# Iot Network Intrusion Alarming System Using Bat Algorithm & Neural Network

Diwakar Kumar Chaudhary[1], Prof. Pritaj Yadav[1],
Mrs. Kanchan Jha[2]

[1]Computer Science and Engineering, Ravindranath Tagore University, Bhopal, India.
[2]School of Advance Computing, Sanjeev Agrawal Educational Global University, Bhopal, India.

Abstract

The scope of IoT networks has expanded drastically in the modern digital environment. Connectivity along with use of the internet, particularly in the form of data collection and exchange, is a primary characteristic of devices in an IoT network. This paper has developed a (Bat IOT Network Intrusion Detection System (BINIDS) that alarms for the intrusion in the IOT network. Paper has work on the input dataset for improving the learning of neural network. Dataset optimization was done by BAT algorithm. Input features were cluster into two category selected and rejected. All selected features were processed to train the neural network. Experiment was done on real IOT dataset under different testing size. Result shows that proposed model has improved the work performance.

Keywords Deep Learning, Intrusion Detection, Feature Optimization, Genetic Algorithm, Soft Computing.

## I. INTRODUCTION

The Internet of Things (IoT) is an emerging technology that has been actively utilized during the past several years. It facilitates communications and interactions among multiple devices through a network, which in turn is driving innovative business process technologies [1]. As a result, the exponential expansion of cybersecurity threats has brought to light a number of difficulties across a wide range of domains, including financial, credibility proof, enforcement, and commercial operations [2]. As a paradigm for providing a variety of resources and services to the consumer on-demand, cloud computing is frequently employed as IoT data storage. The amount of interaction required between customers

and service providers is often low in the cloud computing model [3]. Its outstanding features have garnered significant interest from businesses and individual users alike. However, several obstacles, including those involving the platform's operating mechanism and security, may be encountered throughout the transition to cloud computing. The risk of cloud computing stems from the fact that sensitive information is kept on distant computers. Because of its vulnerability to hackers and invaders, the cloud computing platform is not universally favored or used. The current rise in cyberattacks can be attributed to a number of factors. The availability of simple hacking tools makes it possible for even inexperienced hackers to launch an assault against cloud storage in a short amount of time [4-5].

In addition, there are two types of security attacks: active and passive [6]. At some point in the game's execution, an actual assault occurs. It poses a threat to the hardware and may even break it. Active assaults are more challenging to both execute and detect than their passive counterparts. Most current attacks take the form of a Denial of Service [7]. Active attacks also include spoofing and message alteration as well as packet replay [8]. In a passive attack, the attacker just keeps tabs on their target's data. The information is unaltered while the attackers stay hidden and the communication channel is kept open for intelligence gathering. Network mapping and traffic analysis for eavesdropping are the most popular forms of attack [9]. A real-time network Anomaly-based intrusion detection system is required to stop attackers and mitigate the impact of these assaults on IoT devices and the user.

Rest of paper was organized into four more section. Next section brief the intrusion detection models proposed by other researchers. After this third section brief proposed model BINIDS (Bat IOT Network Intrusion Detection System). Fourth section of paper shows the experimental values of the proposed model on different evaluation parameters. Finally paper concluded with various findings and future work.

## II. Related Work

Using a Dense Random Neural Network (DnRaNN), Latif et al. [10] suggested a unique lightweight approach for IoT network intrusion detection. The authors ran extensive trials on the ToN IoT dataset, including both binary and multi-class classification situations, to assess their technique.

For highly accurate intrusion detection in Smart Home networks, Azumah et al. [11] propose using LSTMs. In [40], LSTM is utilized for the same purpose in Fog computing.

In [12], the authors analyze and evaluate contemporary methods that make use of different types of data. For intrusion detection in ICS, a hybrid deep learning approach is deployed. Normal and abnormal network traffic are distinguished by LSTM and CNN models.

Particle swarm optimization (PSO)-based gradient descent (PSO-LightGBM) was suggested for intrusion detection in [13]. One-class support vector machines (OCSVM) are fed data extracted with PSO-LightGBM, looking for indicators of malicious intent. The intrusion detection model is tested using the UNSW-NB15 dataset.

