www.ijecs.in
*International Journal Of Engineering And Computer Science*
*Volume 11 Issue 04April 2022, Page* **No.25527-25531**
*ISSN: 2319-7242 DOI: 10.18535/ijecs/v11i04.4670*

# Network Intrusion Detection by Artificial Immune System and Neural Network

**Raj Kumar Yaduwanshi[1], Prof. Manoraman Malviya[1]**

[1]Rajiv Gandhi Proudyogiki Vishwavidyalaya MP India
Email Address: **rajkumaryaduwanshi01@gmail.com**

**Abstract:** Easy access, simulation of IOT network increases its application and demands in different area. As many of IOT networks are vulnerable in nature and attracts intruders to take advantage of weak security. This paper has developed a model that can detect the IOT network intrusion. In this work feature optimization was done by use of artificial immune system algorithm. AIS reduces the dimension of the dataset by applying affinity check and cloning steps. Selected features were further use for the traiing of neural network. Trained neural network predict the class of IOT network session (Normal / Malicious). Experiment was done on real dataset of IOT session and result shows that rpopsoed model has improved the detection accuracy as compared o existing models.

**Index Terms**- Clustering, Genetic Algorithm, Intrusion Detection, Neural Network.

## Introduction

As a result of the widespread use of information technology in everyday life, concerns about computer network security and privacy are growing around the world, and computer security has become a must. The proliferation of Internet applications and the emergence of current technologies like the Internet of Things (IoT) have been accompanied by new and recent attempts to infiltrate computer networks and systems. The Internet of Things (IoT) is a collection of interconnected gadgets that can communicate without human involvement. Many devices with sensors (such as coffee makers, lighting, bicycles, and many others) can connect to the Internet via IoT [1]. IoT applications are altering how we work and live by saving time and resources. It also offers incalculable benefits and opens up a plethora of possibilities for knowledge exchange, innovation, and growth. Because the Internet is the core and centre of the IoT, any security threat that exists on the Internet exists on the IoT as well. IoT nodes have little capacity and restricted resources, as well as no manual controls, when compared to other traditional networks. Furthermore, the rapid expansion and widespread acceptance of IoT devices in everyday life makes IoT security a major concern, necessitating the development of network-based security solutions. While existing systems are
capable of detecting some types of attacks, detecting others remains difficult.
Faster and more effective techniques of detection of assaults are required as network attacks expand in tandem with the tremendous increase in the amount of information contained in networks [2], and there is little question that more progressive approaches to improve network security are possible. Machine Learning (ML) is one of the most successful computational models in this context for providing embedded intelligence in the IoT environment. Machine learning algorithms have been utilised for network traffic analysis [3],[4],[5], intrusion detection [6], and botnet identification [7].

Machine Learning is the ability of an intelligent device to alter or automate a knowledge-based state or behaviour, and it is a crucial component of an IoT solution. ML algorithms are employed in tasks such as regression and classification, and they have the ability to infer beneficial knowledge from data supplied by devices or humans. ML can also

provide security services in an IoT network. Machine learning's application in threat detection is becoming increasingly popular, with ML being applied in a variety of cybersecurity applications. Although numerous studies have employed machine learning approaches to determine the best ways to detect assaults in the literature, there is a scarcity of research on effective detection methods for IoT contexts. Signature-based (also known as misuse-based) and anomaly-based cyber-analysis are two types of cyber-analysis that can be used to detect attacks. Signature-based techniques are used to detect known attacks by looking for specified traffic characteristics (sometimes called "signatures") in those assaults. One of the benefits of this type of detection technique is that it can successfully detect all known threats while reducing the amount of false alarms.

## II. Related Work

In [8], the authors offer a deep belief network-based intrusion detection model based on a genetic algorithm. For detecting four types of attacks, they employ the NSL-KDD dataset: DoS, R2L, Probe, and U2R. In contrast to our work, their study employs an outdated dataset that is difficult to apply to modern IoT networks and does not include blockchain as an integrated mechanism for monitoring and safeguarding IIoT networks in their solution.

For securing network traffic of Internet of Things applications, [9] proposes an intrusion detection technique based on statistical flow features. To detect fraudulent traffic events, the authors of this paper apply three machine learning techniques: Decision Trees, Naive Bayes, and Artificial Neural Networks (ANN). They use the same UNSWNB15 dataset as us, but they don't utilising blockchain as an integrated mechanism for monitoring and protecting IIoT networks in their system.

