An Improved HNIDS in Cloud Real Time Prediction Using Fuzzy Decision Making Combination Rule

T. Nathiya and G. Suseendran

Abstract--- Fuzzy Decision Making (FDM) combination rule can be used to improve the real time prediction in cloud. Needs the dynamic approach in day to day to monitor the traffic and notify the illegal problems into system administrator. This type of approach is known as HNIDS (Hybrid Network Intrusion Detection System). So our model HNIDS is introduce the FDM rule in this paper. Not only FDM we are using new upcoming classification learner XGBoost and SVM. SVM is functional dependent and XGBoost is decision tree type of classification. So that the two different type of classification model to predict the cloud network packets whether the packets are normal or abnormal. Finally FDM combination rule to take the decision using belief probability evidences. This is new type of prediction method. Result and Discussion have shown that Our HNIDS using the method to predict the network packets with high accuracy value and minimum computation cost efficiency.

Keywords--- HNIDS, SVM, XGBoost, Fuzzy Decision Making Rule, NSL- KDD Datasets, Python, Azure Cloud.

I. INTRODUCTION

Network security is most important needs in cloud because so many network issues created in day-to-day life. In 2017th year the malware that locks down computer files using encryption that the attack is known as ransomware attacks. And then hackers ask for money is exchanged then release the files. This technique is called WannaCry ransomware attack which is attack thousands of computers and the companies such as Amazon, IBM, and Google. The Twitter, Netflix and other about the DoS attack in 2016, which is the attackers to send flooded useless packet for making unavailable of the system. The virtual machine to notify the escape the attacks reported in 2008 by core security technologies, which is vulnerability found in VMware's operating system. So, we need to lot of security. The attacker find new way to exploit the network, that why many organization dedicated to come up with security concern that is strong sufficient to be employed in a cloud environment[1].

Cipher cloud, cisco security and dell security are some organization that build with making the cloud environment for a safe place. Many researchers have a lot of work regarding the field of security. But entire the cloud not secure completely. So need the dynamic approach in day to day to monitor the traffic and notify the illegal problems into system administrator. This type of approach is known as HNIDS (Hybrid Network Intrusion Detection System) which is activated into two ways, signature based method and another ways are anomaly based method. The signature based method is only to identify the already find the known attacks but anomaly based method is to identify the new type of attacks[2]. The anomalies to using the machine learning algorithms to detect the unknown packets. Looking into cloud network (figure 1), the HNIDS is to secure the cloud network, firewall, secure web gateways, network access control, network access security broker and intrusion detection system these are traditional network securities. But due to new challenges are facing. In cloud lot of virtual machines had produce heavy network traffic. It is difficult to detect the during the network attacks. IDS have to improve the scale up processes[3].

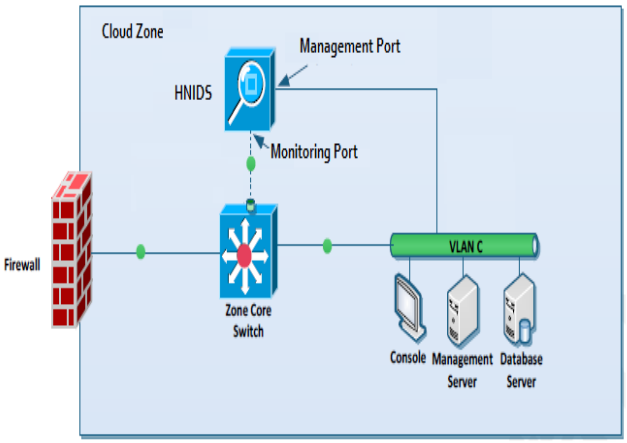

Figure 1: HNIDS Monitor the Cloud Network Packets Framework

In our proposed security framework Hybrid Network Intrusion Detection System (HNIDS) for assembled in cloud. HNIDS monitor to build in network virtual switch and this HNIDS is monitor the network traffic and notify the illegal activities into Restriction Zone[4]. The functioning of HNIDS is described one by one. The first signature based model that is already discussed and next process is feature selection that is the signature not identify the packet goes to anomaly section and before the process is feature selection[5]. In this process first collect the all dataset attributes with class and then using feature selection algorithm to filter the best subset attributes[6]. And then take only the best subset attributes values to get into the anomaly based model. The third HNIDS process of the anomaly based model using machine learning.