By comparing characteristics from the UNSWNB15 and Bot-IoT data-sets based on flow and Transmission Control Protocol (TCP), we were able to generate a data-set of packets from IoT traffic for use in [14]'s proposed Protocol Based Deep Intrusion Detection (PB-DID) architecture. We solve issues like unbalanced and over-fitting to properly categorize normal, DoS, and DDoS traffic.

In [15], the authors investigate identification and discriminative deep learning methods for detecting malware used in cyberattacks. The study did a nice job of summarizing the seven techniques, which included three types of deep learning (RNN, CNN, and DNN) and four types of generative models/methods (RBN, DBN, DBM., and DA). This study also pays special attention to the reliability and availability of research-related dictionaries. This study's experiments show that IDS and Cybersecurity threats may be detected in a collaborative technological setting.
In [16], the authors create a model for IIoT security intrusion detection using feature engineering and machine learning. To cut down on computational cost and prediction time, we integrate Isolation Forest (IF) with Pearson's Correlation Coefficient (PCC). IF is used to find and eliminate anomalies in data sets. To choose the best characteristics, we use the PCC algorithm. In both cases (PCCIF and IFPCC), PCC and IF can be used interchangeably. Improved IDS functionality is achieved by the use of the Random Forest (RF) classifier.

To implement the level-aware black-box adversarial attack strategy against the graph neural network (GNN)-based intrusion detection

in IoT systems on a shoestring budget, the authors of [17] offer a unique hierarchical adversarial attack (HAA) generating approach. An intelligent method using a saliency map approach is built into a shadow GNN model to produce adversarial instances by pinpointing and tweaking the most important parts of the model. Based on their structural properties and the overall loss changes within the targeted IoT network, a group of more susceptible nodes with high attack priority are selected using a hierarchical node selection method based on random walk with restart (RWR). The suggested HAA generating technique is compared to three reference methods using the publicly available data set UNSW-SOSR2019.

## III. PROPOSED METHODOLOGY

THIS SECTION BRIEF THE PROPOSED MODEL BINIDS (BAT IOT NETWORK INTRUSION DETECTION SYSTEM) METHODOLOGY. FIG. 1 SHOWS THE FLOW OF THE TRAINING MODEL WHERE EACH BLOCK WAS DETAILED. FURTHER FIG. 2 SHOWS THE BLOCK DIAGRAM OF TESTING OF TRAINED MODEL. TABLE 1 LIST THE VARIOUS NOTATION OF THE WORK.

**Table 1. BINIDS notation table.**

| Notations | Meaning |
|---|---|
| RID | Raw IOT Dataset |
| PID | Processed IOT Dataset |
| BP | BAT Population |
| b | Number of BATs in BP |
| m | Number of Feature in PID |
| $B_f$ | BAT Fitness |
| $B_b$ | Best Fit BAT |
| FBF | Filter BAT Features |
| Do | Desired Output |
| IDTNN | Intrusion detection trained neural network |

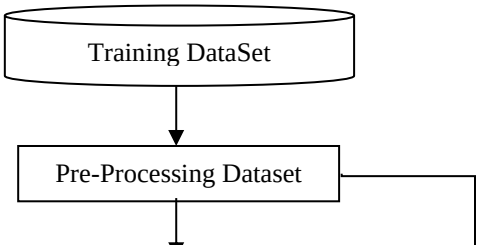
### Pre-Processing of IOT Dataset

IOT network session dataset has feature values and text collection. Some of those features are repetitive or constant in whole dataset. Hence those set of features were removed as a cleaning step of the algorithm. So if RID is raw IOT dataset and PID processed dataset.

PID←IOTDatasetCleaning(RID)------Eq. 1

Further processed dataset is normalize as few of feature values were in range of 0 to 1000 and some of them in 0 to 1. So all were transformed into 0 to 1 scale by taking the ratio with other.

