A Novel Glowworm Swarm Optimization Driven Gated Recurrent Unit Enabled Botnet Detection in IIoT Environment

Tarek Gaber[1], Joseph Bamidele Awotunde[2,*], Chin-Shiuh Shieh[3]

[1] School of Science, Engineering and Environment, University of Salford, UK

[2] Department of Computer Science, University of Ilorin, Ilorin, 240003, Nigeria

[3] Department of Electronic Engineering, National Kaohsiung University of Science and Technology, Taiwan

Emails: tmgaber@gmail.com ; awotunde.jb@unilorin.edu.ng ; csshieh@nkust.edu.tw

Abstract

Accurate and prompt detection of security attacks in the Industrial Internet of Things (IIoT) is important to reduce security risks. Since a massive number of IoT devices are placed over the globe and the quantity gets increased, an effective security solution is necessary. A botnet is a computer network comprising numerous hosts executing on standalone software. In this view, this article develops a novel Glowworm Swarm Optimization Driven Gated Recurrent Unit Enabled Botnet Detection (GSOGRU-BD) model in IIoT Environment. The presented GSOGRU-BD model intends to effectually identify the presence of botnet attacks in the IIoT environment. To do so, the GSOGRU-BD model initially pre-processed the input data to get rid of missing values. In addition, the GSOGRU-BD model involves the GRU model for the effective recognition and classification of botnets. Besides, the GSO algorithm is used for optimal hyperparameter tuning of the GRU model. Comparative experimental validation of the GSOGRU-BD model is tested using a benchmark dataset and the results reported the better outcomes for the GSOGRU-BD model.

Keywords: Botnet detection, Industrial IoT, Security, Attack detection, Machine learning, Deep learning

1. Introduction

Internet of Things (IoT) upgrades customary reasoning of the past and permits association of many, while perhaps not all, objects in the climate to the network. It can interface vehicles, domestic devices, and other electronic gadgets together on the network, which, thusly, brings people a more smart life [1]. The framework acknowledges continuous distinguishing proof, area, following, and observing, and it triggers relating occasions naturally. Moreover, IoT is the pivotal part in the Industrial IoT (IIoT) that intends to create insightful assembling products and lay out shrewd processing plants with tight associations among clients and colleagues [2]. The IoT is encountering dramatic development and getting a great deal of consideration in scholarly regions and industry, however the protection dangers and security weaknesses are arising out of the absence of essential security innovation [3]. A botnet is a PC network comprising of a few hosts running independent programming. A bot in such a network is simply the PC with malware that permits an attacker to play out specific activities utilizing the assets of a contaminated PC. A botnet runs a bot on a few machines connected to the web to frame a botnet worked by a vindictive gathering [4]. Botnets represent a critical danger to network security as they are generally utilized for some Internet wrongdoings like Distributed Denial-of-Service (DDoS) attacks, fraud, email spam, and snap

DOI: https://doi.org/10.54216/JISIoT.060103
Received: October 21, 2021 Accepted: January 15, 2022

misrepresentation. Botnet-based DDoS attacks are wrecking for the objective network as they will deplete all network data transmission and casualty PC assets and cause an interference of administrations. AI strategies are currently normally used to follow these attacks in IoT [5].

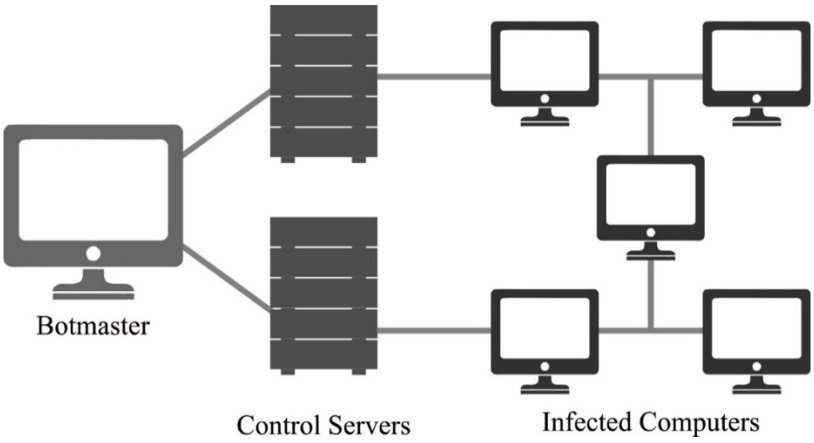

Fig. 1. Botnet Structure

The botnet can be told in designated, appropriated forswearing of administration attacks on any framework on the Internet to consume assets (for instance, transfer speed capacity) of the framework so that it can't as expected serve their authentic clients [6]. The structure of botnet is given in Fig. 1. These days, for all intents and purposes all DDoS attacks are completed from a botnet stage. Notwithstanding its effortlessness, the DDoS attack procedure is extremely successful because of the size of the botnet and the absolute transfer speed of the bots. Presently, computerized reasoning (AI) calculations are utilized to distinguish IoT attacks with more guaranteed recognition. Man-made reasoning innovation even can recognize differences in channels and techniques for attacks. This was one of the difficulties looked by security answers for managing IoT attacks: programmers roll out little improvements in past attacks that security arrangements can't recognize. Engineers and scientists use AI innovations for forestalling any dangers to the IoT climate by investigating network traffic [7]. Profound learning and AI have been incorporated into security frameworks to distinguish such attacks productively. Profound learning is one of the man-made reasoning advances that are available in some genuine applications to deal with complex nonlinear information. Profound intermittent brain network (DRNN) has been executed to recognize botnet attacks from IoT gadgets [8].

