International Journal of Scientific Research and Engineering Development-– Volume 5 Issue 3, May-June 2022

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Neuro Based Strategy for Real Time Protection of Wireless Broadband Ecosystem Against DDoS Attack

Ogbeta L.K.*, Nwobodo L.O.**, Ebere U.C.***

*,**Enugu State University of Science and Technology

***Destinet Smart Technologies

Electrical and Electronics Engineering Department, Enugu State University of Science and Technology, ESUT, Enugu

Email; kelvo4jesus@gmail.com,

----------**********----------

Abstract:

This research presented a neuro based strategy for real time protection of wireless broadband ecosystem against DDoS attack. This was embarked on after series of literature reviews which revealed that DDoS attack is the main attack model used by hackers to cause online threat. To address this problem, the study developed an intelligent security system based on the IEEE 802.11 methodology, using data collection, artificial neural network, system identification, training, classification and prediction. The system was designed using modeling diagrams, self defining equation, algorithms and then deployed on the wireless network using Simulink. The performance was evaluated using Mean Square Error (MSE), Regression (R), response time and it was observed that MSE is 0.0156Mu, R is 0.987 and time of response is 21.2ms which is very good according to the IEC 62591 standard for real time in wireless communication system.

.

Keywords — ***DDOS attack, real time, wireless broadband ecosystem, artificial neural network.***

----------**********----------

I. INTRODUCTION

Recently, Information and Communication Technology (ICT) has grown sporadically, no surprise considering the huge benefits it presents such as the limitless ability to send, receive, store and retrieve information over wireless broadband networks. According to (Motukuri, 2016) wireless broad is a high speed telecommunication technology which allows remote communication access over a wide area network. This technology has been embraced worldwide as it facilitates interoperability between public and private enterprises, thereby enabling the exchange of varieties of data from one network to another.

Over the year, studies have been proposed to improve the quality of wireless broad band network (Brauchhoff et al., 2010; Karun and Uma, 2015), focusing mainly on the optimal throughput, routing speed, loss mitigation, latency mitigation among other key performance indicators of wireless network, but ignored the security architecture of the system which is the most vital component of any reliable communication network. This fundamental flaw in the Wireless Broadband Network (WBN) has been exploited by hackers to cause harm and theft. Hence the need for optimal security of WBN, even though it has been addressed in some studies using encryption techniques (Karun and Uma, 2015), genetic algorithms (Jongsuebsuk et al., 2014), machine learning algorithm (Masduki et al., 2015; Hodo et al., 2016; Hong et al., 2011) among others, yet the issues of data network security remains a top topic for discussion in the field of ICT.

According to (Hodo et al., 2016; Lakhina et al., 2004) some of the recent threat models ranges

from man in the middle attack, wormhole attack, Distributive Denial of Service (DDoS) attack, etc. however the most employed in recent times is the DDoS attack. This attack type targets the WBN server and shut it down using flood of service request until the server gets overloaded and shut down (Mishra et al., 2011). Some of these attack cases were discussed in (Dawoud et al., 2010; Contel, 2020).

Among the various security strategies already pointed out in (Karun and Uma, 2015; Jong et al., 2014; Masduki et al., 2015; Hodo et al., 2016; Hong et al., 2011) the use of Machine Learning Algorithms (MLA) have provided the best solution so far for real time detection of DDoS attack, compared to the counterparts. This is due to the ability of MLA to learn from training data and then make accurate decisions. However the effectiveness of each MLA is dependent on the types of problem under study.

The problem of DDoS attack is a pattern recognition types as the feature vectors of the attack traffic are characterized with certain patterns different to the normal traffic. Hence this justifies the use of Artificial Neural Network (ANN) as the best MLA to address this challenge. However, the conventional ANN solutions as in (Kumar and Muthu, 2014; Suneetha et al., 2019) are unable to achieve real time threat detection objectives, despite their success and this has hindered the reliability of the system for optimal security solution against DDoS among other types of online threats. To address this challenge the researcher proposes a neuro predictive model which will be trained as a reference DDoS attack model and used to detect and predict time series DDoS attack model. This will be achieved in this paper developing a neural network predictive model and training it with data collected from a DDoS attacked WBN repository. This trained reference model will be used for time series classification to provide real time DDoS attack detection on WBN and isolate the threat.

