Detecting IoT Botnets: A Novel Hybrid Approach for Enhanced Security

Ritesh Kumar[1], Sukhman Ghumman[2], Dr. Shweta Loonkar[3], Syed Rashid Anwar[4], M N Nachappa[5], Abhinav Mishra[6]

[1]Assistant Professor, Maharishi School of Engineering & Technology, Maharishi University of Information Technology, Uttar Pradesh, India, Email Id- riteshkumar268@gmail.com, Orcid Id- 0009-0008-6351-083X
[2]Centre of Research Impact and Outcome, Chitkara University, Rajpura- 140417, Punjab, India sukhman.ghumman.orp@chitkara.edu.in https://orcid.org/0009-0005-2008-1009
[3]Assistant Professor, Department of ISME, ATLAS SkillTech University, Mumbai, Maharashta, India, Email Id- shweta.loonkar@atlasuniversity.edu.in, Orcid Id- 0000-0001-8227-5937
[4]Assistant Professor, Department of Computer Science & IT, ARKA JAIN University, Jamshedpur, Jharkhand, India, Email Id- syed.r@arkajainuniversity.ac.in, Orcid Id- 0000-0001-9810-8850
[5]Professor, Department of Computer Science and Information Technology, JAIN (Deemed-to-be University), Bangalore, karnataka, India, Email Id- mn.nachappa@jainuniversity.ac.in, Orcid Id- 0000-0002-4007-5504
[6]Chitkara Centre for Research and Development, Chitkara University, Himachal Pradesh-174103 India abhinav.mishra.orp@chitkara.edu.in https://orcid.org/0009-0005-9856-6727

Internet of Things (IoT) botnet identification and mitigation are the main security concerns by the explosive growth of IoT devices. IoT flaws and possible attacks arise from the inability of current detection technologies to identify complex botnet operations. Thus, for ensuring the reliability and safety of networked IoT devices, a thorough and reliable detection strategy is needed for identifying and eliminating developing IoT botnet threats. Therefore, they present a unique Divergent Grid Search-Driven Gated Recurrent Unit (DGS-GRU) method to recognize IoT botnets in this research. They undertake extensive experiments on Python environment to test the efficiency of our DGS-GRU strategy in various network environments, and they assess its effectiveness using a variety of IoT datasets. The suggested approach is examined by means of accuracy, precision, recall and f1-score from the extensive experiment and contrasted with other current approaches. The findings suggest that our approach has better detection capability than traditional techniques, which bodes well for enhancing IoT security and protecting against developing botnet threats. In the context of the linked IoT world, this research advances IoT security measures and lays the groundwork for proactive safety techniques against new cyber dangers.

Keywords: A Iot, Botnet, Reliability and Safety, Divergent Grid Search-Driven and Gated Recurrent Unit (DGS-GRU).

1. Introduction

The IoT is a network of attached things, gadgets, and sensors that can collect and share data via the internet. These things have sensors and communication capabilities [1]. They range from commonplace products like cars and appliances to industrial machinery and wearable electronics. Smart homes, healthcare, agriculture, and industry are few of the areas where IoT-enabled seamless information and control sharing between devices has resulted in higher efficiency, automation, and better decision-making. By enabling remote monitoring, predictive maintenance, and personalized services, it has the potential to improve our quality of life [2]. To guarantee the dependable and secure functioning of IoT ecosystems, it raises questions regarding data privacy, security, and the necessity for defined protocols.

IoT botnets are collections of compromised IoT devices, including routers, thermostats, and smart cameras, that have been contaminated with malware. Cybercriminals command these botnets to launch a variety of cyber-attacks [3]. The development of IoT devices, coupled with their related holes in terms of safety features, makes them targets of choice for attack. Once a device has been hacked, it can be utilized for illicit activities such as the unauthorized acquisition of data or the perpetration of distributed denial of service (DDoS) assaults [4]. These cases have garnered considerable attention and recognition in the sector. Both manufacturers and customers need to focus on security as a means of mitigating this threat. They should update firmware, change default passwords, and put network-level security measures in place to stop IoT botnet development [5].