Various scientists have zeroed in on creating productive systems to identify botnet attacks and safeguard the IoT climate. In any case, botnet attacks address a large portion of the DDoS attacks that contaminate IoT gadgets. The interruption recognition framework is a strong instrument that is utilized to safeguard network frameworks against any pernicious exercises [9]. The proposed framework can assist with recognizing new attack grouping by coordinating with signature attacks. Interruption identification has two primary strategies, peculiarity based discovery and mark based recognition that recognize attacks by extricating obscure examples from network datasets [10].

The researcher in [11] present a Local-Global best Bat approach for Neural Network (LGBA-NN) to choose feature subset and hyperparameter for effectual recognition of botnet attack, contingent from 9 profitable IoT device infested by two botnets: Mirai and Gafgyt. The presented approach adapted the local-global optimal-based inertia weight to upgrade the bat velocity in the swarm. To address the swarm variety of BA, we projected Gaussian distribution utilized in the initialized population.

The researcher in [12] integrates fog/edge computing and federated learning (FL) to contest malevolent code. The method training a global better method depends on dispersed dataset of collaborator when eliminating the information and transmission constraint. The FL-based recognition method increases the value of dispersed information instance, resultant in a precise method. The researcher in [13] presented a multi-stage DDoS mitigation architecture (MLDMF) to protect against DDoS attack for IIoT that comprises the cloud computing level, edge computing level, fog computing level and. Software determined network is utilized for managing a massive amount of IIoT gadgets and to alleviate DDoS attack in IIoT. The authors in [14] presented a botnet recognition method has been explored by examining

DOI: https://doi.org/10.54216/JISIoT.060103
Received: October 21, 2021 Accepted: January 15, 2022

honeypot with ML to categorize botnet attack. A mimic intelligent factory method has been generated on IoT hardware system.

In [21], the authors suggested hybrid technique on 8330 executable samples, including 5531 IoT botnet samples and 2799 IoT benign samples, to determine its efficacy and superiority. The proposed model tests to be able to detect and categorize IoT botnets with an accuracy of 98.1 percent and 91.99 percent, respectively. The experimental results are more accurate and have a lower degree of complexity than current counterpart methods. In [22], the authors presented a hybrid intelligent DL-enabled technique to protect IIoT network against fatal and complex multi-variant botnet attacks. The suggested mechanism was thoroughly tested using the most recent dataset, as well as conventional and enhanced effectiveness evaluation measures, and the most up-to-date DL benchmark algorithms. In addition, the study do cross validation on the results to demonstrate overall performance. The proposed approaches outperform in detecting multi-variant advanced bot attacks with high accuracy. Furthermore, the proposed technique has shown to be effective in terms of speed. In [23], the authors suggested a set of strong DL-based models for classifying botnet assaults that typically affect IIoT devices and networks. The DL-based models such as the artificial neural network (ANN), the long short-term memory (LSTM), and the gated recurrent unit (GRU) may successfully classify IIoT malware threats with an accuracy of up to 99%, according to the results.

From the reviewed literatures, the performance of the Botnet detection can still be improved by optimization techniques before using classification algorithms. Hence the significant contributions of the study are:

i. this article develops a novel Glowworm Swarm Optimization Driven Gated Recurrent Unit Enabled Botnet Detection (GSOGRU-BD) model in IIoT Environment. Using the GSO algorithm is used for optimal hyper-parameter tuning of the GRU model.
ii. the GSOGRU-BD model involves the GRU model for the effective recognition and classification of botnets.
iii. presented a GSOGRU-BD model to efficiently identify the presence of botnet attacks in the IIoT environment. To do so, the GSOGRU-BD model initially preprocessed the input data to get rid of missing values. and,
iv. a comparative experimental validation of the GSOGRU-BD model is tested using benchmark dataset.

The rest of the study is organized as follows: section 2 presents the proposed model for intrusion detection using GRU model, and GSO model for hyperparameter optimization. Section 3 discusses the implementation of the paper, and finally, section 4 conclude the paper.

2. The Proposed Model

In this study, a new GSOGRU-BD model has been developed for effective botnet detection in IIoT Environment. The presented GSOGRU-BD model intends to effectually identify the presence of botnet attacks in the IIoT environment. To do so, the GSOGRU-BD model initially preprocessed the input data to get rid of missing values. In addition, the GSOGRU-BD model involves the GRU model for the effective recognition and classification of botnets. Besides, the GSO algorithm is used for optimal hyperparameter tuning of the GRU model.

2.1 Intrusion Detection using GRU Model

Firstly, the GSOGRU-BD model involves the GRU model for the effective recognition and classification of botnets. GRU is dissimilar from LSTM whereas the last one comprises three gate functions that is based on RNN system namely forgetting, output, and input gates to memory, output value, and control input [15]. But two gates are anticipated in GRU mechanisms that is, upgrade and reset gates. σ indicates the gate function. GRU implements in forgetting and input gates of LSTM for individual upgrading gate. This technique efficiently reduces the quantity of approximations and the likelihoods of gradient disappearance or explosion. It can be expressed in the following:

$$Z_t = \sigma(W_z \cdot [h_{t-1}, x_t] + b_z), \quad (1)$$

DOI: https://doi.org/10.54216/JISIoT.060103
Received: October 21, 2021 Accepted: January 15, 2022

$$r_t = \sigma(W_r \cdot [h_{t-1}, x_t] + b_r), \quad (2)$$

$$h'_t = tanh(W \cdot [r_t * h_{t-1}, x_t] + b_h), \quad (3)$$

$$h_t = (1 - z_t) * h_{t-1} + z_t * h'_t, \quad (4)$$

$$y_t = \sigma(W_0 \cdot h_t), \quad (5)$$

In which Z_t and r_t denotes reset and upgrade gates. W_z, W_r, W, and W indicate the weight parameter of input data, h_{t-1} represent the output of earlier layer, and x_t characterizes the input of recent layer. b_z, b_r, and b_h determine the bias, σ indicates the sigmoid function, and $tanh$ is applied for changing the value flow through network. The resulting values that are σ and tanh function is ordered among $(0, 1)$ and $(-1,1)$. Afterward finding the last result, the loss value is estimated by loss function.