Manuscript received February 01, 2019

T. Nathiya, Ph.D. Research Scholar, Department of Computer Science, School of Computing Science, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamil Nadu, India. (e-mail: tnathiya17@gmail.com)

G. Suseendran, Department of Information Technology, School of Computing Science, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamil Nadu, India. (e-mail: suseendar_1234@yahoo.co.in)

Machine learning have performing variety of ways but having the two classification algorithm, one is functionally based SVM and another one is taking the decision tree model of new XGBoost model. After that new fuzzy DST rule assign to take the final decision whether the network packets are normal or attack[7].

The aim of this paper is as follows. Section 2 survey the related works, how many researcher doing this area, what are the problems still continued. In section 3 explain the methodology. The proposed prediction algorithm is discussed. Result and discussion of the proposed work analysis in section 4 and section 5 concludes this research work at the end.

II. RELATED WORKS

Mainly intrusion detection system software technique concept is used for detecting the malicious actions.in earlier stage that is big challenging threats and enhance the network security. In the other hand, cryptography are more confused to ensuring integrity.

Wenying Feng et al[8] researchers had applied a new algorithm for IDS. But these are only taken advantages dataset while to avoid the weak dataset. IDS had applied the traditional networks. So they are applying the minimum dataset to classification of training data.

Mehrnaz Mazini et al[9] has considered as the important component of a safe network. The author introduced anomaly network based IDS which is using an artificial bee colony and its algorithm. And they are using two different dataset for classification. The experimental results show the ABC algorithm and efficiency compared with the existing algorithm and shows the accuracy.

Kamran Siddirue et al[10] has proposed an approach to provide the solution with customization. The researcher using ABB feature selection technique to select the optimal subset feature for improving the classification work. But three classification algorithm using this training data. It's improving network intrusion detection. They are using only existing algorithm to prove his work.

Manthira Moorthy et al[11] in this article fully explained the host IDS in cloud. How to build the host based IDS and working on virtual host system. Where increasing the outside traffic is enter the host system to injecting the attacks by malware. At that time the effective cloud is generated the IDS for stopped the error. They are determined the interval between 1.5 to 2 Mbps.

Mohammad Almseidin et al[12] has discussed the evaluation of machine learning concepts about IDS.

It's analyzing for traditional network because not built in cloud. In this article discussed only comparative of machine learning algorithm. The compared to other existing algorithms the random forest algorithm is produced better accuracy rate and low false alarm rate.

III. METHODOLOGY

Enter the machine learning methods before first discussed about machine learning concept. Its subset of artificial intelligence[13]. Where in the system to train to do the programming without any explicit program. The traditional program, give the input and write the program finally get the output. But machine learning program, to give both input and output and system try to write the program on its own. If take this article supervised classification algorithm it is categories of machine learning algorithm. They are basically two stages of learning. One is training stage and another one is testing stage. In the training stage, If take from known categories of IDS dataset it tried to build the model. In the testing stage, depending on the model to builds when to give the new HNIDS data and its try to predict the data. In this article discussed in SVM, XGBoost classification algorithm is to classify the network packet feature and try to predict the attack packets[14].

3.1 Support Vector Machine (SVM)

The most popular machine learning algorithm SVM. It is try to classify the two classes of IDS (normal, anomaly). It is highly predicted the any type of dataset. We present the mathematical calculation of SVM. We will follow step by step function[11][15][16].

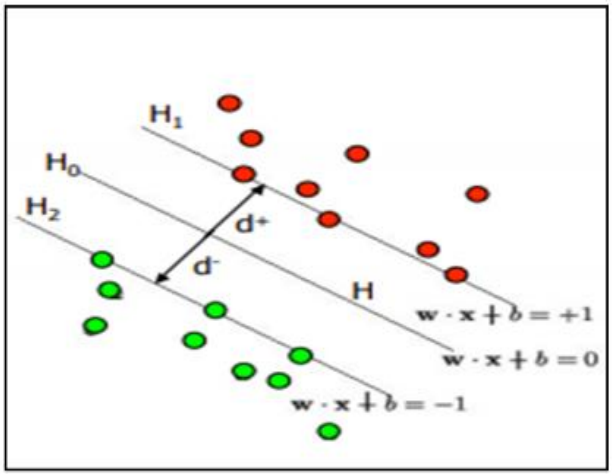

Figure 2: Identify the right hyperplane

Step 1: Dataset D and classify the vector.

