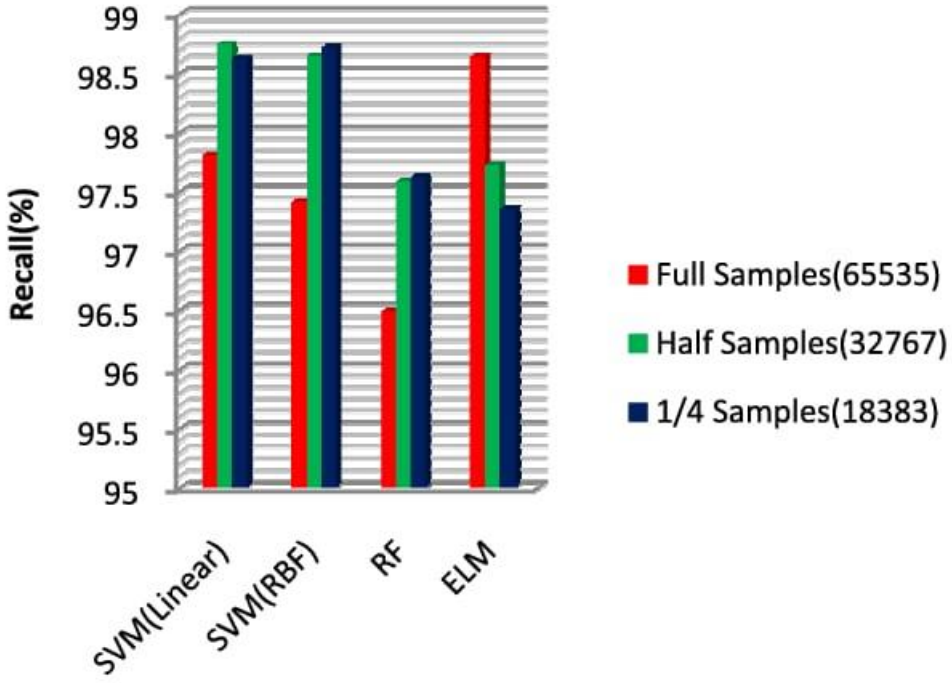

Figure 10. Recall of the SVM, RF and ELM(90% training and 10% testing)

V. CONCLUSION

Intrusion detection and bar area unit essential to current and future networks and data systems, as a result of our daily activities area unit heavily addicted to them. what is more, future challenges can become a lot of intimidating thanks to the net of Things. Dduring this respect, intrusion detection systems are vital within the previous few decades. many techniques are utilized in intrusion detection systems, however machine learning techniques area unit common in recent literature. in addition, totally different machine learning techniques are used, however some techniques area unit a lot of appropriate for analyzing vast information for intrusion detection of network and data systems. to handle this drawback, totally different machine learning techniques, namely, SVM, RF, and ELM area unit investigated and compared during this work. ELM outperforms alternative approaches in accuracy, precision, and recall on the complete information samples that comprise sixty five,535 records of activities containing traditional and intrusive activities. what is more, the SVM indicated higher results than alternative datasets in half the info samples and in 1/4 of the info samples. Therefore, ELM could be a appropriate technique for intrusion detection systems that area unit designed to investigate a large quantity of information. In future, ELM are going to be explored more to research its performance in feature choice and have transformation techniques.

REFERENCES

[1] Cortes C, Vapnik VN. Support vector networks. *Machine Learning* 1995; **20**:273C297.

[2] J.H. Lee, J.H. Lee, S.G. Sohn, et al., Effective value of decision tree with KDD 99 intrusion detection datasets for intrusion detection system, in: 10th International Conference on Advanced Communication Technology (ICACT'08), 2008, pp. 1170–1175

[3] Nelcileno Virgílio de Souza Araújo"identifying important characteristics in the KDD99 intrusion detection dataset by feature selection using a hybrid approach" , 2010 IEEE 17th International ConferenceDOI: 10.1109/ICTEL.2010.5478852,

[4] Ujwala Ravale, Nilesh Marathe, Puja Padiya "Feature Selection Based Hybrid Anomaly Intrusion Detection System Using K Means and RBF Kernel Function" ICACTA (2015), pp. 428-435

[5] A. A. Aburomman and M. B. I. Reaz, ''A novel SVM-kNN-PSO ensemble method for intrusion detection system,'' Appl. Soft Comput., vol. 38, pp. 360–372, Jan. 2016, doi: 10.1016/j.asoc.2015.10.011.