Finding botnets on the IoT essential to protecting networks and linked devices. Proper techniques are necessary to identify and find these adversarial networks. Anomaly-based detection approaches are employed to monitor and identify unusual patterns in the actions of IoT devices. These methods are particularly effective in detecting atypical trends, such as unanticipated data flow or abnormal device activity [6]. It is possible to identify known malware variants connected to IoT botnets using signature-based techniques. In order to detect communication patterns and domains/IP addresses linked to botnet activity, network traffic analysis is crucial [7]. Using machine learning (ML) techniques and intrusion detection systems can improve detection accuracy. Effective mitigation of IoT botnet risks requires ongoing monitoring and prompt action. To strengthen defences against growing botnet threats, it's also critical to collaborate with security professionals, share threat intelligence, and keep IoT devices updated with the latest security updates [8]. This paper present a unique method called the Divergent Grid Search-Driven Gated Recurrent Unit (DGS-GRU) method is proposed for the identification of IoT botnets.

2. Related works

According to the author of, [9] proposed a new and sophisticated approach to IoT botnet identification that builds on static analysis employing dynamic analysis to enhance. The results demonstrate that, in terms of accuracy and complexity, our methodology has fared better than other current counterpart methods. Research [10] proposed approach GWO and GWO algorithm was utilized to optimize the hyper parameters of the OCSVM and simultaneously identify the most suitable features for accurately characterizing the IoT botnet issue. The results indicate an evidenced by higher true positive rates, lower false positive rates, and improved G-mean values in IoT device. The proposed a novel lightweight and versatile Network Intrusion Detection System (NIDS) [11] that employs a two-stage architecture for the purpose of detecting botnet activities specifically on the IoT network. Notably, their proposed NIDS solely relies on readily available packet-length data for its detection capabilities. The results show that our NIDS demonstrates a high level of accuracy in detecting botnet activity.

Study [12] proposed the Fisher score method was (GXGBoost), a popular filter-based feature selection technique that increases inter-class distance and reduces. The results of the IoT botnet attack detection procedure were produced through the cross-validation approaches. To developed a Cross CNN-LSTM [13], a detection technique that combines deep learning models of CNN-LSTM to identify IoT botnets. The results demonstrated that the recommended model is precise and works better than some cutting edge techniques. The developed a unique network-based anomaly detection method for the IoT named N-BaIoT [14]. The Results show the capability to efficiently and swiftly locate the attacks in actual time, origination from the compromised IoT devices that detected a botnet. Author [15] proposed executed ML-based experiments and verified the viability. The results are compared, and ML-based binary and multiclass classification was used to assess the detection effectiveness. Study [16] developed IoT botnet traffic on the 5G core network by an extensive investigation employing machine learning techniques. The results demonstrated how machine learning and AI-based security were used to find the 5GC network. The proposed a first method for finding IoT botnet from normal data using static and dynamic attributes with machine learning classifiers. The results demonstrated the process of training and verifying our proposed method has a significant advantage [17]. The research [18] proposed a method CNN-LSTM was detected botnet on IoT devices. The results showed improved accuracy and a lower rate. Author of, [19] proposed the analysis of using real-world IoT traffic information, the proposed technique was verified. The approach obtained accuracy rates of the botnet dataset, as demonstrated by the results of the experiment.The proposed an original approach called Multi-Objective Dynamic Harris Howks Optimization (MODHHO) [20] for the purpose of identifying Botnets in IoT networks. The results demonstrate that the MODHHO algorithm exhibits strong performance in the realm of Botnet Detection in IoT methodologies based on performance metrics.

The following are the remaining sections of the paper: Section 3 provides an in-depth discussion of the proposed approach technique, while Section 4 displays the study's findings. The fifth section describes the conclusion.

