Intrusion Detection In IoT Using Artificial Neural Networks On UNSW-15 Dataset

Sohaib Hanif, Tuba Ilyas, Muhammad Zeeshan
National University of Sciences and Technology (NUST) Islamabad, Pakistan
{shanif.msit18seecs, tilyas.msit18seecs, muhammad.zeeshan}@seecs.edu.pk

IoT devices are susceptible to numerous cyber-attacks due to its low power, low computational requirements and controlled environment that make it hard to implement authentication and cryptography in IoT devices. In this work we propose artificial neural network based threat detection for IoT to solve the authentication issues. We use supervised learning algorithm to detect the attacks and furthermore controller discards the commands after classifying it as threat. Proposed ANN consist of input, hidden and output layers. Input layer passes the data as signal to hidden layer where these signals are computed with the assigned weights and activation functions are used to transform an input to an output signal. Proposed technique is able to detect attacks effectively and timely decisions are taken to tackle the attacks. Proposed ANN approach achieves an average precision of 84% and less than %8 of average false positive rate in repeated 10-fold cross-validation. This reveals the robustness, precision and accuracy of proposed approach in large and heterogeneous dataset. Approach proposed in this work has the potential to considerably improve the utilization of intrusion detection systems.

Keywords— Intrusion Detection, ANN, Network Security, Machine Learning, IOT

I. Introduction

With rapid growth in IoT, heterogeneity of connected devices and other challenges are very critical which include power minimization, security intrusion detection, and hardware updating and connectivity issues. Our concern is security in IoT to keep the devices safe from different attacks. There are four types of attacks which occur in IoT: Denial of service attack which consumes a lot bandwidth of network and processing capabilities of devices by sending fake requests. Second is malware attack in which attacker intrude and/or tap devices to steal information. Third is data breach attack which retrieved confidential data from the network. Fourth threat is weakening perimeters in which IoT structure is globally not standardized so the devices are not vulnerable for security [1-2]. The artificial intelligence techniques can be used for comparing and identify between normal patterns are threat detection pattern [2]. Existing work on intrusion detection system is carried out on non-heterogeneous data, which is large but it is same type of data.

In this work we propose fast and effective ANN based threat detection mechanism to identify extensive variety of data integrity attacks in IoT framework. We carried out experiments for heterogeneous dataset instead of homogenous dataset and get effective results as we demonstrate the comparison with previous works. In proposed technique dissimilar dataset including valid and invalid scenarios as input constraints. The model is trained on dataset and then implanted in controller of IoT framework to identify any abnormal conduct and prevent from it. Model is trained to identify such scenarios and report to main server.

UNSW-NB 15 [15] is used to train and test the proposed ANN based threat detection approach. This dataset consists of nine kinds of attacks that include backdoors, generic, fuzzers, exploits, shellcode, analysis, worms, DoS and reconnaissance. There are two million records 49 features are available with class labels. There are 175,341 records for training purpose and for testing purpose there are 82,332 records and each record comprise of different type, either be normal or attack. This dataset is different from previous datasets like KDDCUP 99 which has less number of networks and more repetition and fewer features [16]. As this dataset has different kind of attacks, larger networks and large amount of data which makes it suitable for IoT networks.

ANN is general machine learning approach used for classification. As we are interested in threat detection in IoTs which has usually large amount of data, ANN fulfills the need. The dataset used has large amount of data and different types of attacks. For this Neural Networks works well for these type of large datasets. Furthermore, IoT is complex model and it connects different devices and machines which produces enormous amount of data. ANN is best fit for classification problem of these type of complex and enormous data. ANN model consist of three layers specifically input, hidden and output layer. Data is passing through input layer as signals (x1, x2) to hidden layer. Hidden layer computes activation function with the help of input signal and assigned weights. Activation function converts the input signal to an output signal. We used one hidden layer in our model as MLP (multi-layer perception) is normally used for complex problems like face recognition where each layer works on different features. Hidden layer can't be accessed from outside. Error is collected from each training data and weights are updated.

We compared our results with neural network based attack classification and intrusion detection, [18] intrusion detection by fuzzy interpolation, [14] and intrusion detection by fuzzy clustering [17]. Our results are still comparable with these approaches beside the fact our approach is on IoT based dataset and have more networks, less repetition and more attacks. Results demonstrate that proposed approach is efficient for recognizing threats with very high precision and insignificant quantities of false positives. The proposed method is authenticated by means of recurring cross validation and verified by admiration to making of false positive cautions on a huge dataset of usual network traffic file subjects. Following are the contribution of this work:

- We present the design and implementation of intrusion detection system built on artificial neural networks using latest and heterogeneous dataset UNSW-15.
- Proposed method is able to classify threats with high accuracy of 84% and 8% of low false positive rate on latest heterogeneous UNSW-15 dataset.