$$E_t = \frac{1}{2}(y_d - y_t^0)^2, \quad (6)$$

$$E = \sum_{t=1}^{T} E_t, \quad (7)$$

Now E_t denotes the loss of individual instance at time, y_d implies real label dataset, y_t^0 denotes the resulting value of main iteration, and E indicates the loss of individual instance [16]. Fig. 2 shows the structure of GRU model.

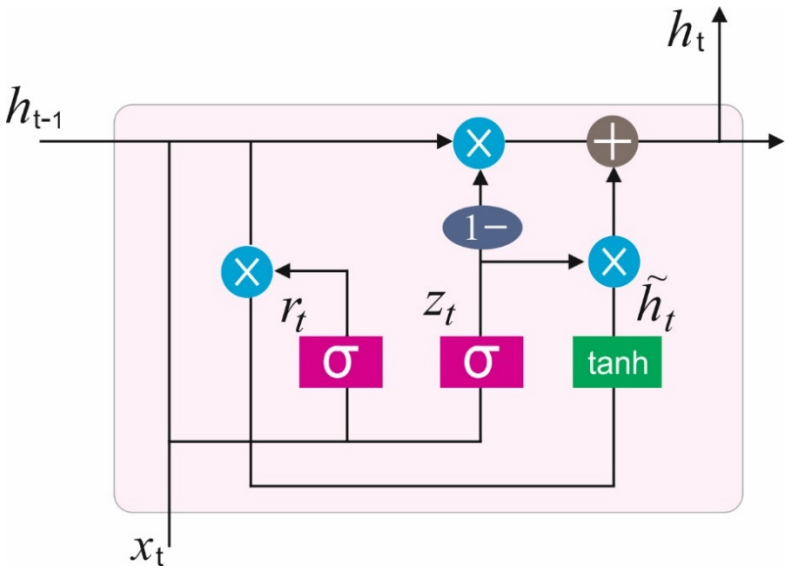

Fig. 2. Structure of GRU Model

2.2 Hyperparameter optimization using GSO algorithm

At this stage, the GSO algorithm is used for optimal hyperparameter tuning of the GRU model. GSO algorithm is considered as an intelligent swarm optimization approach that is utilized in quickening brightness characteristics of firefly. In GSO approach, it is dispersed in a solution space according to Fitness Function (FF) of each glowworm position. The strong glowworm has highest illumination and an optimum location whereby it protects highest FF rate. Glowworm is encompassed of dynamic line of sight, called as a decision area that has the ranges of density for adjacent node. Alternatively, the decision radius is constraint whereas the glowworm travels toward a same kind of stronger fluorescence in a decision area. Each glowworm will be positioned in the optimal position when high value of iteration is accomplished. It is composed of five stages as shown [17]:

- Fluorescence in concentration

DOI: https://doi.org/10.54216/JISIoT.060103
Received: October 21, 2021 Accepted: January 15, 2022

- Neighboring set
- Decision area radius
- Moving possibility
- Glowworm location

The can be shown in the following.

$$l_i(t) = (1-\alpha)l_i(r-1) + \beta f(x_i(t)), \tag{8}$$

Whereas α denotes the fluorescence in volatilization coefficient, $l_i(f)$ denotes the fluorescence in the attentiveness of i-th glowworm at time f, f(x) represents the fitness function, β indicates fluorescence in improvement factor, and $x_i(r)$ characterizes the place of i-th glowworm at f time that is given below.

$$N_i(t) = \{j: \|x_j(r) - x_i(t)\| < r_d^i; l_i(t) < l_j(t)\}, \tag{8}$$

Now $r_d^i(r)$ denotes the range of decision field for i-th glowworm and f $N_i(f)$ denotes the neighboring subset of ith glowworm as follows.

$$r_d^i(t+1) = \min\{r_s, \max\{r_d^i(t) + \gamma(n_i - |N_i(t)|)\}\}, \tag{10}$$

Now r_s characterizes the accomplished range of a glowworm, γ denotes the number of decision area, and n_i displays the neighboring threshold. The motion likelihood of upgraded method is showed by.

$$p_{ij}(r) = \frac{l_j(t) - l_i(t)}{\sum_{k\in N_t} l_k(t) - l_i(r)}, \tag{11}$$

In the equation, $p_{ij}(t)$ displays the probability in which i-th glowworm travel to the j-th glowworm in r time as follows.

$$x_i(t+1) = x_i(t) + s\left(\frac{x_j(t) - x_i(t)}{\|x_j(t) - x_i(t)\|}\right), \tag{12}$$

The presented method is a goal in powerful optimization approach for optimizing the convergence rate of varied heuristic optimization techniques. The powerful efficacy of presented method assists to the approximation of opposite population and the current population in an analogous generation to recognize the ideal candidate solution. The presented method has efficiently been employed in different meta-heuristics to enhance the convergence rate. Assume $N \in N[x,y]$ denotes a real value. It can be represented as follows [18]:

$$N^o = x + y - N \tag{13}$$

For d-dimensional searching region, the explanation should be prolonged by:

$$N_i^o = x_i + y_i - N_i \tag{14}$$

whereas $(N_1, N_2, .. N_d)$ represents d-dimension searching region and $N_i[x_i, y_i], i = 1,2,..,d$. From Oppositional Based Optimization (OBO), the presented approach is employed in this initialized method of the GSO approach and for all the iterations, in the applications of jumping speed.