Training entire dataset D is as $(x1, y1), \ldots \ldots \ldots, (xn, yn)$

The i[th] data $x_i = (x_i(1), \ldots\ldots, x_i(d))\ \ j = 1, \ldots d$

$x_i(j)$ is a real value. $y_i \boldsymbol{\varepsilon} \{-1, +1\}$

The initial dataset theory:

$$D = \left\{ (x_i, y_i) \mid x_i \varepsilon \mathrm{T}^{\mathrm{p}}, \mathrm{y_i} \varepsilon \{-1,1\} \right\}_{i\_1}^{N} \qquad (1)$$

x_i have a lot of dimensions, so x_i is P dimension vector.

Step 2: Equation of hyperplane

$$W^H.\mathrm{X} = 0 \qquad (2)$$

The vector W is always normal. The hyperplane can write the set of points x satisfying

$W.\mathrm{x} + \mathrm{b} = 0$ $W.\mathrm{x}$ is $W^H.\mathrm{X}$

i.e $W.x_i + b \geq 1 \qquad (3)$

When $x_i = A$, the points on the hyperplane.

$$W.x_i + b = 1$$

When $x_i = C$, the points over the hyperplane. $W.x_i + b > 1$

So that $y1(W.x_i + b) \geq 1$ for x_i having the class -1.

In figure 2, X and Y plot differentiate between two classes. The hyperplane H0, H1and H2 in between the two classes.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The edge of the hyperplane H1 and H2 interact with two points one is green dot point and another one is red dot points. That is the predict value of data.H0 is in between determine the hyperplane[17].

3.2 XGBoost Classification

XGBoost algorithm mainly comes from three most gradient boosting techniques such as gradient boosting, stochastic and regularized boosting. XGBoost was mainly designed for increasing the speed of performance using gradient boosted decision tree. That is called extreme Boosting supervised classification algorithm. Using this algorithm, to reduce the computation time and provides the optimal value to predict in minimum memory usage[18].

3.2.1 XGBoost Mathematical Function

The main motivation of XGBoost decision tree is to learn about the tree with simple way to do optimize the objective function.

$$EXG_{obj(\theta)} = EXG_{tl(\theta)} + EXG_R(\theta) \quad (4)$$

θ represents the parameter of objective function. $EXG_{tl(\theta)}$represents the training loss value and its used to predict the model. $EXG_R(\theta)$ is denoted by regularization. The XGBoost is to train the tree and adding the each step because used to optimize the tree. So adding the XGBoost some parameter to fulfill the objective function.

$$EXG_{obj}(t) = \sum_{i=1}^{n}\left[m_i f_t(p_i) + \frac{1}{2}c_i f_t 2(p_i)\right] + EXG_R(f_t) \quad (5)$$

Where p_i denoted as total no of training data, m_i and c_i input values. The reflect results to desired the new optimization tree $f_t(p)$.

$$f_t(p_i) = w_g(p), w\epsilon^L, g: R^d \rightarrow \{1,2,3 \ldots., L\} \quad (6)$$

In the above the mathematical equation mention the symbol w represents a vector leaf score and g represents the corresponding data points. L is the number of leaves. The regularization of XGBoost of complexity is $EXG_R(f_t)$.

$$EXG_R(f) = \alpha L + \frac{1}{2}\beta\sum_{j=1}^{L} w_j 2 \quad (7)$$

Therefore the according to the XGBoost theorem to get the tree structure is calculated by leaf score and objective function level.

The XGBoost run the tree and classification of the data and get the accuracy and other parameters are calculated. Using XGBoost algorithm to improving our HINDS dataset analysis to get the predict value whether the network packet normal or abnormal. And also we get the predict probability value of testing data for improving our accuracy value. In figure 3, no of training data is build the XGBoost classification model using parameter of max_ depth, learning rate, silent, n_estimators.

After trained the model we had to put the new real time data for testing and to get predict, predict probability value and accuracy scores[19][20].