- Tested the efficiency of proposed scheme on a latest large heterogeneous dataset UNSW-15.

The rest of work is organized as follows: Existing work related to threat/intrusion detection in IoT is summarized in section II. The general method and implementations specifics of the proposed ANN based intrusion detection and prevention mechanism for an IoT framework is described in Section III. Experiments and results are described in Section IV and Section V concludes this work and highlights some potential direction for further work.

II. Related work

In recent work like [1], authors proposed thread detection in IoT using artificial Neural Network (ANN) and used a supervised ANN to packet trace than detects DDoS attack. The objective of technique is to classify the normal pattern and threat pattern, save bandwidth and resources which consume distributed DDoS attack. Authors in [2] address intrusion detection in software define IoT networks by using IA techniques, two stages of prevent SDN IoT networks from thread. The objective of technique is low overhead and more accuracy compare with other existing solutions. IoT indicates to a system of linked physical devices that are implanted with software, sensors, hardware, and communication components [3]. IoT has high volume logical data which empowers almost every field of human life [4]. Security and privacy are the biggest problems of IoT [5-6].

Interoperability is additional examination for IoT as of the requirement to deal with an expansive number of varied things that have a room with numerous phases [7]. Work in [8] presents intrusion detection in IoT for prevention of different attack by using data mining technique in smart grid. In [9] the authors address intrusion detection in IoT devices by leverage data flows as seen by provenance graphs. The provenance graphs show comparison to other reduction of dimensionally and vector space representation. The object of technique is to detect false and true positive rates of technique. In [10] authors introduce Clort which is extension of NIDS snort which is best for offloading pattern matching on GPU. The object of technique is low power consumption and throughput in IoTs. The Clort have 25% faster throughput than GPU and 33% less energy is consumed.

In [11] authors represent intrusion detection and prevention in IoT by using Random neural network (RNN). The objective of technique is minimal performance overhead. The accuracy is 97.23% in random anomalous activities. In [12], authors' present algorithm which is capable of identifies and definitively true or false intrusion detection without operator input in random environment which changes time to time. The objective of algorithm is identified number of intrusions effected packets it is 34% accuracy of detection all type of intrusion. It uses two tired negative selection process to decrease effected packet by co-simulation. Work in [13], is intrusion detection using artificial neural network. The ANN is capable of differentiate malicious packets and normal packets. The objective is to decrease false positive rate which is less 2%. The ANN used both conventional network traffic and cyber network traffic analyzer. The performance is maximizing and minimizing false rate which is less than 2%.

We propose an artificial intelligence based algorithm to detect threats and work efficiently as compared to previous works on threat detection in IoT and it performs much better. It detects the threat efficiently and takes decisions timely to block that attack. System is trained on specific dataset and classifies unknown behavior easily. With proposed technique there is very rare chances of error rate and detects threats efficiently.

III. ANN BAsed Intrusion Detection

A. Problem Domain

Previous work defines intrusion as accessing the confidential information, availability of computer resources and data integrity. Intrusion includes software, hardware and password sniffing. In IoT the data can be manipulate and information can steal through intrusions. Enormous amount of traffic is directed towards the network and network resources are wasted without usage. Simple intrusion detection system (IDS) is not capable of threat detection for unseen data. When large amount of data is sent, false positive rate increases. Packets which are even benign are considered as anomalous packets. To overcome above mentioned problems, artificial intelligence (AI) techniques are used like ANN which captures non-benign data and false positives efficiently.

B. Artificial Neural Networks

Artificial Neural Networks are the method of machine learning algorithm encouraged through the actions of biotic neurons situated in the mind and central nervous system. Inputs to ANN is automatically served to the artificial neurons in generally one or more hidden layers, weighted and managed to select the production to the next level. An association between neurons is represented by number and non-linear function is used to process outcome of each neuron. These associations are named as edges. These weights change as the learning continues and this change increments or decrements association's sign quality. The sign is possibly sent if the total sign crosses the edge.