3. Methods

The Divergent grid search-driven gated recurrent unit (DGS-GRU) method is a revolutionary approach that is introduced to identifying IoT botnets.

3.1 Gated Recurrent Unit (GRU)

The GRU's purpose is to make possible for recurrent blocks to successfully capture dependencies across multiple temporal as shown in Figure 1. The activation functions used in neural networks are either the hyperbolic tangent $tanh$ or sigmoid functions. In the $i-th$ GRU, the calculation of the candidate update $\tilde{g}_s^i$ is performed initially when provided with an input vector x at time t Equation (1).

$$\tilde{g}_s^i = tanh\big(Xw_s + V(q_s \otimes g_{s-1})\big)^i \qquad (1)$$

Where $\otimes$ is an element-wise multiplication operation. The computation of a reset gate, g is done where the amount that the unit updates from all the prior activations in the same layer is controlled by a series of reset gates $\tilde{g}_s^i$ Equation (2).

$$q_s^i = \sigma\big(X_q w_s + V_q g_{s-1}\big)^i \qquad (2)$$

A sigmoid σ function is the activation function. Next, the GRU's activation is produced using the most recent candidate update and its prior activation Equation (3).

$$g_s^i = \big(1 - y_s^i\big)g_{s-1}^i + y_s^i \tilde{g}_s^i \qquad (3)$$

Where the update gate y_s^i is determined as follows and determines the amount of updates the unit receives after activation Equation (4).

$$y_s^i = \sigma(X_y w_s + V_y g_{s-1})^i \qquad (4)$$

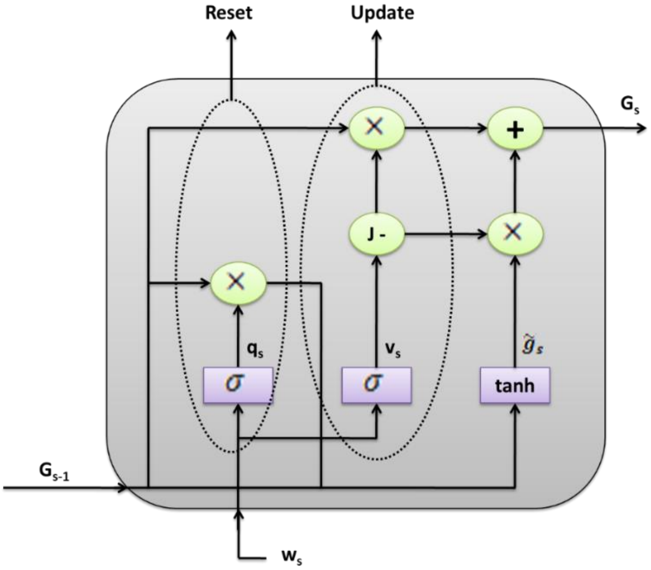

Figure 1: The framework of the Gated Recurrent Unit (GRU) (Source: Author)

3.2 Grid search (GS)

Grid search is a systematic machine learning technique that tests various combinations of hyper parameters to maximize model performance by analysing all potential combinations. W_S, is utilised to locate an improved subset K that can optimise the resulting model E by minimising a loss function K (W, E). The determination of the parametrization in this approach is contingent upon a collection of hyperparameters, which are represented as W_o. The machine learning technique known as grid search is the subject of discussion Equation (5).

$$\lambda^{*} = \arg\min_{\lambda} K\big(W_o; b(W_S; \lambda)\big) = \arg\min_{\lambda} E(\lambda; b, W_s, W_o, K) \tag{5}$$

The loss function of the training subset, denoted as K, and the method of the testing subset are under consideration. The set λ represents the hyper-parameters that are to be optimised. W_s and W_o is an objective function that measuring the performance of the new set of hyper-parameters λ^{*}. W_o is the set of hyper parameters is the focus of optimisation; W_s is a function meant to assess the effectiveness of immediately picked hyper-parameters. E and K is the function of loss.