[6] chi cheng; ELM for intrusion detection 30 july 2012,10.1109/IJCNN.2012.6252449

[7] N. Farnaaz and M. A. Jabbar, ''Random forest modeling for network intrusion detection system,'' Proc. Comput. Sci., vol. 89, pp. 213–217, Jan. 2016, doi: 10.1016/j.procs.2016.06.047

[8] G.-B. Huang, Y.-Q. Chen, and H. A. Babri, "Classification ability of single hidden layer feedforward neural networks," IEEE Transactions on Neural Networks, vol. 11, no. 3, pp. 799— 801, 2000.

[9] Al-Sultan, S., Al-Doori, M. M., Al-Bayatti, A. H., Zedan, H.A comprehensive survey on vehicular Ad Hoc networkJournal of Network and Computer Applications201437138039210.1016/j.jnca.2013.02.0362-s2.0-8489043016

[10] Jegadeesan,R.,Sankar Ram M.Naveen Kumar JAN 2013 "Less Cost Any Routing With Energy Cost Optimization" International Journal of Advanced Research in Computer Networking,Wireless and Mobile Communications.Volume-No.1: Page no: Issue-No.1 Impact Factor = 1.5

[11]. Jegadeesan,R.,Sankar Ram, R.Janakiraman September-October 2013
"A Recent Approach to Organise Structured Data in Mobile Environment" R.Jegadeesan et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (6) ,Page No. 848-852 ISSN: 0975-9646 Impact Factor:2.93

[12]. Jegadeesan,R., Sankar Ram October -2013 "ENROUTING TECHNICS USING DYNAMIC WIRELESS NETWORKS" International Journal of Asia Pacific Journal of Research Ph.D Research Scholar 1, Supervisor2, VOL -3 Page No: Print-ISSN-2320-5504 impact factor 0.433

[13]. Jegadeesan,R., Sankar Ram, M.S.Tharani (September-October, 2013)
"Enhancing File Security by Integrating Steganography Technique in Linux Kernel" Global journal of Engineering,Design & Technology G.J. E.D.T., Vol. 2(5): Page No:9-14 ISSN: 2319 – 7293

[14]. Ramesh,R., Vinoth Kumar,R., and Jegadeesan,R., January 2014
"NTH THIRD PARTY AUDITING FOR DATA INTEGRITY IN CLOUD" Asia Pacific Journal of Research Vol: I Issue XIII, ISSN: 2320-5504, E-ISSN-2347-4793 Vol: I Issue XIII, Page No: Impact Factor:0.433

[15]. Vijayalakshmi, Balika J Chelliah and Jegadeesan,R., February-2014 "SUODY-Preserving Privacy in Sharing Data with Multi-Vendor for Dynamic Groups" Global journal of Engineering,Design & Technology. G.J. E.D.T.,Vol.3(1):43-47 (January-February, 2014) ISSN: 2319 –7293

[16]. Jegadeesan,R.,SankarRam,T.Karpagam March-2014 "Defending wireless network using Randomized Routing process" International Journal of Emerging Research in management and Technology

[17].Jegadeesan,R.,T.Karpagam, Dr.N.Sankar Ram , "Defending Wireless Network using Randomized Routing Process" International journal of Emerging Research in management and Technology ISSN: 2278-9359 (Volume-3, Issue-3) . March 2014

[18]. Jegadeesan,R., Sankar Ram "Defending Wireless Sensor Network using Randomized Routing "International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 9, September 2015 ISSN: 2277 128X Page | 934-938

[19]. Jegadeesan,R., Sankar Ram,N. "Energy-Efficient Wireless Network Communication with Priority Packet Based QoS Scheduling", Asian Journal of Information Technology(AJIT) 15(8): 1396-1404,2016 ISSN: 1682-3915,Medwell Journal,2016 (Annexure-I updated Journal 2016)

[20]. Jegadeesan,R.,Sankar Ram,N. "Energy Consumption Power Aware Data Delivery in Wireless Network", Circuits and Systems, Scientific Research Publisher,2016 (Annexure-I updated Journal 2016)

[21]. Jegadeesan,R., Sankar Ram , and J.Abirmi "Implementing Online Driving License Renewal by Integration of Web Orchestration and Web Choreogrphy" International journal of Advanced Research trends in Engineering and Technology (IJARTET) ISSN:2394-3785 (Volume-5, Issue-1, January 2018

[22]. Pooja,S., Jegadeesan,R., Pavithra,S., and Mounikasri,A., "Identification of Fake Channel Characteristics using Auxiliary Receiver in Wireless Trnsmission" International journal for Scientific Research and Development (IJSRD) ISSN (Online):2321-0613 (Volume-6, Issue-1, Page No. 607-613, April 2018

[23]. Sangeetha,R., Jegadeesan,R., Ramya,P., and Vennila.,G "Health Monitoring System Using Internet of Things" International journal of Engineering Research and Advanced Technology (IJERAT) ISSN :2454-6135 (Volume-4, Issue-3, Page No. 607-613, March 2018.