3. Experimental Validation

In this section, a detailed experimental validation of the GSOGRU-BD model is performed using the benchmark N-BaIoT dataset [19].

DOI: https://doi.org/10.54216/JISIoT.060103
Received: October 21, 2021 Accepted: January 15, 2022

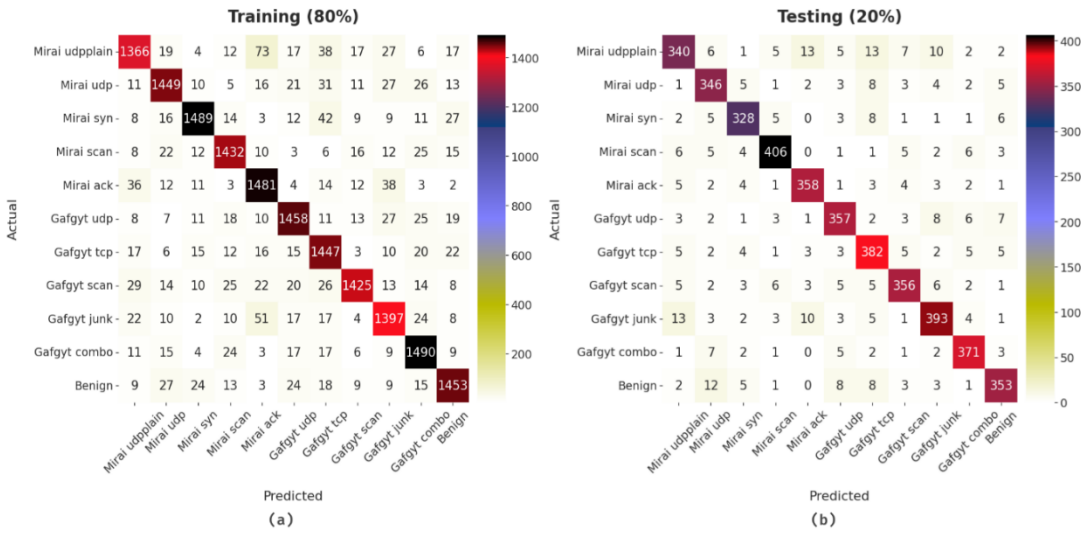

Fig. 3. Confusion matrices of GSOGRU-BD model

Fig. 3 highlights the confusion matrices offered by the GSOGRU-BD model on 80% of training data and 20% of testing data. The results denoted that the GSOGRU-BD model has shown effective identification and classification of data samples under different categories.

Table 1 provides an overall detection performance of the GSOGRU-BD model on 80% of training data and 20% of testing data.

Fig. 4 inspects a detailed detection result analysis of the GSOGRU-BD model on 80% of training data with distinct classes. The GSOGRU-BD model has classified Mirai udpplain class samples with $accu_y$, $prec_n$, $reca_l$, and F_{score} of 97.79%, 89.57%, 85.59%, and 87.54% respectively. In addition, the GSOGRU-BD model has classified Mirai udp class samples with $accu_y$, $prec_n$, $reca_l$, and F_{score} of 98.19%, 90.73%, 89.44%, and 90.08% respectively. Along with that, the GSOGRU-BD model has classified Mirai syn class samples with $accu_y$, $prec_n$, $reca_l$, and F_{score} of 98.56%, 93.53%, 90.79%, and 92.14% respectively. Moreover, the GSOGRU-BD model has classified Mirai scan class samples with $accu_y$, $prec_n$, $reca_l$, and F_{score} of 98.49%, 91.33%, 91.74%, and 91.53% respectively.

Table 1 Botnet classification outcomes of GSOGRU-BD model

Training (80%)				
Class Labels	**Accuracy**	**Precision**	**Recall**	**F-Score**
Mirai udpplain	97.79	89.57	85.59	87.54
Mirai udp	98.19	90.73	89.44	90.08
Mirai syn	98.56	93.53	90.79	92.14
Mirai scan	98.49	91.33	91.74	91.53
Mirai ack	98.06	87.74	91.65	89.65
Gafgyt udp	98.30	90.67	90.73	90.70
Gafgyt tcp	97.98	86.80	91.41	89.05
Gafgyt scan	98.40	93.44	88.73	91.03
Gafgyt junk	98.03	88.53	89.44	88.98
Gafgyt combo	98.39	89.81	92.83	91.30
Benign	98.35	91.21	90.59	90.90
Average	**98.23**	**90.31**	**90.27**	**90.26**
Testing (20%)				
Mirai udpplain	97.57	88.77	84.16	86.40

DOI: https://doi.org/10.54216/JISIoT.060103
Received: October 21, 2021 Accepted: January 15, 2022