PID←Normalization(PND)----------Eq. 2



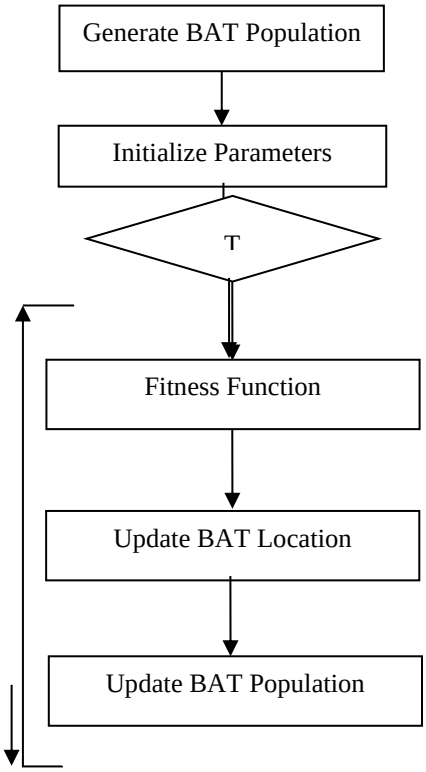



**Fig. 1 Flow diagram of BINIDS proposed model.**

**BAT Algorithm Optimization**

PND dataset was processed further for the optimization of training dataset by BAT Algorithm. As BAT finds the path to the prey with help of sound vibration and sensing organs. This paper has implement BAT for getting the good set of training feature that impacts the decision.

**Generate BAT Population**

In this step a set of BAT were artificially generate by Gaussian position function. Each BAT is a set of feature position having binary value where 1 means taken in the training vector and 0 means feature is not involve in training. As genetic algorithm works dynamically hence feature position is generate by Gaussian function. So let dataset have m number of features in PID matrix and b number of BATs were generate, then BAT population BP is a matrix of bxm.

BP←GenerateBAT(b, m)----------Eq. 3

**Initialize Parameters**

BAT work on voice / sound vibration to select path that give a perception of any path. So a sound with loudness l is generate BAT have a ulse rates r. Further BAT set its frequency range between $F_{min}$ and $F_{max}$. So each BAT have few initial parameters (l, r, $F_{min}$ and $F_{max}$).

**BAT Fitness Function**

Each BAT were rank as per distance. So evaluation of distance done by fitness value. BAT feature vector pass into the neural network for training and intrusion detection accuracy of the work. This detection accuracy value is fitness of the BAT in the population.

$B_f$←Fitness(BP, PID) ----------Eq. 3

**Update BAT Location**

Once F value obtain by fitness function then sort f in deseeding order and find best BAT out of all chromosomes available in the population.

```
bfreq(i,1)=fmin+(fmax-bfreq(i,1))*beta;

 bv(i,1)=bv(i,1)+(bpos(i,1)-agg_obj(i,1))*bfreq(i,1);

agg_obj(i,1) = w1*sum(Moth_pos(i,1))+w2*(100-fitness(i,1)*100)+w3*fitness(i,1)*100;

    bpos(i,1)=bpos(i,1)+bv(i,1);
```

chg = floor(bfreq(i,1));

Genetic algorithm success depends on change of chromosomes, hence as per changing parameter X, number of random position value of BATs were modified. This operation was not done in best local BAT [19]. In this step each BAT X number of positions were modified randomly from zero to one or one to zero as per best three local BAT feature sets.

**Update BAT Population**

These BAT were further test for fitness value with parent BAT if child BAT has better values then remove parent otherwise parent will continue. After this step if maximum ieration steps occur then jump to filter feature block otherwise evaluate fitness value of each BAT BAT.

**Filter Feature**

Once iteration get complete then find best BAT from the last updated population. Feature having value one in chromosome consider as selected feature for training vector and other consider as unselected.

**FBF←FilterFeatures(PID, $B_b$)**

**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. IDTNN Intrusion detection trained neural network was directly used for predicting the session class as attack or normal.