Literature review

Senthilnayaki and Kannan (2015) used generic based support vector machine to address the problem of DDoS attack on WBN and achieved 95.38% detection accurate, however the limitation is delay detection time which was over 50 minutes delay time. Suneetha et al. (2019) presented a comprehensive survey of existing literature on cloud computing security challenges and solution is presented. At the end of this paper the authors identified the DDoS threat as the most recent threat methodology for cloud attack and proposed the use of artificial intelligence as the best approach to tackle the menace. Nabeel (2016) Presented a research work on data security model using artificial neural network and database fragmentation in cloud computing. The research was implemented using dynamic hashing fragmented components and implemented for storing fragmented sensitive secret data. The proposed algorithm applied shows high data security confidentiality on cloud database. However, the percentage accuracy was not specified in the work to justify the efficiency of the training algorithm. Alma et al. (2019) presented a network traffic analysis strategy against DDoS attack in air interface. The study was conducted to help mitigate the effects of DDoS on WBN, but despite the success was unable to detect the threat in real time. Keval et al. (2020) addressed the problem of DDoS in timely manner using internet of things and wireless sensor network, but the study can be improved using machine learning. Nadia (2020) used a multiple classification approach to address the issues of DDoS on WBN, but despite the success, the study was limited due to high computational time taken to detect the attack

II. METHODS AND SYSTEM MODELLING

Senthilnayaki and Kannan (2015) used generic based support vector machine to address the problem of DDoS attack on WBN and achieved 95.38% detection accurate, however the limitation is delay detection time which was over 50 minutes delay time. Suneetha et al. (2019) presented a comprehensive survey of existing literature on cloud computing security challenges and solution is presented. At the end of this paper the authors

identified the DDoS threat as the most recent threat methodology for cloud attack and proposed the use of artificial intelligence as the best approach to tackle the menace. Nabeel (2016) Presented a research work on data security model using artificial neural network and database fragmentation in cloud computing. The research was implemented using dynamic hashing fragmented components and implemented for storing fragmented sensitive secret data. The proposed algorithm applied shows high data security confidentiality on cloud database. However, the percentage accuracy was not specified in the work to justify the efficiency of the training algorithm. Alma et al. (2019) presented a network traffic analysis strategy against DDoS attack in air interface. The study was conducted to help mitigate the effects of DDoS on WBN, but despite the success was unable to detect the threat in real time. Keval et al. (2020) addressed the problem of DDoS in timely manner using internet of things and wireless sensor network, but the study can be improved using machine learning. Nadia (2020) used a multiple classification approach to address the issues of DDoS on WBN, but despite the success, the study was limited due to high computational time taken to detect the attack

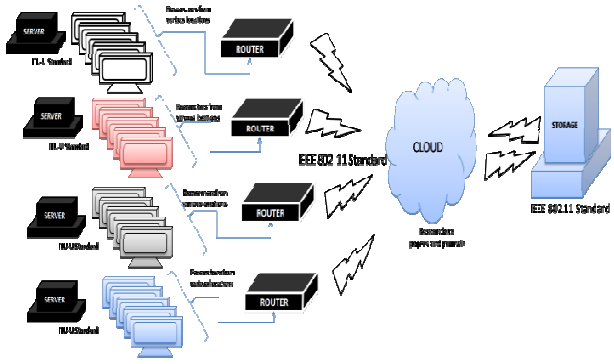

Figure 1: Architectural model of the WBN

The figure1 presented the architectural model of the case study WBN where interconnected users shares information over the cloud and are stored on the virtual server. The users communicated over the network based on IEEE 802.11 methodology through interconnected wireless local area network composed of user equipments, routers, servers and necessary communication devices. The aim of this research is to protect this network against DDoS attack.