Mirai udp	98.18	88.27	91.05	89.64
Mirai syn	98.57	91.36	91.11	91.24
Mirai scan	98.64	93.76	92.48	93.12
Mirai ack	98.68	91.79	93.23	92.51
Gafgyt udp	98.34	90.61	90.84	90.72
Gafgyt tcp	97.95	87.41	91.61	89.46
Gafgyt scan	98.39	91.52	90.36	90.93
Gafgyt junk	98.05	90.55	89.73	90.14
Gafgyt combo	98.75	92.29	93.92	93.10
Benign	98.25	91.21	89.14	90.17
Average	**98.31**	**90.69**	**90.69**	**90.68**

Fig. 5 studies a comprehensive detection result investigation of the GSOGRU-BD model on 20% of testing data with dissimilar classes. The GSOGRU-BD model has classified Mirai udpplain class samples with $accu_y$, $prec_n$, $reca_l$, and F_{score} of 97.57%, 88.77%, 84.16%, and 86.40% respectively. In addition, the GSOGRU-BD model has classified Mirai udp class samples with $accu_y$, $prec_n$, $reca_l$, and F_{score} of 98.18%, 88.27%, 91.05%, and 89.64% respectively. Along with that, the GSOGRU-BD model has classified Mirai syn class samples with $accu_y$, $prec_n$, $reca_l$, and F_{score} of 98.57%, 91.36%, 91.11%, and 91.24% respectively. Moreover, the GSOGRU-BD model has classified Mirai scan class samples with $accu_y$, $prec_n$, $reca_l$, and F_{score} of 98.64%, 93.76%, 92.48%, and 93.12% respectively.

Fig. 6 offers a detailed precision-recall and ROC examination of the GSOGRU-BD model with 80% of training data and 20% of testing data. The figure indicated that the GSOGRU-BD model has offered maximum values of precision-recall and ROC under both datasets.

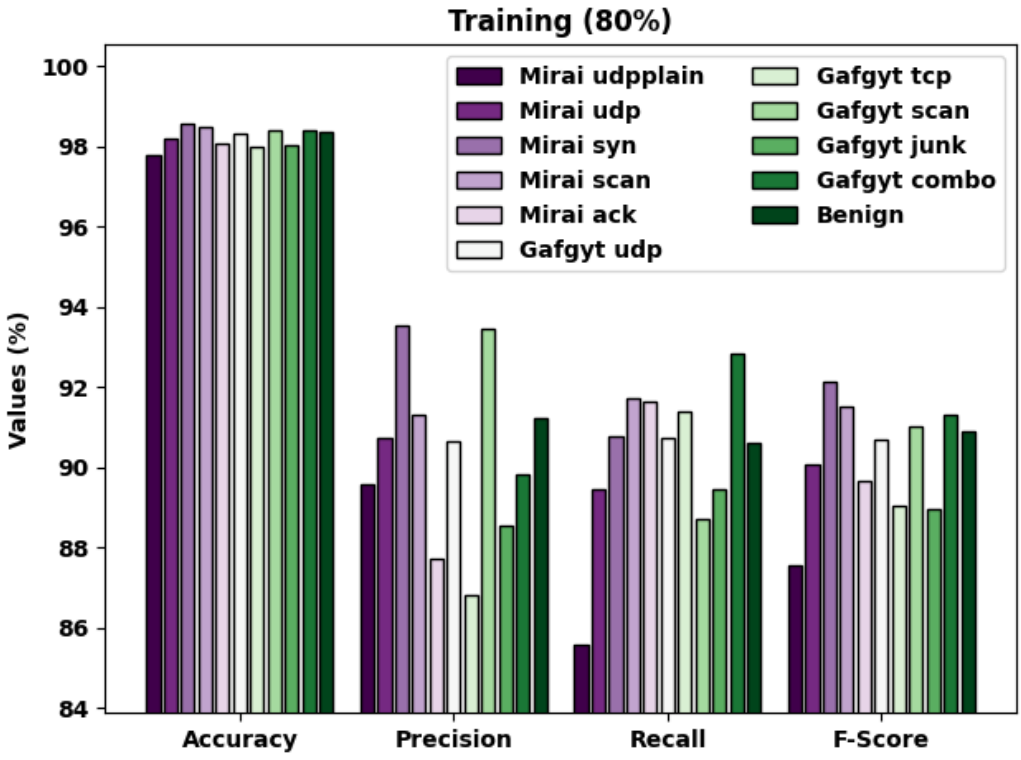

Fig. 4. Classification outcomes of GSOGRU-BD model on 80% of training data

DOI: https://doi.org/10.54216/JISIoT.060103
Received: October 21, 2021 Accepted: January 15, 2022