3.3 Divergent grid search-driven gated recurrent unit (DGS-GRU)

The field of cyber security employs a novel and efficient method for identifying IoT botnets by integrating GRUs with grid search optimising, thereby demonstrating its effectiveness and contemporary relevance. The objective of this research group is enhancing the accuracy and effectiveness of botnet detection systems by focused on the dynamic characteristics of cyber-attacks aimed at IoT devices. The gating methods employed by GRUs, which regulate the information flow inside the network, make them very suitable for evaluating the dynamic and time-sensitive attributes of IoT data. The hybrid model employs grid search optimisation to investigate a broad spectrum of hyper parameter combinations, hence ensuring the optimal configuration of the GRU to manage the unique attributes of botnet-related IoT data. The hybrid method is considered the most effective approach for managing the intricacy of IoT environments, characterized by the constant generation of diverse data from various devices. The model demonstrates its capability to address various IoT network scenarios due to the comprehensive exploration of hyper parameter values facilitated by grid search optimization. In the meantime, the GRU's capacity to retain temporal relationships equips the system with the capability to distinguish intricate and ever-changing patterns related to botnet activity. The algorithm 1 shows Divergent grid search-driven gated recurrent unit (DGS-GRU).

Algorithm 1: DGS-DGRU

```
import GRU
import GridSearch
def preprocess_data(data):
def create_GRU_model(input_shape, hyperparameters):
model = GRU.build_model(input_shape, hyperparameters)
return model
defdivergent_grid_search(data, hyperparameter_space):
best_model = None
best_accuracy = 0
```

```
for hyperparameters in hyperparameter_space:
model = create_GRU_model(data.shape, hyperparameters)
model.train(data)
accuracy = model.evaluate(validation_data)
if accuracy >best_accuracy:
best_model = model
best_accuracy = accuracy
return best_model
if _name_ == "_main_":
data = preprocess_data(load_data())
hyperparameter_space = GridSearch.generate_hyperparameter_grid()
best_model = divergent_grid_search(data, hyperparameter_space)
test_accuracy = best_model.evaluate(test_data)
print(f"Best model accuracy on test data: {test_accuracy}")
```

4. Result

4.1 Dataset

The comprehensive UNSW-NB15 dataset [4] was used in this investigation since UNSW determined to be the best training dataset. A random selection of 82,000 records was employed in this experiment. To classify the training and testing models. The data had to be prepared and cleansed. To code numerical data, categories including "proto," "type of service," "state," "sptks," "sload," and "attack cat" were employed. Two sets of data were randomly selected, one containing “75% of the data for training and 25% of the data for testing”.

4.2. Experimental setup

The Python 3.10 platform was used to evaluate the proposed techniques. The proposed optimisation techniques were shown using a Windows 10 laptop equipped with an Intel i5 12th Generation processor and 12 GB of RAM.

We compare the efficacy of the proposed strategy with existing methods, such as GWO-OCSVM [19], BO-GP-DT [19], and PSO-ONE-SVM [19]. The level to which risk botnet operations in IoT devices can be discovered and discriminated is referred to the efficacy of IoT botnet detection.

Accuracy is refers to the degree of accuracy in identifying harmful botnet activities. The metric measures the proportion of correctly identified positive and negative occurrences in the total number of instance, hence indicating the overall effectiveness of the model in differentiating between normal and malicious activity. Figure 2 and table 1 displays the accuracy of proposed method.