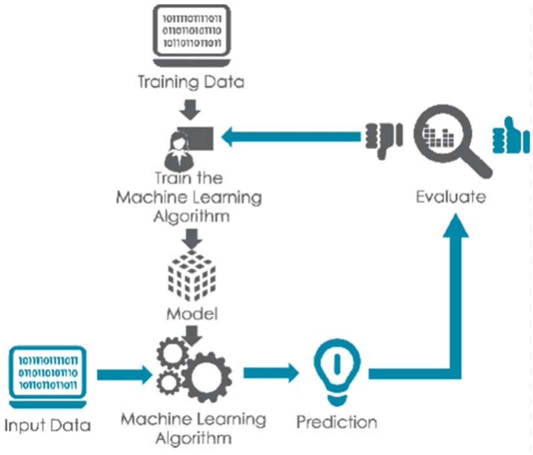
Training Data
Train the Machine Learning Algorithm
Evaluate
Model
Input Data
Machine Learning Algorithm
Prediction

Fig. 1. Supervised learning scheme

Normally, neurons are collected into layers. Source input is transformed by changes performed by various layers. Sign passes by layers in some specified sequence and its value keeps on transforming. ANN is a supervised learning technique and makes usage of learning instructions that permits the weights and biasness of the hidden layer and final level neurons to be acclimatize. Fig 1 Shows supervised learning scheme that how supervised learning detects the correct output in large dataset.

C. Artificial Neural Network Architecture

We develop threat detection system by means of artificial neural network (ANN) in IoT. IoT is complex model and it connects different devices and machines which produces enormous amount of data. ANN is best fit for classification problems of these type of complex and enormous data. Dataset is distributed into training and testing chunks and further use to validate the architecture. The ANN technique is implemented in IoT controller which classify non-benign packet and discards in case of any attack. We used three layered neural network consisting input, hidden and output layers.

The input layer is used to feed the data into model in the form of signals X1, X2, X3, Xn. Weights W1, W2, W3 and Wn are assigned to each input signals. b is biasness value and its role is similar to threshold and it determines whether the neuron is activated or not. Information is saved on neural network is form of weights and bias.

$$V=(X1*w1) + (X2*w2) + (X3*w3) + b \qquad (1)$$

The equations (1) clearly show that the effect of the signals is less than the assigned weight. In equation, inputs are multiplied with the assigned weights and at last we add bias value b. The weighted sum is then passed to activation function.

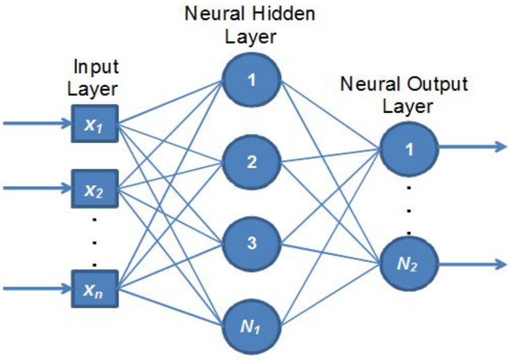

Fig. 2. Architecture of ANN

Fig 2 shows the architecture of ANN in which single input layer which passes signals to hidden layer node. Hidden layer is not accessed through outside of the environment. Hidden layer can be multiple but in our approach single hidden layer is used. The third layer shows the output of the hidden layer. Input pass signals to hidden layer which give result to output layer. The activation function determined the behavior of the function. The overall equation is:

$$Y= \phi(V) = \phi(WX +b) \qquad (2)$$

Equation 2 computes the activation function, the purpose of activation function is to convert an input signal of a specific node in artificial neural network to output signal. The hidden layer can be divided on the basis of complexity of network. The hidden layers are responsible for actual calculations and it cannot access from outside the environment and its functions are hidden. The input layer puts signal to the hidden layers and hidden layers nodes leave through output layer. The training data is used to train the neural network model and the test data used to validate the model. Equation 3 calculates the error from the difference between output and correct output by the following equation:

$$ei= di + Yi \qquad (3)$$

After calculating the error adjust the weights w1, w2, w3. This is done for all training data. The weights are adjusted by the given equation

$$\Delta Wij = l(ERR) \qquad (4)$$

$$Wij =Wij + \Delta Wij \qquad (5)$$

In equation 4 ΔWij is change in weight and l is learning rate which is typically between 0 and 1. Equation 5 shows the weights updating. Error is collected on each training data. Half of the batches are training data and half of the testing data. For activation function sigmoid function is used to training of data. The output of the input and hidden layers signals in for of binary digits which are zero or one where one represents threat and zero for not threat. The two functions and two scripts are running for this training and testing.