IDTNN ← Train(FBF, Do)

**Proposed BINIDS Algorithm**

Input: RID

Output IDTNN

1. PID←IOTDatasetCleaning(RID)
2. PID←Normalization(PND)
3. BP←GenerateBAT(b, m)
4. Initialize parameters (l, r, $F_{min}$ and $F_{max}$)
5. Loop 1:itr
6. $B_f$←Fitness(BP, PID)
7. SP←UPDATE_BAT(SP)
8. EndLoop
9. $B_f$←Fitness(BP, PID)

10. Best←max($B_f$)
11. TV←Training_Vector($B_f$, PID)
12. DO←Desired_Output(PID)
13. EndLoop
14. IDTNN ← Train(FBF, Do)

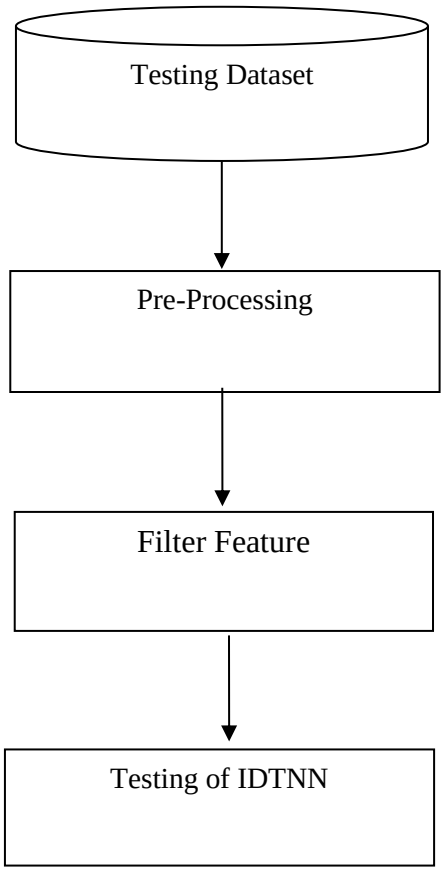



Fig. 2 Testing of BININDS model.

**Testing of BINIDS Model**

In order to test IDTNN model testing dataset takes IOT dataset as input. Pre-processing steps are same as done in training phase. Further in this phase no need to run BAT algorithm, just filter selected feature as per BAT cluster centers obtained while training session. Finally pass the selected feature in trained IDTNN model.

## IV. EXPERIMENT AND RESULTS

Experimental setup: BINIDS and comparing model was developed on MATLAB software. Experimental machine having 4 GB ram, i3 6$^{th}$ generation processor. Comparison of **BINIDS** was done with previous IOT malicious session detection model proposed in [18]. : IOT dataset was taken from [19]. This dataset has 86 attributes, where three is the class of session and rest 83 is to training/testing

features. Total number of sessions are 625784, with two and multiclass named sessions.

**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). Obtaining values can be put in the mention parameter formula to get results.

$$\text{Precision} = \frac{\text{True\_Positive}}{\text{True\_Positive} + \text{False\_Positive}}$$

$$\text{Recall} = \frac{\text{True\_Positive}}{\text{True\_Positive} + \text{False\_Negative}}$$

$$F\_Score = \frac{2 * \text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}}$$

$$Accuracy = \frac{Correct\_Classification}{Correct\_Classification + Incorrect\_Classification}$$

**Results**

**Table 2. Precision value based comparison of network intrusion detection models.**

| Dataset Size | Previous Work | BINIDS |
|---|---|---|
| **5000** | 0.923 | 0.9858 |
| **10000** | 0.9984 | 0.9861 |
| **15000** | 1 | 0.9865 |
| **20000** | 0.9236 | 0.9894 |
| **25000** | 0.8365 | 0.9846 |

Table 2 shows that proposed BINIDS model has improved the true alarm detection with high precision value. Further it was found that BAT algorithm based feature selection for the training of neural network has improved the work. Use of single population update model increases the precision value by 0.508%, as compared to previous model proposed in [18].

**Table 3. Recall value based comparison of network intrusion detection models.**

| Dataset Size | Previsous Work | BINIDS |
|---|---|---|
| **5000** | 0.799 | 0.9761 |
| **10000** | 0.9346 | 0.9756 |
| **15000** | 0.942 | 0.9906 |
| **20000** | 0.7633 | 0.9942 |
| **25000** | 0.8654 | 0.9718 |

Recall value of intrusion detection models were list in the table and it was found that proposed BINIDS has increases the recall value by 12.3% as compared to [18]. This enhancement was done by the proposer training of neural network.