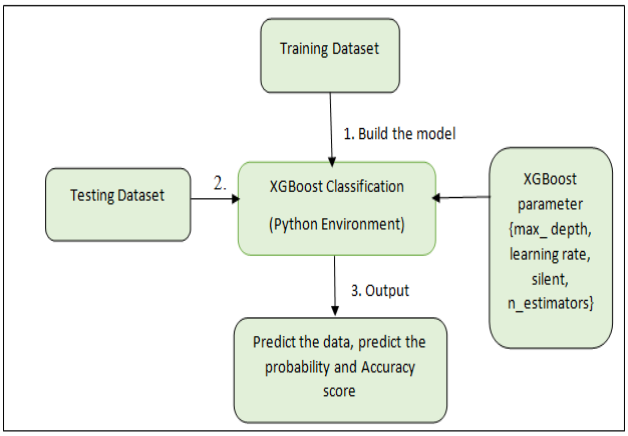

Figure 3: XGBoost Data Flow Diagram

3.3 Fuzzy Dempster Shafer Theory (FDST)

In order to the FDST problem, the belief function denotes the different verity pieces of evidence need to be combined. Each pieces of evidence is called separate belief function. A frame of discernment θ is a finite set of elements in a domain. For example, A is a hypothesis is a subset $A \subseteq \theta$ of frame discernment. $p(\theta)$ is an element of power set. $A = \{a, b\}$ this hypothesis belief elements and complement of belief element can be less than 1[21].

$$belief(A) + belief(\bar{A}) \leq 1, \quad \forall A \subseteq \theta \quad (8)$$

3.3.1 Mass function

A mass function is called basic probability assignment function. The mass function denoted the symbol m and m is mapping the $p(\theta) \rightarrow [0,1]$ the value assign to each hypothesis $A \subseteq \theta$ of the frame of discernment θ so that

$$\sum_{A\subseteq\theta} m(A) = 1 \quad (9)$$

The value $m(A)$ is belief strictly committed to hypothesis. Where a mass value does not assign the positive value in the empty set.

$$m(\emptyset) = 0 \quad (10)$$

3.3.2 FDST Combination Rule

In order to the function (1), (2) & (3) FDST combination rule $\oplus$ is defined as, the mass function $m1 \oplus 2 = m1 \oplus m2$

$$m_{1\oplus_2}(A) = \eta \sum_{B\cap C=A} m_1(B)m_2(c), \quad \forall A \subseteq \theta, A \neq \emptyset$$

$$m1 \oplus 2(\emptyset) = 0.$$

IV. PROPOSED WORK

The proposed method used to the fuzzy dempster shafer theory and its enabling two evidence. We are proposed FDM (Fuzzy Decision Making) combination algorithm that is related with FDST method. Evidence 1 and Evidence 1 are implementing our proposed method. It is calculated the predict probability value and weighted average value. The proposed method (see figure 3) comprises the following steps:

Evidence 1: After preprocessing the training and testing dataset into the feature selection using filter method. After filter, only selected feature we are implementing the SVM_IDS classification algorithm. In this method using training dataset into build the model. After the building model, we are predict the real time dataset. In this section testing stage. Finally we got predict data with probability value (see the Algorithm 1)

Algorithm 1: SVM_IDS (Evidence 1)

Input: $D = \left\{(x_i, y_i) \mid x_i \varepsilon T^p, y_i \varepsilon \{-1,1\}\right\}^{N}_{i=1}$ training set, N – No of feature, C is label

Output: SVM_model, SVM_prob_resultset

Algorithm:

In eq.(2) & (3) for all points to check the conditions

If point (x_train) yi_train * (w. x_train + b) = 1

Point = display the correct classified parameter

Else if point (x_train) yi_train * (w. x_train + b) >1

Point = display the misclassified parameter

Else

Retrain **End**

Evidence 2: This is same process of evidence 1. But evidence 2 we are using XGB_IDS classification algorithm (see the Algorithm 2).