The recommended DGS-GRU technique have a high accuracy ratio of 97.6%, compared to the current GWO-OCSVM, BO-GP-DT, and PSO-ONE-SVM, which have poor accuracy ratios of 96.68%, 96.05%, and 97.01%, respectively as shown in Equation (6).

$$Accuracy = \frac{(TP+TN)}{(TP+TN+FP+FN)} \tag{6}$$

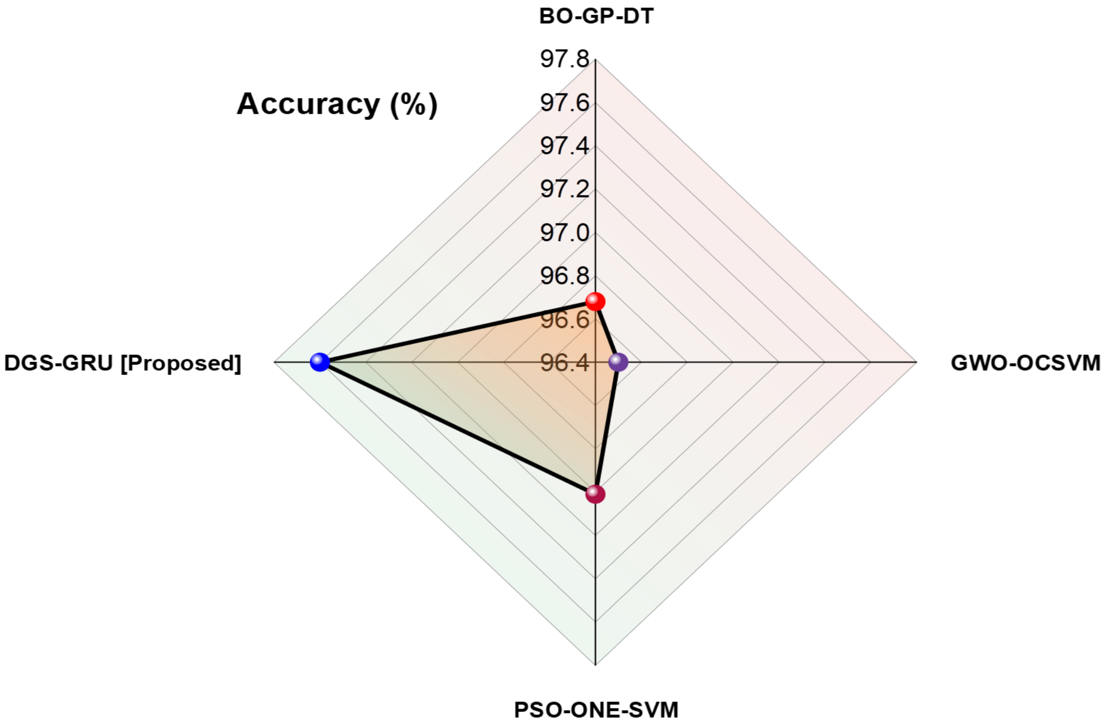

Figure 2: Accuracy (Source: Author)

Table 1: Accuracy (Source: Author)

Methods	Accuracy (%)
BO-GP-DT [19]	96.68%
GWO-OCSVM [19]	96.05%
PSO-ONE-SVM [19]	97.01%
DGS-GRU [Proposed]	97.6%

The precision in IoT botnet detection refers to the degree of precision is correctly detecting occurrences that are true positives. It serves as a measure of the proportion of detected actions that are actually harmful in nature. The primary focus includes the reduction of false positives, so increasing the possibility of accurately identifying serious threats, and subsequently enhancing the dependability and effectiveness of the system. Figure 3 and Table 2 displays the result of precision.