In [10], an IoT security architecture based on machine learning is proposed. They created a dataset based on the NSL-KDD dataset and tested their solution in a real-world smart building situation. An old dataset may not be suited for newer IoT networks, as we discussed in earlier related publications. DDoS, Probe, U2R, and R2L assaults are all detected using a single-class SVM (Support Vector Machine) approach. They do not, however, employ blockchain to monitor IIoT networks.

Using a deep-learning system, the authors of [11] created a method for identifying denial-of-service (DoS) assaults. Random Forests, a Multilayer Perceptron, and a Convolutional Neural Network are three techniques they utilise to detect DoS attacks. They use the same dataset as us, but their goal is to detect only one type of attack (DoS), and their system does not include blockchain.

In [12] authors proposes a methodology for detecting and mitigating botnet-based distributed denial of service (DDoS) assaults in IoT networks using a machine learning algorithm. They employ a variety of machine learning methods, including K-Nearest Neighbour (KNN), Naive Bayes, and Multi-layer Perception Artificial Neural Networks (MLP ANN). They use the same dataset as us, but their goal is to detect only one type of attack (DoS), and their system does not include blockchain.

The authors of [13] offer an IoT security analysis model that uses Machine Learning (ML) techniques to identify intrusion and cyber threats traffic. Random Forest, Random Tree, Decision Tree, Naive Bayes, and BayesNet are four machine learning approaches used by the authors in this study to detect harmful traffic events. They use the same dataset as we do, but their solution does not use blockchain.

## Proposed Methodology

This section gives a quick overview of the proposed Immune System-based Network Security (ISIDS). The suggested model is depicted in Figure 1 as a block diagram, with dataset processing, dimension reduction, and training blocks included. This section had distinct headlines for each block's explanation.

### Data Cleaning

This stage cleans data by removing undesirable information from the collection. Input data has a variety of attributes, each with its own significance. For example, the input dataset utilised in this study comprises n fields, and the first few feature values were deleted from the work, such as session ID, connection type, and transferring protocol.

$$CD \leftarrow Dataset\_Cleaning(RD) \text{-------} 1 \text{ eq}$$

The raw dataset matrix is RD in eq. 1, and the clean dataset matrix is CD in eq. 1. The processed data was organised in a row-column matrix, with each row representing a session and the columns representing the session's feature set.

**Optimizing features**

The immune system algorithm was used to further process the input CD matrix, lowering the training vector values and improving learning accuracy.

**Generate Antibodies**

Random set of features were developed by Gaussian function that is a combination of 0 and 1 value. This binary feature set is antibody in the genetic algorithm. This work has two flag for a feature 1 act as presence and 0 act as absent. Further population has lower bound for presence and upper bound for absence of feature. So m number of antibodies A, is a collection represent initial population.

**A←Generate_Antibody(m)**

**Affinity**

Affinity of antibody present in the population were estimate by developing temporary neural neural network as per present features in chromosome. As per trained neural network intrusion detection was done for accuracy estimation. Accuracy value of correct intrusion class detection is affinity of antibody. Training of model is detailed in neural network heading of this section.

**Cloning**

As per affinity value of each antibody in population, best solution $A_b$ is obtained. As per best antibody $A_b$ feature set few status were randomly change. By change in feature status present to absent or absent to present cloning of the model is done.