The sigmoid function is activation function which is used to train the network and training script to save and test the network performance. The block diagram shows artificial neural network in which the weights are updated according to error generator. Fig 3 shows the error generator, when training the data, error occurred and weights are updated.

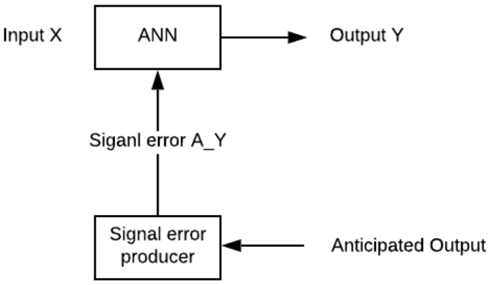

Fig. 3. Block diagram of error adjustment

IV. Experiments and Results

A. Dataset

We have used UNSW-15 and NSL-KDD dataset for training and testing of proposed algorithm. It is static dataset of 49 sample features with class label. It is almost 2.5 million of data instances. It is large enough to train and test the model. It has label class which is target of the data. Make a network with 10 neurons on each node and 1 error probability to input data and target data is select. We train data set for 1000 iterations and it take 10 minutes roughly. We use neural network tool in MATLAB 2019 and 2010a for experiments conduct. The neural network tool gives three type of validation and of testing and training of data.

B. Performance measures

1) Accuracy

Accuracy is a measure of classifier to evaluate the performance. Accuracy is the fraction of predictions our model got right. It is calculated by number of correct predictions from total number of predication.

$$Accuracy = \frac{Number\ of\ Correct\ predictions}{Total\ number\ of\ predictions} \qquad (6)$$

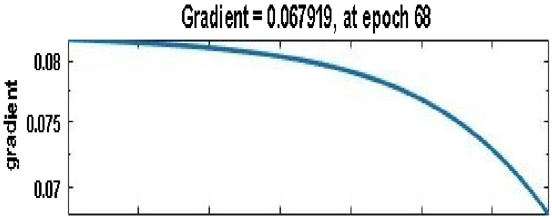

Fig. 4. Gradient of training

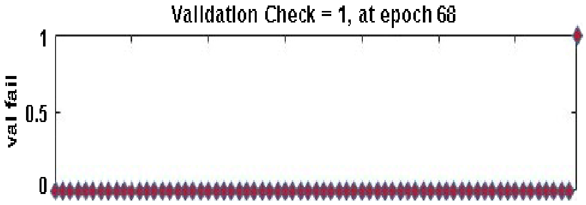

Fig. 5. Validation checks

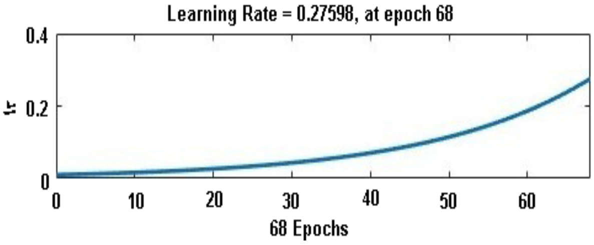

Fig. 6. Learning Rate

Equation 6 describes accuracy is fraction of number of predictions classify as correct in total number of predictions.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \qquad (7)$$

Equation 7 shows the how accuracy for binary classification, Where TP is true positive, TN is true negative, FP false positive, and FN is false negative.

2) Precision

Precision is the number of positive predictions divided by the total number of positive class values predicted.

$$Precision = \frac{TP}{TP+FP} \qquad (8)$$

Precision refers to exactness of model and it tells how many predictions are predicted correct out of correct predictions.

C. Analysis

The graphs in Fig 4-6 shows gradient, validation and learning rate separately. The error probability with 1 at epoch at 68 and leaning rate is 98% which is exactly opposite of gradient performance which is increases with learning decreases. Learning rate is increases with increase in epochs, while gradient decreases. In Fig 7 graph shows the performance of the validation of train data which explain training, testing and validation of dataset. The 39bparameters of IoT is key parameters which shows that the intrusion is highly detect using artificial neural network. The controller detects the malicious packet and discards it. Test line is greater than best line which shows the validity of algorithm.