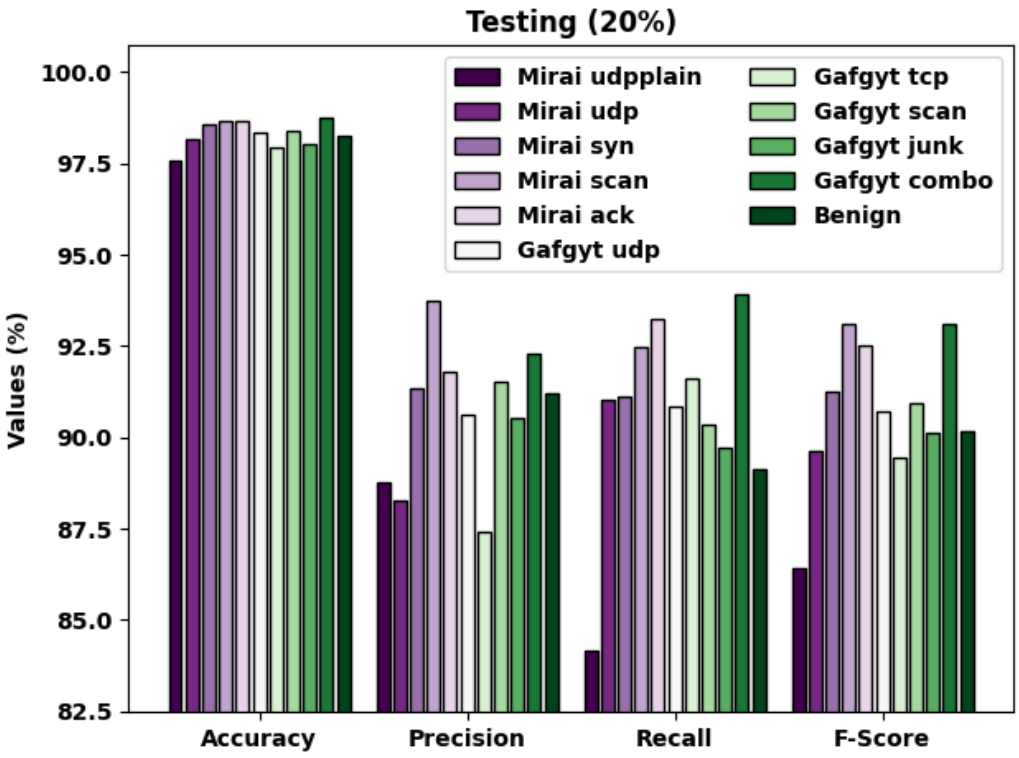

Fig. 5. Classification outcomes of GSOGRU-BD model on 20% of testing data

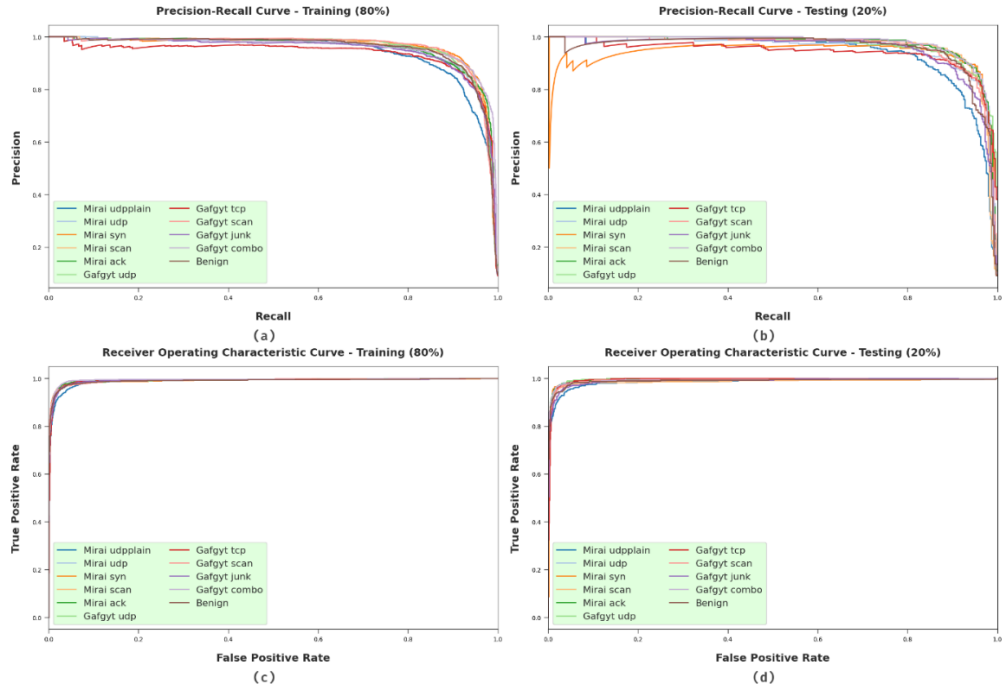

Fig. 6. Precision-recall and ROC of GSOGRU-BD model

Table 2 and Fig. 7 highlights a detailed comparative study of the GSOGRU-BD model with recent models [20]. The experimental result analysis reported that the NN-WOHP model has accomplished least detection outcome with $accu_y$, $prec_n$, $reca_l$, and F_{score} of 80.74%, 73.33%, 81.64%, and 75.71% respectively. Also, the NN-WOGN model has gained certainly improved performance with $accu_y$,

DOI: https://doi.org/10.54216/JISIoT.060103
Received: October 21, 2021 Accepted: January 15, 2022

$prec_n$, $reca_l$, and F_{score} of 83.51%, 79.74%, 84.43%, and 81.26% respectively. In addition, the BA-NN model has accomplished reasonable with $accu_y$, $prec_n$, $reca_l$, and F_{score} of 85.67%, 84.55%, 86.92%, and 85.33% respectively.