Algorithm 2: XGB_IDS (Evidence 2)

Input: $\{(x_i, y_i)\}^{N}_{i=1}$, differentiated loss function $L(y, F(x))$, M is no of iteration

Output: XGB_model, XGB_prob_resultset

Algorithm:

Initialize model $f_t(p_i) = w_g(p), w\epsilon^L, g: R^d \rightarrow \{1,2,3 \ldots., L)$

For M = 1 to m

Compute the model

$$EXG_{obj}(t) = \sum_{i=1}^{n} \left[m_i f_t(p_i) + \frac{1}{2} c_i f_t 2(p_i) \right] + EXG_R(f_t)$$

Fit the XGB = XGB_train i.e. train it using training set

XGB_model = $EXG_{obj}(t)$

Update the model XGB_model

XGB_prob_resultset = XGB_model (y_test)

Repeat

Decision Making: As rule of FDST theory took no of evidence and taking the decision. So in our proposed work FDM algorithm got the evidence 1& 2 and taking the decision whether the cloud network packet normal or attack packets (see the algorithm 3).

Algorithm 3: FDM combination Algorithm

Input: F= F {f1, f2……., fn, c} //n – no of feature, C is label

Output: Prediction Dataset

Algorithm:

TS{F1, F2… Fp} //p- no of training packets, TS is training set.

XS{F1, F2… Fq} //q – no of testing packets, XS is testing set.

//Evidence 1

SVM_model = get. SVM_model(TS)

SVM_prob_resultset = SVM_model. Get probset(XS)

//Evidence 2

XGB_model = get. XGB_model (TS)

XGB_prob_resultset = XGB_model. Get probset (XS)

For i=1 to q

$$pre(f_i) = \max\left(\sum_{0 \le j \le n}^{i} \left(p_{svm}(f_j) * p_{XGB}(f_j)\right)\right)$$

Loop

Return $pre(f_i)$

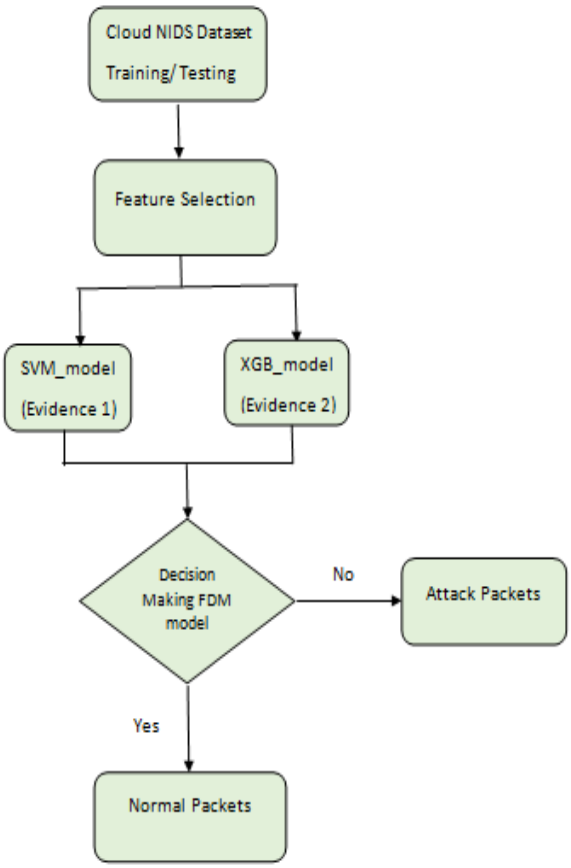

Figure 3: Executes of the Proposed (HNIDS) Model

V. IMPLEMENTATION

Our VM is created by Azure and installed python programming in windows 10 operating system, 7.00GB RAM, 64- bit operating system. Spyder IDE 3.3.2 is an open source python framework for building a network intrusion detecting applications. Wireshark tool to be installed when we getting real time network tcp packet details. The exploited data sets are demonstrated in section 5.1.

5.1 Datasets

In this paper, a proposed FDM combination model is applied on high dimensional datasets that are derived from GitHub Repository. The descriptions of these datasets given in table 1.

Table 1: Characteristics of Data sets

S. No	NSL_KDD Data Set	# Feature	# Instance	# Class
1	Training Data from GitHub	13	44,300	22
2	Testing Data from our system	13	25,000	22

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

After collecting the datasets, preprocessing work such as incomplete data's to be removal and also removed the relevant data. And then selecting feature using feature selection algorithm (discussed detail wok in previous paper) and using classification algorithm for build the model. In Table 2 represents the explanation of feature used in NSL_KDD data sets.