**Table 4. F-Measure value based comparison of network intrusion detection models.**

| Dataset Size | Previous Work | BINIDS |
|---|---|---|
| **5000** | 0.8568 | 0.9809 |
| **10000** | 0.9655 | 0.9808 |
| **15000** | 0.97 | 0.9885 |
| **20000** | 0.8359 | 0.9918 |
| **25000** | 0.8507 | 0.9781 |

Table 3 shows that f-measure value of the comparing models and it was found that use of BAT algorithm for the training dataset feature optimization has improved the work performance. Table 3 shows that increase of testing dataset has not make a high difference in the f-measure values.

**Table 5. Accuracy value based comparison of network intrusion detection models.**

| Dataset Size | Previous Work | BINIDS |
|---|---|---|
| **5000** | 0.8953 | 0.9767 |
| **10000** | 0.9538 | 0.988 |
| **15000** | 0.9733 | 0.9876 |
| **20000** | 0.8966 | 0.9892 |
| **25000** | 0.9162 | 0.9692 |

Table 5 shows that accuracy of normal class detection of proposed BINIDS is high as compared to previous existing models. Use of genetic algorithm for training feature optimization has increases the work performance by 5.61%.

**Table 6. Accuracy of Normal intrusion class detection models.**

| Dataset Size | Previous Work | BINIDS |
|---|---|---|
| **5000** | 95.7067 | 98.5799 |
| **10000** | 99.676 | 98.6066 |
| **15000** | 100 | 98.652 |
| **20000** | 96.6758 | 98.9378 |
| **25000** | 93.553 | 98.4571 |

**Table 7. Accuracy of DOS intrusion class detection models.**

| Dataset Size | Previsous Work | BINIDS |
|---|---|---|
| **6000** | 99 | 100 |
| **8000** | 99.8775 | 100 |
| **12000** | 100 | 100 |
| **14000** | 98.4483 | 100 |
| **16000** | 97.06 | 100 |

**Table 8. Accuracy of Probe intrusion class detection models.**

| Dataset Size | Previous Work | BINIDS |
|---|---|---|
| **5000** | 33.0078 | 90.625 |
| **10000** | 32.696 | 90.8222 |
| **15000** | 41.8738 | 90.8222 |
| **20000** | 29.2543 | 90.8222 |
| **25000** | 27.533 | 85.4985 |

**Table 9** Accuracy of R2L intrusion class detection models.

| Dataset Size | Previous Work | BINIDS |
|---|---|---|
| **5000** | 98.2866 | 98.1308 |
| **10000** | 99.519 | 99.5194 |
| **15000** | 98.5595 | 99.5194 |
| **20000** | 98.3192 | 99.5194 |
| **25000** | 99.319 | 98.1132 |

**Table 10** Accuracy of U2R intrusion class detection models.

| Dataset Size | Previsous Work | BINIDS |
|---|---|---|
| **5000** | 93.6782 | 51.2739 |
| **10000** | 94.0267 | 50.0766 |
| **15000** | 94.0267 | 50.0766 |
| **20000** | 14.968 | 50.0766 |
| **25000** | 67.3226 | 50.0766 |

Class detection accuracy for intrusion detection models is compared across test dataset sizes in Tables 6, 7, 8, 9, and 10. When compared to conventional approaches, the proposed BINIDS model was shown to improve DOS detection accuracy by 1.12%. R2L also saw growth, rising by 0.1615% percent.

## IV. Conclusion

IOT network are quick to start network need low cost to setup. This feasibility of communication attract many people to work on IOT infrastructure. So attacks are possible in the network as no hard protecting layers were installed. This paper has resolved the work network attack issue, by alarming suspicious activity. BAT algorithm was used in the proposed BINIDS model for identifying the features of the dataset that increases the accuracy of true alarm. For learning model uses neural network. Experiment was done on IOT network dataset and result shows that propose model use of single population update model increases the precision value by 0.508%. Further BINIDS model improves DOS detection accuracy by 1.12%. R2L also saw growth, rising by 0.1615% percent. In future scholars can apply same technique in other dataset.