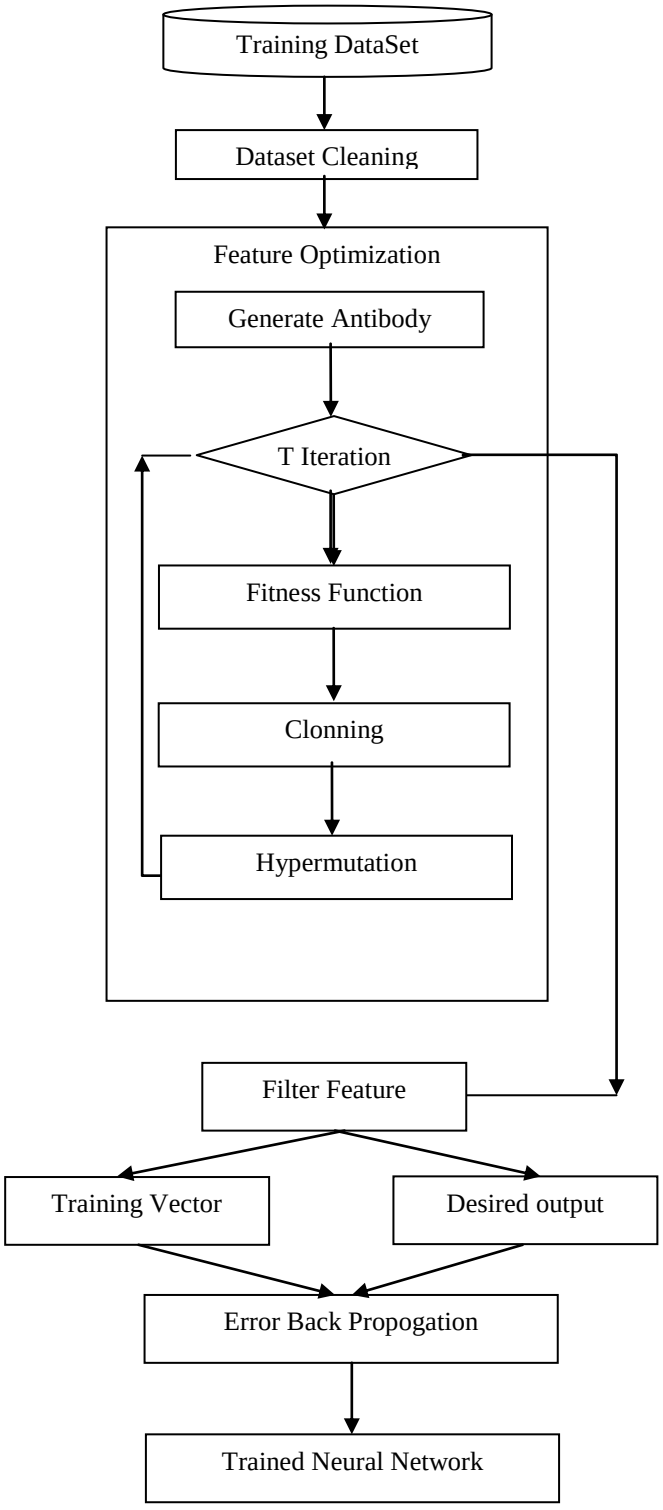


Fig. 1 Block diagram of AIFCMSD.

$A \leftarrow Cloning(A_b, A)$

**Hypermutation**

The clones are then subjected to a hyper mutation procedure, in which they are mutated in inverse

proportion to their affinity, with the best antibody's clones being mutated the least and the poorest antibody's clones being mutated the most. The clones and their original antibodies are then analysed, and the best N antibodies are chosen for the next iteration. It's possible for the mutation to be uniform, Gaussian, or exponential.

$$A \leftarrow \text{Hypermutation}(A)$$

**Filter Feature**

Once iteration get complete then find best immune system antibody from the last updated population. Feature having value one in chromosome consider as selected feature for training vector and other consider as unselected. Desired output matrix was also prepared in this section.

**Training of Neural Network**

Neural network consider takes input traing vector and desired output during training. For each set of training vector neuron weight value adjust for e number of epochs. Tained neural network was directly used for predicting the session class as attack or normal.

## EXPERIMENT AND RESULTS

Experimental setup: MFOCMSD and comparing model was developed on MATLAB software. Experimental machine having 4 GB ram, i3 6$^{th}$ generation processor. IO dataset was taken from [14]. Comparison of **AISIDS** was done with cloud malicious session detection model proposed in [15].

**Evaluation Parameter**

To test our results, this work usesthe following measures Precision, Recall, and F-score. These parameters are dependent on the TP (True Positive), TN True Negative), FP (False Positive), and FN (False Negative).

**Results**

**Table 1. Precison based IDS models comparison.**

| IOT Dataset Sessions | Previous work [15] | AISIDS |
|---|---|---|
| 4000 | 0.84936 | 0.959261 |
| 8000 | 0.847291 | 0.962937 |
| 12000 | 0.846565 | 0.964628 |
| 16000 | 0.845466 | 0.965189 |
| 20000 | 0.844679 | 0.964279 |

Table 1 shows precision values of IOT network intrusion detection at different dataset sizes. It was obtained that porposed modle has increases the detection precision value by 12.1% as compared to previous model proposed in [15]. Use of artificial immune genetic algororithm for intrusion detection has improved the training dataset.

**Table 2. Recall based IDS models comparison.**

| IOT Dataset Sessions | Previous work [15] | AISIDS |
|---|---|---|
| 4000 | 0.931913 | 0.984922 |
| 8000 | 0.932851 | 0.983941 |
| 12000 | 0.932791 | 0.98428 |
| 16000 | 0.933879 | 0.984525 |
| 20000 | 0.932294 | 0.983219 |

Table 2 shows that proposed artificial immune genetic algorithm has enhanced the recall values of intrusion detection as compared to previous model. Neural network has increases the work efficiency of correct class prediction.