Table 2: Meaning of features in datasets

S.NO	Name of Feature	Meaning of Feature
1	protocol	It represents the type of protocol used in connection
2	flag	It represents the connection status
3	src_bytes	The no of data bytes transferred from source to destination in a single connection
4	dst_bytes	The no of data bytes transferred from destination to source in a single connection
5	wrong_fragment	It represents the wrong fragments in a single connection.
6	num_file_creations	It represents the no of times the file creation cmd was used in the connection
7	srv_serror_rate	The connection that used "flag" s3,s2,s1,s0 among the connection aggregated in "srv_count"
8	srv_rerror_rate	The connection aggregated in "srv_count", that used the"REJ" flag
9	srv_diff_host_rate	The connection aggregated in"srv_count" that a different destination address.
10	dst_host_diff_srv_rate	The percentage of connection aggregated in "dst_host_count" that used different service.
11	dst_host_same_src_port_rate	The percentage of connection aggregated in "dst_host_srv_count" that used the same port number.
12	dst_host_srv_diff_host_rate	The percentage of connection aggregated in "dst_host_srv_count" that used the different destination address
13	dst_host_serror_rate	The percentage of connection aggregated in "dst_host_count", that used "flag" s3, s2, s1,, s0

VI. RESULT AND DISCUSSION

The first algorithm 1 executes the SVM_IDS for predicting the packet which is normal or abnormal. The algorithm returns the two output one is predict the data and another one is predict probability value for each attributes. We have three times trained the packets at each time we put 5000 data and after build the model. In testing time, we put number of data and it gave better result (see the Table 3 SVM_IDS, XGB_IDS& HNIDS performance result)

The proposed work FDM, how to executes the SVM_IDS and XGB_IDS predict data and probability value. We have explained one sample input dataset.

SVM_IDS Predict Probability Data = (0.00012219,**0.992202006**,0.00095222,0.000863351,0.000777872,0.000569769,0.00127828,0.000914989,0.000953905,0.000344022,0.000442808,0.000150132,0.000142813,0.000142284,0.000142805)

XGB_IDS Predict Data = (0.00152938,**0.99802196**,8.89E-05,2.55E-05,1.42E-05,2.29E-05,8.85E-05,5.70E-05,1.77E-05,1.99E-05,2.31E-05,2.18E-05,2.30E-05,2.30E-05,2.30E-05)

HNIDS Predict Data = {**0.9902394**} = 1

Table 3: Performance analysis of FDM Combination Rule in HNIDS

Actual Data	XGB_IDS Predict Data	SVM_IDS Predict Data	HNIDS Predict Data
1	1	0	1
0	0	0	0
10	10	10	1
0	0	0	0
1	1	1	1
7	7	0	7
0	0	0	0

This is class details:

normal = 0,neptune = 1,warezclient = 3,ipsweep = 4,portsweep = 5,teardrop = 6,nmap = 7,satan = 8,smurf = 9,pod = 10,back = 11,guess_passwd = 12,ftp_write = 13,multihop = 14,rootkit = 15,buffer_overflow = 16,imap = 17,warezmaster = 18,phf = 19,land = 20,loadmodule = 21,spy = 22.

If we calculated the probability value of each algorithm and then get a maximum value of class is (HNIDS Predict Data = {**0.9902394**}) = 1. Class value 1 is Neptune that packet is attack to be find it.