The proposed DGS-GRU technique have a high precision ratio is 98.01%, compared to the current GWO-OCSVM, BO-GP-DT, and PSO-ONE-SVM, which have low ratios of 96.73%, 96.54%, and 97.08%, respectively as shown in Equation (7).

$$Precision = \frac{TP}{(TP+FP)} \tag{7}$$

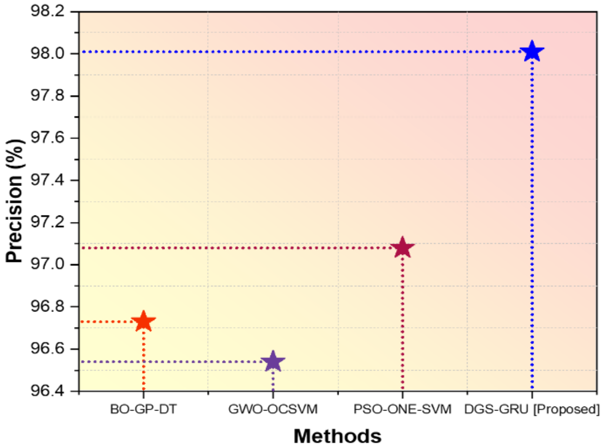

Figure 3: Precision (Source: Author)

Table 2: Precision (Source: Author)

Methods	Precision (%)
BO-GP-DT [19]	96.73%
GWO-OCSVM [19]	96.54%
PSO-ONE-SVM [19]	97.08%
DGS-GRU [Proposed]	98.01%

The recall metric used in the framework of IoT botnet detection measures its ability to identify actual instances of botnets. It measures the system's ability to capture and detect true positive cases, which is necessary for decreasing the amount of false negatives and increasing the overall effectiveness in the IoT ecosystem. Figure 4 and table 3 displays the result of recall. The existing methods GWO-OCSVM, BO-GP-DT, and PSO-ONE-SVM, exhibited recall rates of 96.68%, 96.5%, and 97.01% correspondingly. The suggested DGS-GRU method has a high recall rate of 97.05% as shown in Equation (8).

$$Recall = \frac{TP}{(TP+FN)} \tag{8}$$

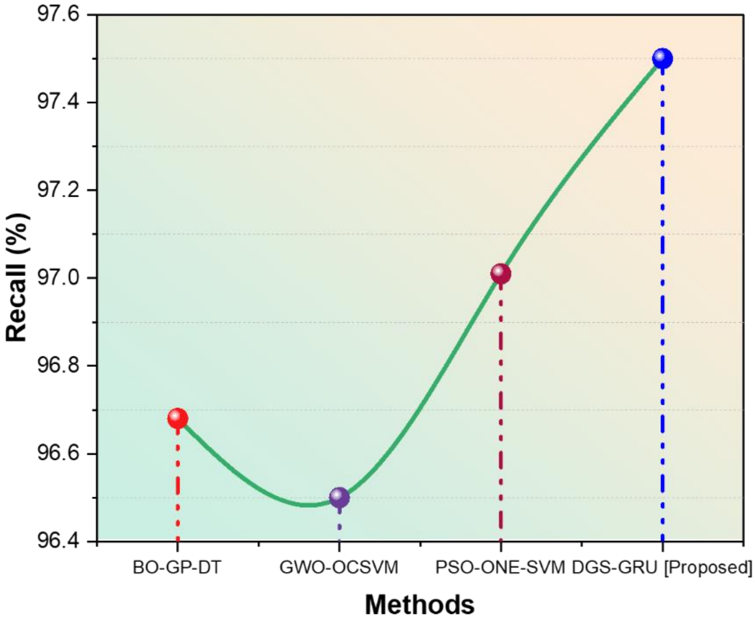

Figure 4: Recall (Source: Author)

Table 3: Recall (Source: Author)

Methods	Recall (%)
BO-GP-DT [19]	96.68%
GWO-OCSVM [19]	96.5%
PSO-ONE-SVM [19]	97.01%
DGS-GRU [Proposed]	97.5%

The F1-score of IoT botnet detection, quantifies the balance between precision and recall. The metric take advantage both positives and negatives, producing a unique value that indicates the efficacy of the model in detecting botnet behaviour in IoT networks. Figure 5 and table 4 displays the F1-score proposed method. The DGS-GRU method exhibits a significantly higher f1-score ratio of 98.07%, when compared to the GWO-OCSVM, BO-GP-DT, and PSO-ONE-SVM methods in use. The mentioned methods display lower ratios of 96.68%, 96.5%, and 97.01% respectively as shown in Equation (9).