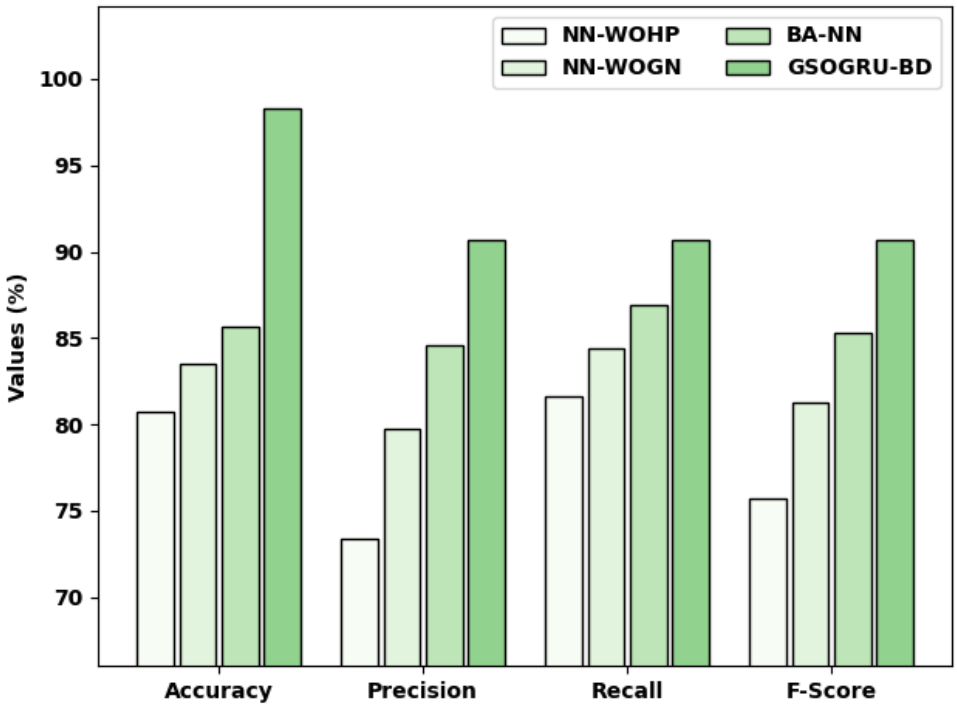

Fig. 7. Comparative examination of GSOGRU-BD model with recent approaches

Table 2 Comparative study of GSOGRU-BD model on botnet classification

Methods	Accuracy	Precision	Recall	F-Score
NN-WOHP	80.74	73.33	81.64	75.71
NN-WOGN	83.51	79.74	84.43	81.26
BA-NN	85.67	84.55	86.92	85.33
GSOGRU-BD	98.31	90.69	90.69	90.68

DOI: https://doi.org/10.54216/JISIoT.060103
Received: October 21, 2021 Accepted: January 15, 2022

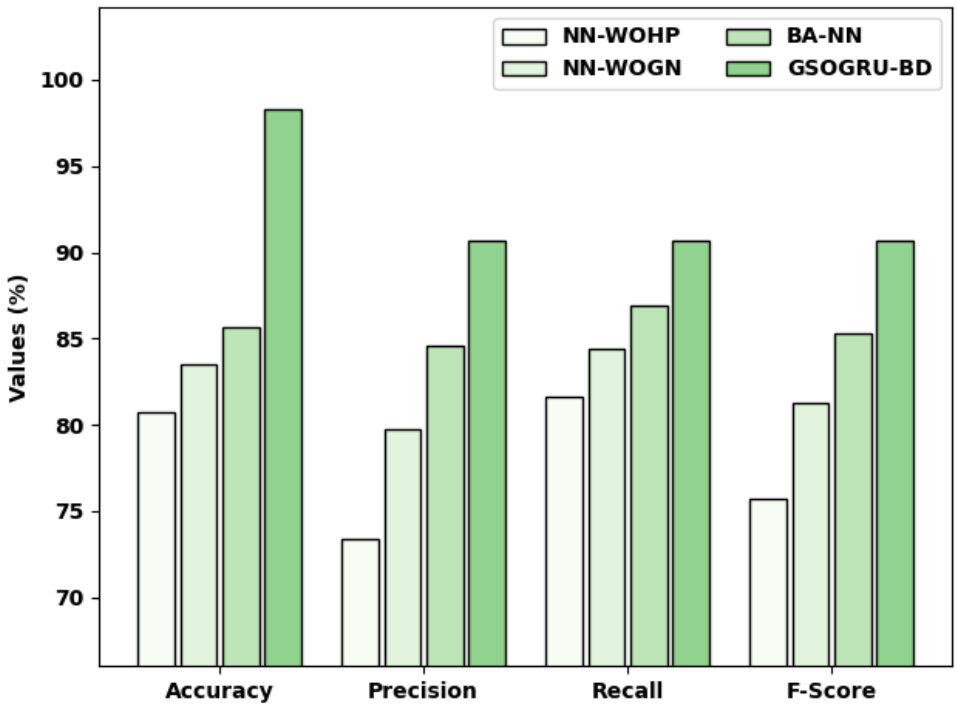

Fig. 7. Comparative examination of GSOGRU-BD model with recent approaches

4. Conclusion

In this study, a new GSOGRU-BD model has been developed for effective botnet detection in IIoT Environment. The presented GSOGRU-BD model intends to effectually identify the presence of botnet attacks in the IIoT environment. To do so, the GSOGRU-BD model initially preprocessed the input data to get rid of missing values. In addition, the GSOGRU-BD model involves the GRU model for the effective recognition and classification of botnets. Besides, the GSO algorithm is used for optimal hyperparameter tuning of the GRU model. A comparative experimental validation of the GSOGRU-BD model is tested using benchmark dataset and the results reported the better outcomes of the GSOGRU-BD model. As a part of future scope, the performance can be raised by the outlier removal and clustering schemes.

References

[1] Xenofontos, C., Zografopoulos, I., Konstantinou, C., Jolfaei, A., Khan, M.K. and Choo, K.K.R., 2021. Consumer, commercial and industrial iot (in) security: attack taxonomy and case studies. IEEE Internet of Things Journal.