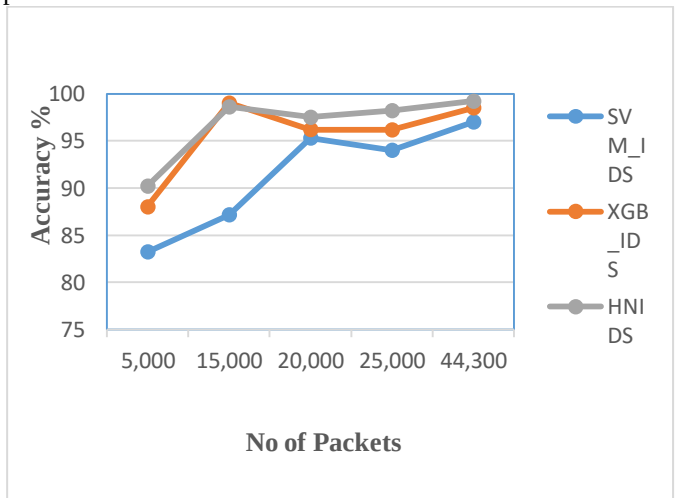

Figure 4: Performance analyze of HNIDS

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The comparative analysis of our proposed method HNIDS using FDM combination rule to improve the prediction data. Because the SVM_IDS classification learner to predict the some packets are abnormal and XGB_IDS classification learner to predict the some packets are abnormal. In that time some normal packets are not allowed the VM. So avoid this situation to improve the IDS, HNIDS introduce the FDM combination rule to analyze the packet. Whether the packet normal or abnormal (see the table 3). The compared to other method our proposed model is increasing the accuracy value to display the table 4 and how to improved our performance to see the graphical representation in figure 4. And over accuracy of SVM_IDS, XGB_IDS and HNIDS to display the figure 5.

Table 4: Comparative result on Accuracy values of proposed model with two best classification model

Over All Accuracy	SVM_IDS Accuracy	XGB_IDS Accuracy	HNIDS Accuracy (Proposed model)
	97	98.5	99.2

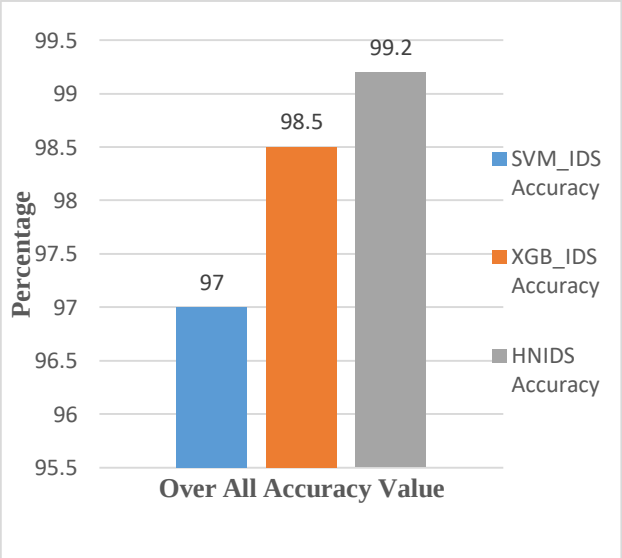

Figure 5: Results of Proposed System

VII. CONCLUSION

In this paper, we have presented a new distributed virtual HNIDS machine. HNIDS is a Hybrid Network Intrusion Detection System and its working in both signature and anomaly based intrusion detection. So, we are using supervised machine learning technique. The motivation of our goal is improved the real time prediction in minimum computation time. In this work,

We have applied the two most recent prediction classification learner one is SVM_IDS and another one is XGB_IDS. In this paper, we introduced the new rule that is fuzzy decision making rule. It takes the decision about the two classification gave some prediction result. Finally virtual network packet before enter the virtual machine the HNIDS to predict the packet whether the packet normal or any malicious attacks.

We have introduce the FDM Combination Rule to predict the packet with high accuracy value 99.2% with minimum time consuming and it's compared to XGB_IDS and SVM_IDS (97% & 98.5%) algorithm. In future work, HNIDS enhanced with IOT device to detected unwanted packets. The HNIDS using deep learning and its algorithms to predict the network packets in short time consuming.