Model of the DDOS Attack

The modeling of the proposed system was presented using universal modeling diagram and self defining equations. These design approach employs logical diagrams like the data flow diagram, system flow charts, use case and architectural diagram for the design of the new system. The data flow model of the DDoS attack model is presented in figure2;

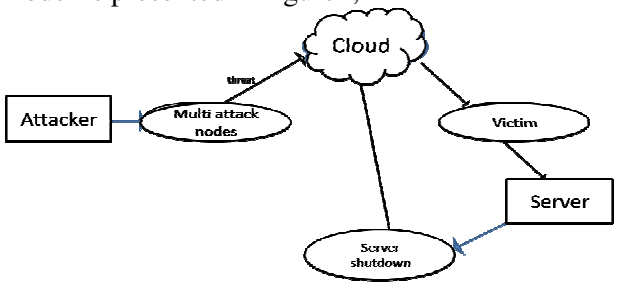

Figure 2: Data flow diagram of the DDoS attack model

The model shows how attackers create multi virtual nodes which are packets IP and send to the server at the same time, which over loads it and then shut it down. The characteristics of the attack are presented using the data description Table 1 which contains nine input classes of the DDoS attack attributes as presented in the table 1;

Table 1: CAIDA DDoS dataset parameters (Source: Brauckhoff et al., 2010)

S/N	Name	Description	Data Type
1	Average Packet time interval	Time interval close to zero seconds since agent send multiple data very fast	Continuity type
2	Average Packet flow size	They have the same packet size usually less then 100bytes	Continuity type
3	Protocol type	TCP, UDP, UP or more	Integers
4	TCP SYN	No server response	Discrete

	response	acknowledgement	type
5	Destination IP	Similar IP destination within short time	Continuity type
6	Average packet flow rate	DDoS is sending large packet flow in order to disable the server	Discrete type
7	Land connection	1 if connection is from same host or 0 if otherwise	Binary
8	Packet size variance	Massive number in small time frame	Continuity type
9	IP flood	Flooding the server with numerous IP at ones	Continuity type

Model of the artificial neural network

Model of the artificial neural network is designed considering the number of input attack vectors from table 1 and then feed forward to the neural network as a nonlinear auto regressive (NARX) model as shown below:

$$y(k+d)=N(y(k),y(k-1),\ldots,y(k-n+1),u(k),u(k-1),\ldots\ldots u(k-n+1)) \quad 1$$

The NARX is a mathematical functions used by neural network to identify dynamic time series events for training. Where u(k) is the attack feature vectors input, N is the non linear function, n is the number of i9nput unit, d is an integer delay, and y(k) is the system output. Now that we have defined the system, the neural network model in equation 1 was trained to approximate the function (N) so as to generate a reference prediction model. The training model is presented as shown below;

$$y(k+d)=f(y(k),y(k-1),\ldots,y(k-n+1),u(k-1),\ldots,u(k-m+1))+g(y(k),y(k-1),\ldots,y(k-n+1),u(k-1),\ldots,u(k-m+1))\cdot u(k) \quad 2$$

From the training structure in equation 2, the training is formulated as a procedure for modifying the weight and biases of a network. In order to move the outputs (y) closer to the target (f), the objective is to reduce the mean square error, meaning of which is the difference between the neuron response (n) and the target vector (m) at which the loss function (mean square error) takes a minimum value k, while g is the training algorithm.

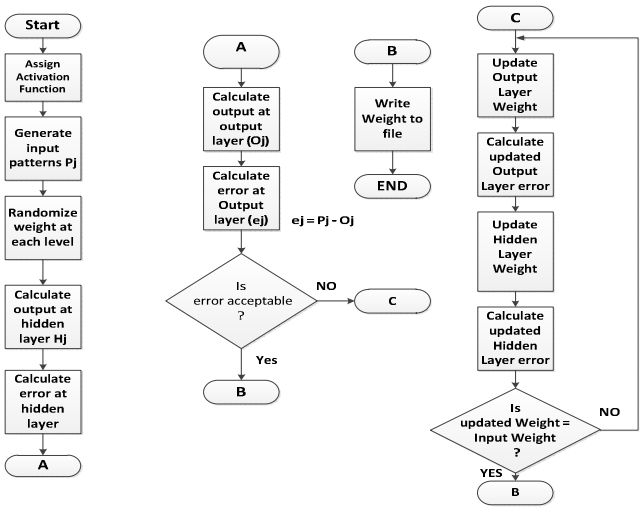

Figure 3: Logical Flow model for the training algorithm

The training algorithm shows how the neural network weights and bias are activated to learn the patterns of the DDoS attack vectors. The algorithm uses a computation of gradient loss function for the weights and bias to fine tune the neurons, based on the update values, until an acceptable error margin is recorded.