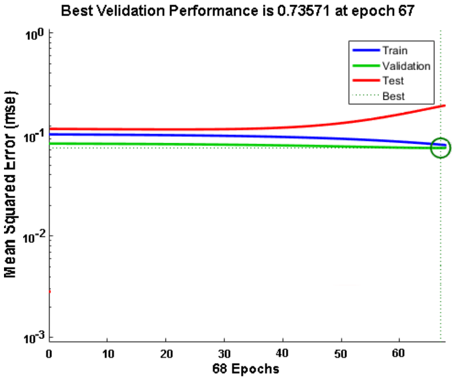

Fig. 7. Best validation Performance

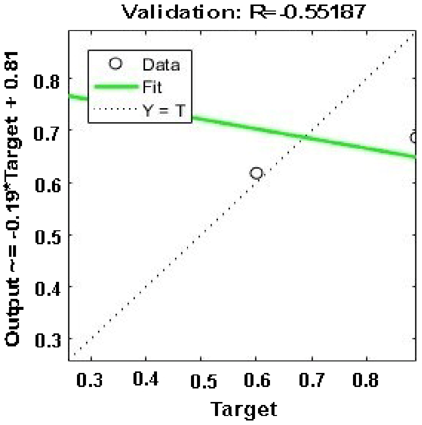

Fig. 8. Performance of training

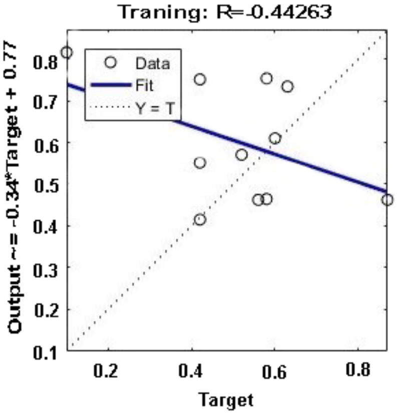

Fig. 9. Performance of validation

Fig 8-11 shows the regression plot of training, validation, testing and overall performance. We compare our approach with intrusion detection system by fuzzy interpolation which is better when data is already known. If the data is too large and unknown then this system does not differentiate between normal traffic and malicious traffic. It considers most of traffic is malicious and its false positive rate is high. But in ANN the large dataset is differentiate between malicious and normal packets. Table 1 shows the comparison between proposed model and intrusion detection system by fuzzy interpolation approach [14], neural network based attack classification [18] and intrusion detection using ANN and fuzzy clustering [17]. All the compared approaches used NSL data sets which are small in size, less number of attacks, less number of networks and have more repetitions as compared to UNSW-15 dataset. Our results are still comparable with above approaches as we used UNSW-15 dataset.

TABLE I. COMPARIOSN

Performance Terms	**Proposed**	**[14]**	**[17]**	**[18]**
Detection Rate	Low false positive	High false positive	Low false positive	Low false positive
Accuracy	84%	74.41%	96.7 %	95.05%
Dataset	UNSW-15	NSL	NSL	NSL
Dataset size	Large	Small	Small	Small
No of Attacks	Large	Small	Small	Small