REFERENCES

1. A. Kumbhare and M. Chaudhari, "IDS : Survey on Intrusion Detection System in Cloud Computing," International Journal of Computer Science and Mobile Computing, vol. 3, no. 4, pp. 497–502, 2014.
2. B. Mahalakshmi and G. Suseendran, "Effectuation of Secure Authorized Deduplication in Hybrid Cloud," Indian Journal of Science and Technology, vol. 9, no. 25, Jul. 2016.
3. T. Nathiya and G. Suseendran, "An Effective Hybrid Intrusion Detection System for Use in Security Monitoring in the Virtual Network Layer of Cloud Computing Technology," Data Management, Analytics and Innovation, Advances in Intelligent Systems and Computing, vol. 839, pp. 483–497, 2019.
4. J. Song, "Feature Selection for Intrusion Detection System Jingping Song Declaration and Statement," Department of Computer Science Institute of Mathematics, Physics and Computer Science, Aberystwyth University , Ph.D. Thesis, p. 132, 2016.
5. T. Nathiya and G. Suseendran, "An Effective Way of Cloud Intrusion Detection System Using Decision tree , Support Vector Machine and Naïve Bayes Algorithm," International Journal of Recent Technology and Engineering (IJRTE), vol. 7, no. 4S2, pp. 38–43, 2018.
6. T. Nathiya, "Reducing DDOS Attack Techniques in Cloud Computing Network Technology," International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE), vol. 1, no. 1, pp. 23–29, 2017.
7. M. Alauthman, O. Dorgham, A. Almomani, F. Albalas, and A. Obeidat, "An Online Intrusion Detection System to Cloud Computing Based on Neucube Algorithms," International Journal of Cloud Applications and Computing, vol. 8, no. 2, pp. 96–112, 2018.
8. W. Feng, Q. Zhang, G. Hu, and J. X. Huang, "Mining network data for intrusion detection through combining SVMs with ant colony networks," Future Generation Computer Systems, vol. 37, pp. 127–140, 2014.
9. M. Mazini, B. Shirazi, and I. Mahdavi, "Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms," Journal of King Saud University - Computer and Information Sciences, 2018.
10. K. Siddique, Z. Akhtar, M. A. Khan, Y. H. Jung, and Y. Kim, "Developing an intrusion detection framework for high-speed big data networks: A comprehensive approach," KSII Transactions on Internet and Information Systems, vol. 12, no. 8, pp. 4021–4037, 2018.
11. M. S. Moorthy Manthira and M. Rajeswari, "Virtual host based intrusion detection system for cloud," International Journal of Engineering and Technology, vol. 5, no. 6, pp. 5023–5029, 2013.
12. M. Almseidin, M. Alzubi, S. Kovacs, and M. Alkasassbeh, "Evaluation of machine learning algorithms for intrusion detection system," SISY 2017 - IEEE 15th International Symposium on Intelligent Systems and Informatics, Proceedings, pp. 277–282, 2017.
13. M. Raza, I. Gondal, D. Green, and R. L. Coppel, "Fusion of FNA-cytology and Gene-expression Data Using

Dempster-Shafer Theory of Evidence to Predict Breast Cancer Tumors," Bioinformation, vol. 1, no. 5, pp. 170–175, 2012.
14. A. Verma and V. Ranga, "Statistical analysis of CIDDS-001 dataset for Network Intrusion Detection Systems using Distance-based Machine Learning," Procedia Computer Science, vol. 125, pp. 709–716, 2018.
15. G. Ansari, "Framework for Hybrid Network Intrusion Detection and Prevention System," Interational journal of computer Technology & Application, vol. 7, no. August, pp. 502–507, 2016.
16. L. Hoang Son et al., "APD-JFAD: Accurate Prevention and Detection of Jelly Fish Attack in MANET," IEEE Access, vol. 6, no. Issue(1), pp. 56954–56965, 2018.
17. F. H. Botes, L. Leenen, and R. De La Harpe, "Ant colony induced decision trees for intrusion detection," European Conference on Information Warfare and Security, ECCWS, no. June, pp. 53–62, 2017.
18. H. Liu, Z. Wu, C. Peng, F. Tian, and L. Lu, "Adaptive gaussian mechanism based on expected data utility under conditional filtering noise," KSII Transactions on Internet and Information Systems, vol. 12, no. 7, pp. 3497–3515, 2018.
19. S. S. Dhaliwal, A. Al Nahid, and R. Abbas, "Effective intrusion detection system using XGBoost," Information (Switzerland), vol. 9, no. 7, 2018.
20. G. Suseendran, E. Chandrasekaran and Anand Nayyar ,"Defending Jellyfish Attack in Mobile Ad hoc Networks via Novel Fuzzy System Rule G.," Data Management, Analytics and Innovation, Advances in Intelligent Systems and Computing, vol. 839, pp.437-455, 2019..
21. T. Reineking, "Belief functions: theory and algorithms," 2014.