## References

1. Lee, “The internet of things for enterprises: an ecosystem, architecture, and iot service business model,” Internet of Things, vol. 7, Article ID 100078, 2019.

2. Lee, “Internet of things (iot) cybersecurity: literature review and iot cyber risk management,” Future Internet, vol. 12, no. 9, p. 157, 2020.

3. G. S. Kushwah and V. Ranga, “Voting extreme learning machine based distributed denial of service attack detection in cloud computing,” Journal of Information Security and Applications, vol. 53, Article ID 102532, 2020.

4. P. Louvieris, N. Clewley, and X. Liu, “Effects-based feature identification for network intrusion detection,” Neurocomputing, vol. 121, pp. 265–273, 2013.

5. J. Man and G. Sun, “A residual learning-based network intrusion detection system,” Security and Communication Networks, vol. 2021, Article ID 5593435, 9 pages, 2021.

6. Jhaveri Rutvij H, Patel Sankita J, Jinwala Devesh C. “DoS attacks in mobile ad hoc networks: A survey.” 2012 second international conference on advanced computing & communication technologies. IEEE, 2012.

7. Goyal Priyanka, Batra Sahil, Singh Ajit. A literature review of security attack in mobile ad-hoc networks. Int J Comput Appl. 2010;9(12):11–5.

8. Keerthika M, Shanmugapriya D. Wireless sensor networks: Active and passive attacks-vulnerabilities and countermeasures. Global Trans Proc. 2021;2(2):362–7.

9. Keerthika M, Shanmugapriya D. Wireless sensor networks: Active and passive attacks-vulnerabilities and countermeasures. Global Trans Proc. 2021;2(2):362–7.

10. S. Latif, Z. e. Huma, S. S. Jamal, F. Ahmed, J. Ahmad, A. Zahid, K. Dashtipour, M. Umar Aftab, M. Ahmad, Q. H. Abbasi, Intrusion Detection Framework for the Internet of Things using a Dense Random Neural Network, IEEE Transactions on Industrial Informatics (2021).

11. S. W. Azumah, N. Elsayed, V. Adewopo, Z. S. Zaghloul, C. Li, A Deep LSTM based Approach for Intrusion Detection IoT Devices Network in Smart Home, in: 7th IEEE World Forum on Internet of Things, WF-IoT 2021, 2021, pp. 836–841.

12. Diro, N. Chilamkurti, Leveraging LSTM Networks for Attack Detection in Fog-to-Things Communications, IEEE Communications Magazine 56 (9) (2018) 124–130.

13. Kachhwaha, R. ., Vyas, A. P. ., Bhadada, R. ., & Kachhwaha, R. . (2023). SDAV 1.0: A Low-Cost sEMG Data Acquisition & Processing System For Rehabilitatio. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2), 48–56.

14. J. Liu, D. Yang, M. Lian and M. Li, "Research on Intrusion Detection Based on Particle Swarm Optimization in IoT," in IEEE Access, vol. 9, pp. 38254-38268, 2021.

15. M. Zeeshan et al., "Protocol-Based Deep Intrusion Detection for DoS and DDoS Attacks Using UNSW-NB15 and Bot-IoT Data-Sets," in IEEE Access, vol. 10, pp. 2269-2283, 2022.

16. I. A. Kandhro et al., "Detection of Real-Time Malicious Intrusions and Attacks in IoT Empowered Cybersecurity Infrastructures," in IEEE Access, vol. 11, pp. 9136-9148, 2023.

17. M. Mohy-Eddine, A. Guezzaz, S. Benkirane, M. Azrour and Y. Farhaoui, "An Ensemble Learning Based Intrusion Detection Model for

Industrial IoT Security," in Big Data Mining and Analytics, vol. 6, no. 3, pp. 273-287, September 2023.

18. 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, pp. 123448-123464, 2021, doi: 10.1109/ACCESS.2021.3109081.

19. 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.