$$F1 - score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (9)$$

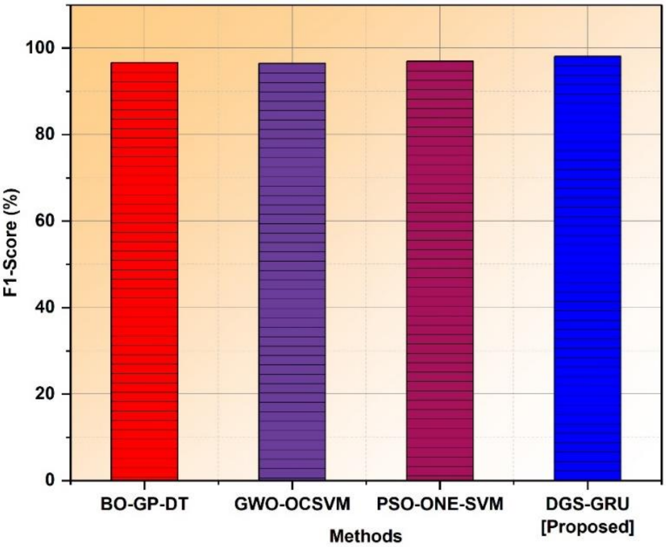

Figure 5: F1-score (Source: Author)

Table 4: F1-score (Source: Author)

Methods	F1-score (%)
BO-GP-DT [4]	96.68%
GWO-OCSVM [4]	96.5%
PSO-ONE-SVM [4]	97.01%
DGS-GRU [Proposed]	98.07%

‘

4. Conclusion

IoT botnet detection involves monitoring network traffic, spotting unusual activity, and applying ML algorithms to pinpoint suspect trends. Installing intrusion detection systems is essential to guaranteeing that IoT devices are shielded from possible security breaches. The DGS-GRU strategy, which is introduced in this study, represents an innovative method for identifying IoT botnets. Experimental result such as accuracy (97.6%), precision (98.01%), recall (97.5%), and F1 score (98.07%) which shows that our proposed method is superior in detecting IoT botnets. The intricate nature of this model's computational constraints may pose challenges in scaling for large datasets or real-time applications, especially due to the resource-intensive grid search process it employs. The computational constraints associated with grid search-driven gated recurrent units may be mitigated by the advancement of technology and algorithm optimization, leading to improved efficiency in the future.