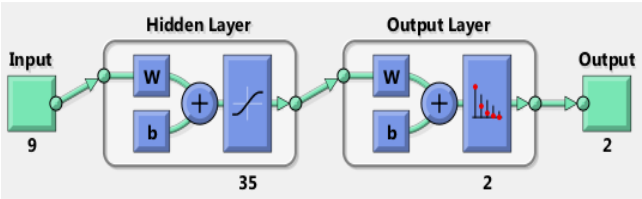

Figure 4: Simulink structure of the ANN

The figure 4 presented the neural network architecture developed with the neural network toolbox in simulink. This was achieved feeding the dataset into the neural network tool for automatic configuration of the architecture already modeled in equation 1 and 2; which shows the input layers with the number of input attributes of DDoS attach which in this case is 9, the hidden layer which is 35 and the 2 output

layer which are either an attack traffic or normal traffic

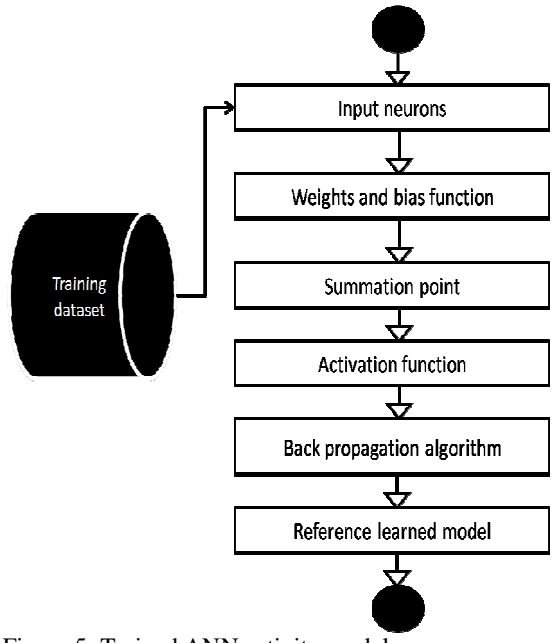

Figure 5: Trained ANN activity model

Table 2: Simulation Parameters

Parameters	Values
Training epochs	20
Size of hidden layers	35
Number of algorithms used	3
Training segments	30
No. delayed reference input	2
Maximum feature output	2
Maximum feature input	9
Number of non hidden layers	10
Maximum interval per sec	2
No. delayed output	1
No. delayed feature output	2
Minimum reference value	-0.7
Maximum reference value	0.7
Time	0.05sec

The input of the neural network are presented with x(t) at unit delay interval time lag. The activation function used is a tansig hyperbolic mathematical function in (Emenike, 2021) which was used at the middle layer of neural network to calculate the middle layer's output from the net input of the input layers. It was used because it can handle values between -1 and +1. This is good in case there is a negative input value. At the output layer, the purelin function (Emenike, 2021) was used because it has the capability of handling variable inputs and producing a single output as the training result which is the attack reference model as shown below;

$$u(k+1) = \frac{yr(k+d) - f(y(k),\ldots..,y(k-n+1),u(k),\ldots..,u(k-n+1))}{g(y(k),\ldots..,y(k-n+1),u(k),\ldots..,u(k-n+1))} \quad 3$$

The model of equation 3 presented the neural network reference classification model which represented the learned DDoS attack vector and was used as a reference point for time series classification to detect future DDoS attack threat on the WBN and then predict it using the model in equation 4; (See training parameters in table 2)

$$J = \sum_{j=N_i}^{N_2}(y_r(t+j) - y_m(t+j)^2 + p\sum_{j=1}^{N_u} u^i(t+j-1) - u^i(t+j-2))^2 \quad 4$$

Where N_1, N_2, and N_u define the horizons over which the training error and the prediction features are evaluated. The u' variable is the tentative feature vectors, y_r is the desired response, and y_m is the network model response. The p value determines the contribution that the sum of the squares of the control increments has on the performance index. The model consists of the neural network training model and the optimization block. The optimization block determines the values of u' that minimize J, and then the optimal u is input to the network.