**Table 3. F-Measure based IDS models comparison.**

| IOT Dataset Sessions | Previous work [15] | AISIDS |
|---|---|---|
| 4000 | 0.888724 | 0.971922 |
| 8000 | 0.888015 | 0.973325 |
| 12000 | 0.887589 | 0.974355 |
| 16000 | 0.887476 | 0.974761 |
| 20000 | 0.886327 | 0.973657 |

Table 3 shows inverse average of the precision and recall values. It was shown in table that proposed f-measure values was enhaced in artificial immune system and genetic algorithm. Feature reduction reduces the confusion of the data while training and improve decision catching of the model.

**Table 4. Accuracy based IDS models comparison.**

| IOT Dataset | Previous work | AISIDS |
|---|---|---|

| Sessions | [15] | |
|---|---|---|
| 4000 | 0.887778 | 0.970757 |
| 8000 | 0.886139 | 0.971879 |
| 12000 | 0.886343 | 0.973086 |
| 16000 | 0.88607 | 0.973439 |
| 20000 | 0.884156 | 0.972101 |

Accuracy value of correct class detection is shown in Table 5. It was obtained that proposed model has increases the work efficiency of true alarm generation with les number of features.

**Conclusion**

IOT network increases the use of electronic devices and provide support for various industries. Many of intrusders are taking advantages of weak security. This paper has proposed a model that detects the malicious session in the network and generate alarm for that. Proposed model uses artificial immune system genetic algorithm for feature reduction and train the neural network for detection. Experiment was done on real dataset obtained from [14]. Result shows that preciosn value was enhaced by 12.1% and accuracy of the model was enhanced by 8.86% as compared to existing models.In future scholar can train other machine learning models for getting better results.

**References:**


**[1]** J. Deogirikar and A. Vidhate, "Security attacks in iot: A survey," International Conference on I-SMAC (I-SMAC), pp. 32–37, 2017.

**[2]** T. Bodstrom and T. H ¨ am¨ al¨ ainen, "State of the art literature review ¨ on network anomaly detection with deep learning," Internet of Things, Smart Spaces, and Next Generation Networks and Systems, pp. 64–76, 2018.

**[3]** I. Arnaldo, A. Cuesta-Infante, A. Arun, M. Lam, C. Bassias, and K. Veeramachaneni, "Learning representations for log data in cybersecurity," International Conference on Cyber Security Cryptography and Machine Learning, pp. 250–268, 2017.

**[4]** M. Du, F. Li, G. Zheng, and V. Srikumar, "Deeplog: Anomaly detection and diagnosis from system logs through deep learning," Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1285–1298, 2017.

**[5]** B. J. Radford, B. D. Richardson, and S. E. Davis, "Sequence aggregation rules for anomaly detection in computer network traffic," arXiv preprint arXiv:1805.03735, 2018.

**[6]** I. Lambert and M. Glenn, "Security analytics: Using deep learning to detect cyber attacks," 2017.

**[7]** M. Stevanovic and J. M. Pedersen, "Detecting bots using multi-level traffic analysis." IJCSA, vol. 1, no. 1, pp. 182–209, 2016.

**[8]** Zhang, Y.; Li, P.; Wang, X. Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network. IEEE Access 2019, 7, 31711–31722.

**[9]** Moustafa, N.; Turnbull, B.; Choo, K.R. An Ensemble Intrusion Detection Technique based on proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things. IEEE Internet Things J. 2018, 6, 4815–4830.

**[10]** Bagaa, M.; Taleb, T.; Bernal, J.; Skarmeta, A. A machine learning Security Framework for Iot Systems. IEEE Access 2020, 8, 114066–114077.

**[11]** Susilo, B.; Sari, R. Intrusion Detection in IoT Networks Using Deep Learning Algorithm. Information 2020, 11, 279.

**[12]** Pokhrel, S.; Abbas, R.; Aryal, B. IoT Security: Botnet detection in IoT using Machine learning. arXiv 2021, arXiv:2104.02231.

**[13]** 21. Shafiq, M.; Tian, Z.; Sun, Y.; Du, X.; Guizani, M. Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city. Future Gener. Comput. Syst. 2020, 107, 433–442.

**[14]** Ullah I., Mahmoud Q.H. (2020) A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks. In: Goutte C., Zhu X. (eds) Advances in Artificial Intelligence. Canadian AI 2020.

**[15]** A. Fatani, M. Abd Elaziz, A. Dahou, M. A. A. Al-Qaness and S. Lu, "IoT Intrusion Detection System Using Deep Learning

and Enhanced Transient Search Optimization," in IEEE Access, vol. 9.