[2] Khan, W.U., Malik, J., Hasan, T., Bibi, I., Al-Wesabi, F.N., Dev, K. and Huang, G., 2022. Securing Industrial Internet of Things Against Botnet Attacks Using Hybrid Deep Learning Approach.

[3] Scheidt, N. and Adda, M., 2021. Threats in industrial IoT. In Internet of Things, Threats, Landscape, and Countermeasures (pp. 137-166). Boca Raton and London: CRC Press.

[4] Popoola, S.I., Ande, R., Adebisi, B., Gui, G., Hammoudeh, M. and Jogunola, O., 2021. Federated deep learning for zero-day botnet attack detection in IoT edge devices. IEEE Internet of Things Journal.

[5] Nguyen, T.N., Ngo, Q.D., Nguyen, H.T. and Giang, N.L., 2022. An Advanced Computing Approach for IoT-Botnet Detection in Industrial Internet of Things. IEEE Transactions on Industrial Informatics.

[6] Bhatt, S. and Ragiri, P.R., 2021. Security trends in Internet of Things: A survey. SN Applied Sciences, 3(1), pp.1-14.

DOI: https://doi.org/10.54216/JISIoT.060103
Received: October 21, 2021 Accepted: January 15, 2022

[7] Franco, J., Aris, A., Canberk, B. and Uluagac, A.S., 2021. A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems. IEEE Communications Surveys & Tutorials, 23(4), pp.2351-2383.
[8] Kumar, P., Singh, A. and Sengupta, A., 2021. Industrial IoT: Challenges and Mitigation Policies. In Computer Networks, Big Data and IoT (pp. 143-159). Springer, Singapore.
[9] Kumar, P., Kumar, R., Gupta, G.P., Tripathi, R. and Srivastava, G., 2022. P2TIF: A Blockchain and Deep Learning Framework for Privacy-preserved Threat Intelligence in Industrial IoT. IEEE Transactions on Industrial Informatics.
[10] Popoola, S.I., Adebisi, B., Ande, R., Hammoudeh, M. and Atayero, A.A., 2021. Memory-efficient deep learning for botnet attack detection in iot networks. Electronics, 10(9), p.1104.
[11] Alharbi, A., Alosaimi, W., Alyami, H., Rauf, H.T. and Damaševičius, R., 2021. Botnet attack detection using local global best bat algorithm for industrial internet of things. Electronics, 10(11), p.1341.
[12] Li, J., Lyu, L., Liu, X., Zhang, X. and Lv, X., 2021. FLEAM: A federated learning empowered architecture to mitigate DDoS in industrial IoT. IEEE Transactions on Industrial Informatics.
[13] Yan, Q., Huang, W., Luo, X., Gong, Q. and Yu, F.R., 2018. A multi-level DDoS mitigation framework for the industrial Internet of Things. IEEE Communications Magazine, 56(2), pp.30-36.
[14] Lee, S., Abdullah, A., Jhanjhi, N. and Kok, S., 2021. Classification of botnet attacks in IoT smart factory using honeypot combined with machine learning. PeerJ Computer Science, 7, p.e350.
[15] Zhang, Y.G., Tang, J., He, Z.Y., Tan, J. and Li, C., 2021. A novel displacement prediction method using gated recurrent unit model with time series analysis in the Erdaohe landslide. Natural Hazards, 105(1), pp.783-813.
[16] Zhang, Y. and Yang, L., 2021. A novel dynamic predictive method of water inrush from coal floor based on gated recurrent unit model. Natural Hazards, 105(2), pp.2027-2043.
[17] Sampathkumar, A., Mulerikkal, J. and Sivaram, M., 2020. Glowworm swarm optimization for effectual load balancing and routing strategies in wireless sensor networks. Wireless Networks, 26(6), pp.4227-4238.
[18] Xiuwu, Y., Qin, L., Yong, L., Mufang, H., Ke, Z. and Renrong, X., 2019. Uneven clustering routing algorithm based on glowworm swarm optimization. Ad Hoc Networks, 93, p.101923.
[19] Meidan, Y.; Bohadana, M.; Mathov, Y.; Mirsky, Y.; Shabtai, A.; Breitenbacher, D.; Elovici, Y. N-BaIoT: Network-based Detection of IoT Botnet Attacks Using Deep Autoencoders. IEEE Pervasive Comput. 2018, 17, 12–22.
[20] Alharbi, A., Alosaimi, W., Alyami, H., Rauf, H.T. and Damaševičius, R., 2021. Botnet attack detection using local global best bat algorithm for industrial internet of things. Electronics, 10(11), p.1341.
[21] Nguyen, T. N., Ngo, Q. D., Nguyen, H. T., & Giang, N. L. 2022. An Advanced Computing Approach for IoT-Botnet Detection in Industrial Internet of Things. IEEE Transactions on Industrial Informatics.
[22] Hasan, T., Malik, J., Bibi, I., Khan, W. U., Al-Wesabi, F. N., Dev, K., & Huang, G., 2022. Securing industrial internet of things against botnet attacks using hybrid deep learning approach. IEEE Transactions on Network Science and Engineering.
[23] Mudassir, M., Unal, D., Hammoudeh, M., & Azzedin, F., 2022. Detection of Botnet Attacks against Industrial IoT Systems by Multilayer Deep Learning Approaches. Wireless Communications and Mobile Computing, 2022.

DOI: https://doi.org/10.54216/JISIoT.060103
Received: October 21, 2021 Accepted: January 15, 2022