The system Architectural Diagram

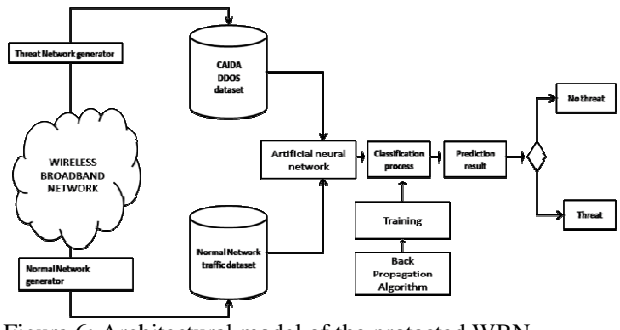

Figure 6: Architectural model of the protected WBN

The figure 6 presented the deployment of the intelligent security model developed on the WBN. This was achieved deploying the intelligent DDoS security monitoring and detection system developed on the network. To achieve this, the intelligent security model monitors data flow from the WBN via training of every parameters based on the attributes of table 1 to detect patterns of DDoS attack and isolate immediately from the network.

Performance evaluation

The overall accuracy of the neural network classifier is estimated by dividing the total correctly classified positives and negatives feature vectors by the total number of samples in the CAIDA dataset. The accuracy of a classifier on a given set is the percentage of test set features that are correctly classified by the network as shown below;

$$\text{True Positive Rate (TPR)} = \frac{TP}{TP+FN} \quad 5$$

$$\text{False positive Rate (FPR)} = \frac{TN}{TN+FP} \quad 6$$

Where TN = true negative,
FN = false negative,
FP = false positive and
TP = true positive.

$$MSE = \frac{1}{N}\sum_{n=1}^{N}(S_o(n) - S_f(n))^2 \quad 7$$

Where S_o is the learned model of DDoS attack, S_f is the time series data from the WBN, n is the number of input, N is the average time for n sample of data collected.

III. IMPLEMENTATION

To implement the system developed, communication system toolbox, neural network toolbox, statistics and machine learning toolbox, WLAN toolbox, the modeling diagram and equations developed and Simulink.

IV. RESULTS AND DISCUSSIONS

This section presented the performance of the intelligent DDoS protection system developed and deployed on the WBN. The result was achieved using the neural network training toolbox. The toolbox automatically divided the training set into three multi sets of 70:15:15 for training, test and validation. The performance of the multi sets are evaluated using the mean square error (MSE) analyzer instrument in figure 7;

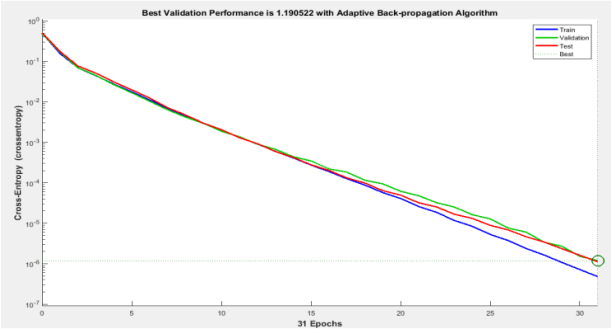

Figure 7: Result of the improved training algorithm

From the result presented in figure 7, the performance of the intelligent DDoS security scheme based on MSE is 0.0156, while best validation result is 1.190522 at epoch 31 which is the epoch value the neural predictive model performs best. The error histogram is presented in figure 8;

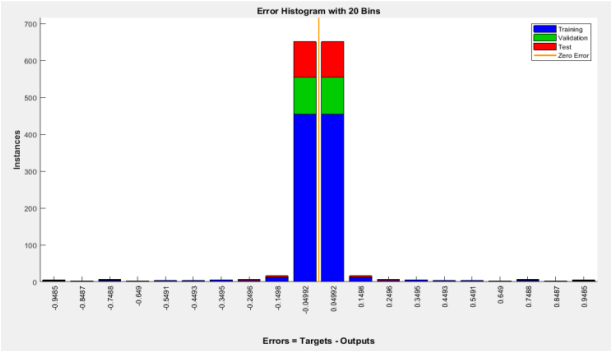

Figure 8: The error histogram result

This graph in figure 8 was used to determine the histogram of errors between target values and predicted values after training the neural network. The total error from the training process ranges from -0.9485 to 0.9485 which are divided into 20 bins with an average weight of 1.897, this weight value was used to update the learning rate as the training process was performed and the performance analyzed using the regression graph in figure 9;