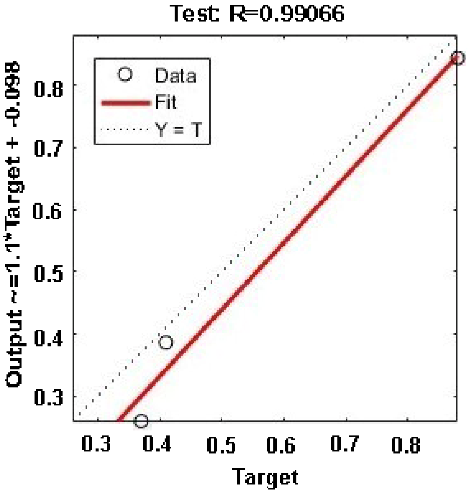

Fig. 10. Performance of testing

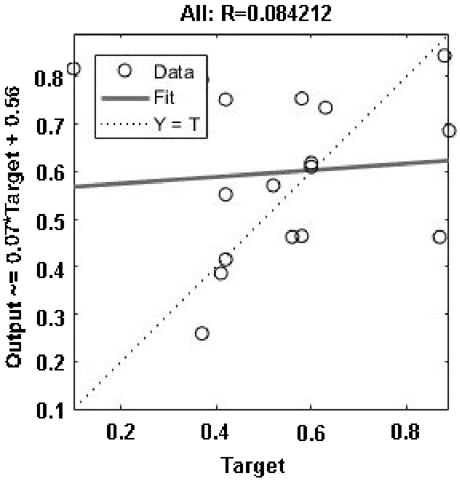

Fig. 11. Overall Performances

V. Conclusion and Future Work

Proposed approach considerably advances the performance of signature-based detection. It is tested upon large dataset which includes benign network data and various types of malicious and heterogeneous data. Proposed approach is implemented in IoT controller, which decides which data is benign and which is malicious. Malicious packet is then discarded considering as a threat timely and efficiently. It achieves an average accuracy of 84% and an average false positive rate of less than 8%. This illustrates that the proposed technique is robust, precise and accurate in large and heterogeneous dataset. In future work, we intent to integrate this approach with real time network traffic.

References

[1] E. Hodo, X. Bellekens, A. Hamilton, P.-L. Dubouilh, E. Iorkyase, C. Tachtatzis, and R. Atkinson, "Threat analysis of IoT networks using artificial neural network intrusion detection system," 2016 International Symposium on Networks, Computers and Communications (ISNCC), 2016.J.

[2] J. Li, Z. Zhao, R. Li, and H. Zhang, "AI-Based Two-Stage Intrusion Detection for Software Defined IoT Networks," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2093–2102, 2019.

[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.

[4] S. Sukode, and S. Gite, "Vehicle Traffic Congestion Control & Monitoring System in IoT," International Journal of Engineering Research, vol 10, pp 19513-19523.

[5] L. Atzori, A. Lera, and G. Morabita, "The internet of things: A survey," Computer Networks., vol. 54, no. 15, pp. 2787–2805, 2010.

[6] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things:Vision, applications and research challenges," Ad Hoc Networks vol. 10, no. 7, pp. 1497–1516, 2012

[7] A. Dunkels, J. Eriksson, and N. Tsiftes, "Low-power interoperability for the IPv6-based Internet of Things," in Proc. 10th Scandinavian Workshop Wireless ADHOC, Stockholm, Sweden, 2011, pp. 10–11.

[8] A. Subasi, K. Al-Marwani, R. Alghamdi, A. Kwairanga, "Intrusion Detection in Smart Grid Using Data Mining Techniques," 21st Saudi Computer Society National Computer Conference (NCC'2018) 10.1109/NCG.2018.8593124.

[9] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac and P. Faruki, "Network Intrusion Detection for IoT Security based on Learning Techniques," in *IEEE Communications Surveys & Tutorials*. doi: 10.1109/COMST.2019.2896380

[10] C. Stylianopoulos, L. Johansson, O. Olsson, and M. Almgren, "CLort: High Throughput and Low Energy Network Intrusion Detection on IoT Devices with Embedded GPUs," 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28-30, 2018, 10.1007/978-3-030-03638-6_12.

[11] A. Saeed, A. Ahmadinia, A. Javed, and H. Larijani, "Intelligent Intrusion Detection in Low-Power IoTs," ACM Transactions on Internet Technology. 16. 1-25. 10.1145/2990499.

[12] M. E. Pamukov and V. K. Poulkov, "Multiple negative selection algorithm: Improving detection error rates in IoT intrusion detection systems," *2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Bucharest, 2017, pp. 543-547

[13] A. Shenfield, D. Day, and A. Ayesh, "Intelligent intrusion detection systems using artificia," Neural networks, ICT Express. 4. 10.1016/j.icte.2018.04.003

[14] L. Yang, J. Li, G. Fehringer, P. Barraclough, G. Sexton and Y. Cao, "Intrusion detection system by fuzzy interpolation," *2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, Naples, 2017,pp.1-6. doi: 10.1109/FUZZ-IEEE.2017.8015710.

[15] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," *2015 Military Communications and Information Systems Conference (MilCIS)*, Canberra, ACT, 2015, pp. 1-6

[16] N. Moustafa and J. Slay, "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set," *2016 Information Security Journal: A Global Perspective,1-14*. 10.1080/19393555.2015.1125974.

[17] G. Wang, J. Hao, J. Ma, and L. Huang, "A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering", *Expert Systems with Applications, 2016* 37. 6225-6232. 10.1016/j.eswa.2010.02.102.

[18] B. Subba, S. Biswas and S. Karmakar, "A Neural Network based system for Intrusion Detection and attack classification," *2016 Twenty Second National Conference on Communication (NCC)*, Guwahati, 2016, pp. 1-6. doi: 10.1109/NCC.2016.7561088.