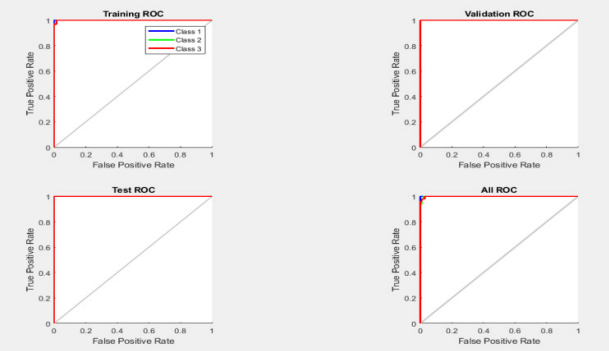

Figure 9: Regression result

The result in figure 9 presents the regression performance of the neural network, when trained for the multi sets. From the result, the true and false positive values for each set are analyzed and the result presented in figure using the table 4.4;

Table 4.4: training performance for the improved training algorithm

Training result	False positive value	True positive value
Test set	0.000	1.000
Train set	0.009	0.981
Validation set	0.000	1.000
Overall	0.013	0.987

From the table 4.4, the regression performance of the new algorithm was presented showing the true and false positive rates respectively. From the overall performance it was observed that overall regression result for the training process is 0.987 for true positive rate. The implication of this result shows that the correct detection and prediction accuracy of the attack vector by the network is very précised. The response time behavior of the neural network predictive controller is presented in figure 10;

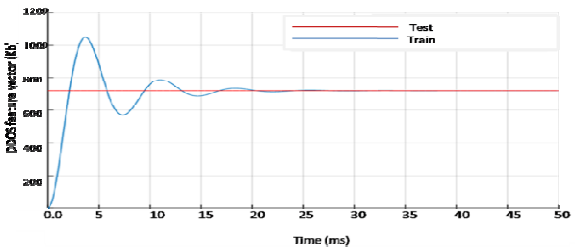

Figure 10: response time of attack detection

The result in figure 10 presented the response time of the neural network predictive controller to detect and isolate DDOS attack threat on the network. From the result it was observed that the intelligent security system detected the DDoS feature abnormally at 0.22ms and isolated it at 21.2ms. The implication of this result show that the intelligent neural network security model developed was able to protect the WBN in real time based on the IEC 60870-6 definition of real time.

V. CONCLUSION

This paper has successfully presented an intelligent security model for real time protection of WBN. The model employed a predictive approach which collected data of DDoS abnormally and train to detect an attack on the network and isolate within 21.2ms. The regression result showed that the security model developed was reliable as it recorded a regression performance of 0.987 and a MSE performance of 0.0156.

VI. CONTRIBUTION TO KNOWLEDGE

i. Neural network predictive model was developed for the real time protection of WBN against DDOS attack
ii. The security model developed was able to detect and isolate DDOS attack in real time of 21.2ms.

REFERENCES

[1] Alma D Lopez, Asha P Mohan, and Sukumaran Nair (2019) "Network traffic behavioral analytics for detection of ddos attacks. SMU Data Science Review, 2(1):14.
[2] Brauckhoff, D., Salamatian, K., and May, M., (2010).A signal processing view on packet sampling and anomaly detection. In Proceedings of the 29th conference on Information communications, INFOCOM'10, pages 713–721, Piscataway, NJ, USA; IEEE Press.
[3] Brauckhoff, D., Salamatian, K., and May, M., (2010).A signal processing view on packet sampling and anomaly detection. In Proceedings of the 29th conference on Information communications, INFOCOM'10, pages 713–721, Piscataway, NJ, USA, 2010. IEEE Press.

[4] Contel Bradford (2020)," 7 most famous cloud security breaches"; storage craft technology corporation.
[5] Dawoud W., Takouna, I., Meinel, C. (2010), "Infrastructure as a service security: Challenges and solutions," in *the 7th International Conference on Informatics and Systems*, Cairo.
[6] Emenike N. (2021) "Real time flood monitoring and detection system using artificial intelligence technique" Master's Thesis. Unizik Awka. Nigeria. (unpublished)
[7] Hodo, X. Bellekens, A. Hamilton, P.-L. Dubouilh, E. Iorkyase, C. Tachtatzis, and R. Atkinson (2016) "Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System," 3rd International Symposium on Networks, Computers and Communications (ISNCC), 2016, pp. 1–6.
[8] Hodo, X. Bellekens, A. Hamilton, P.-L. Dubouilh, E. Iorkyase, C. Tachtatzis, and R. Atkinson (2016), "Threat analysis of IoT networks Using Artificial Neural Network Intrusion Detection System," 3rd International Symposium on Networks, Computers and Communications (ISNCC), pp. 1–6.
[9] Horng, M.-Y. Su, Y.-H. Chen, T.-W. Kao, R.-J. Chen, J.-L. Lai, and C. D. Perkasa, (2011) "A novel intrusion detection system based on hierarchical clustering and support vector machines," Expert Syst. Appl., vol. 38, no. 1, pp. 306–313.
[10] IEC 62591 Ed. 1.0 b: 2010, "Wireless Communication Network and Communication Profiles—Wireless HART™," 2010.
[11] Jongsuebsuk, N. Wattanapongsakorn, and C. Charnsripinyo (2014) "Network intrusion detection with Fuzzy Genetic Algorithm for unknown attacks," in The International Conference on Information Networking (ICOIN).
[12] Karun Handa, Uma Singh (2015), "Data Security in Cloud Computing using Encryption and Steganography", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 4, Issue. 5, pp.786 – 791.
[13] Keval Doshi, Yasin Yilmaz, and Suleyman Uludag (2020) "Timely Detection and Mitigation of Stealthy DDoS Attacks via IoT Networks" arXiv:2006.08064v1 .
[14] Kumar P. R.Muthu Vijay Deepak (2014): Privacy Preserving Back-Propagation Neural Network In Cloud Computing. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 6.
[15] Lakhina, A., Crovella, M., and Diot, C., (2004). Characterization of network-wide anomalies in traffic flows. In Proceedings of the 4th ACM SIGCOMM conference on Internet measurement, IMC '04, pages 201–206, New York, NY, USA, 2004. ACM.
[16] Masduki, K. Ramli, F. A. Saputra, and D. Sugiarto (2015), "Study on implementation of machine learning methods combination for improving attacks detection accuracy on Intrusion Detection System (IDS)," International Conference on Quality in Research (QiR), 2015, pp. 56–64.
[17] Mishra, A., Gupta, B., B., and Joshi, R., C., (2011). "A Comparative Study of Distributed Denial of Service Attacks, Intrusion Tolerance and Mitigation Techniques," Proc. of European Intelligence and Security Informatics Conference (EISIC), IEEE, pp. 286-289, September 2011.
[18] Motukuri Prashanthi (2016); Analysis of Security Issues in Virtualization Cloud Computing; Assistant Professor, CSE Dept., CMR Engineering College, Hyderabad; Motukuri Prashanthi, International Journal of Computer Science and Mobile Computing, Vol.5 Issue.8, August- 2016, pg. 274-281
[19] NabeelKhana, Adil Al-Yasiri (2016):The 2nd International Workshop on Internet of Thing: Networking Applications and Technologies;(IoTNAT' 2016) Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework University of Salford, 43 Cresent Salford, Manchester and M5 4WT, United Kingdom. Procedia Computer Science 94 (2016) 485 – 490 on Recent Advances in Information Technology (RAIT), 2012, pp. 131–136
[20] Nadia Chaabouni (2020) "Intrusion detection and prevention for IoT systems using Machine Learning"; Systems and Control. Université de Bordeaux, 2020. English. NNT :
[21] Senthilnayaki, K. Venkatalakshmi, and A. Kannan (2015) "Intrusion detection using optimal genetic feature selection and SVM based classifier," 3rd International Conference on Signal Processing, Communication and Networking (ICSCN), 2015, pp. 1–4.
[22] Suneetha D. Rathna Kishore, G.G.S.Pradeep (2019); Data Security Model Using Artificial Neural Networks and Database Fragmentation in Cloud Environment ; International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-2, ,5972 Published By: Blue Eyes Intelligence Engineering & Sciences Publication
[23] Suneetha D. Rathna Kishore, G.G.S.Pradeep (2019); Data Security Model Using Artificial Neural Networks and Database Fragmentation in Cloud Environment ; International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-2, ,5972 Published By: Blue Eyes Intelligence Engineering & Sciences Publication