References

1. Popoola, Segun I., Bamidele Adebisi, Ruth Ande, Mohammad Hammoudeh, Kelvin Anoh, and Aderemi A. Atayero. "smote-drnn: A deep learning algorithm for botnet detection in the internet-of-things networks." Sensors 21, no. 9 (2021): 2985. https://doi.org/10.3390/s21092985
2. Panda, Mrutyunjaya, A. Mousa Abd Allah, and Aboul Ella Hassanien. "Developing an efficient feature engineering and machine learning model for detecting IoT-botnet cyber attacks." IEEE Access 9 (2021): 91038-91052. https://doi.org/10.1109/ACCESS.2021.3092054
3. Pokhrel, Satish, Robert Abbas, and Bhulok Aryal. "IoT security: botnet detection in IoT using machine learning." arXiv preprint arXiv:2104.02231 (2021). https://doi.org/10.48550/arXiv.2104.02231
4. Alshamkhany, Mustafa, Wisam Alshamkhany, Mohamed Mansour, Mueez Khan, Salam Dhou, and Fadi Aloul. "Botnet attack detection using machine learning." In 2020 14th International Conference on Innovations in Information Technology (IIT), pp. 203-208. IEEE, 2020. https://doi.org/10.1109/IIT50501.2020.9299061
5. Hussain, Faisal, Syed Ghazanfar Abbas, Ivan Miguel Pires, Sabeeha Tanveer, Ubaid U. Fayyaz, Nuno M. Garcia, Ghalib A. Shah, and Farrukh Shahzad. "A two-fold machine learning approach to prevent and detect IoT botnet attacks." Ieee Access 9 (2021): 163412-163430. https://doi.org/10.1109/ACCESS.2021.3131014
6. Khan, Saad. "Lightweight deep learning framework to detect botnets in iot sensor networks by using hybrid self-organizing map." (2020). Maurya, Sandeep, Santosh Kumar, Umang Garg, and Manoj Kumar. "An efficient framework for detection and classification of iot botnet traffic." ECS Sensors Plus 1, no. 2 (2022): 026401. 10.1149/2754-2726/ac7abc
7. Lefoane, Moemedi, Ibrahim Ghafir, Sohag Kabir, and Irfan-Ullah Awan. "Machine learning for botnet detection: An optimized feature selection approach." In The 5th International Conference on Future Networks & Distributed Systems, pp. 195-200. 2021. https://doi.org/10.1145/3508072.3508102
8. Jung, Woosub, Hongyang Zhao, Minglong Sun, and Gang Zhou. "IoT botnet detection via power consumption modeling." Smart Health 15 (2020): 100103. https://doi.org/10.1016/j.smhl.2019.100103
9. Nguyen, Tu N., Quoc-Dung Ngo, Huy-Trung Nguyen, and Giang Long Nguyen. "An advanced computing approach for IoT-botnet detection in industrial Internet of Things." IEEE Transactions on Industrial Informatics 18, no. 11 (2022): 8298-8306. https://doi.org/10.1109/TII.2022.3152814
10. Al Shorman, Amaal, Hossam Faris, and Ibrahim Aljarah. "Unsupervised intelligent system based on one class support vector machine and Grey Wolf optimization for IoT botnet detection." Journal of Ambient Intelligence and Humanized Computing 11 (2020): 2809-2825. https://doi.org/10.1007/s12652-019-01387-y
11. Wei, Chongbo, Gaogang Xie, and Zulong Diao. "A lightweight deep learning framework for botnet detecting at the IoT edge." Computers & Security (2023): 103195.
12. Alqahtani, Mnahi, Hassan Mathkour, and Mohamed Maher Ben Ismail. "IoT botnet attack detection based on optimized extreme gradient boosting and feature selection." Sensors 20, no. 21 (2020): 6336. https://doi.org/10.3390/s20216336
13. Wazzan, Majda, Daniyal Algazzawi, Aiiad Albeshri, Syed Hasan, Osama Rabie, and Muhammad Zubair Asghar. "Cross Deep Learning Method for Effectively Detecting the Propagation of IoT Botnet." Sensors 22, no. 10 (2022): 3895. https://doi.org/10.3390/s22103895
14. Meidan, Yair, Michael Bohadana, Yael Mathov, Yisroel Mirsky, Asaf Shabtai, Dominik Breitenbacher, and Yuval Elovici. "N-baiot—network-based detection of iot botnet attacks

using deep autoencoders." IEEE Pervasive Computing 17, no. 3 (2018): 12-22. https://doi.org/10.1109/MPRV.2018.03367731

15. Kim, Ye-Eun, Min-Gyu Kim, and Hwankuk Kim. "Detecting IoT Botnet in 5G Core Network Using Machine Learning." Computers, Materials & Continua 72, no. 3 (2022). http://dx.doi.org/10.32604/cmc.2022.026581
16. Malik, Kainat, Faisal Rehman, Tahir Maqsood, Saad Mustafa, Osman Khalid, and Adnan Akhunzada. "Lightweight internet of things botnet detection using one-class classification." Sensors 22, no. 10 (2022): 3646. https://doi.org/10.3390/s22103646
17. Ngo, Quoc-Dung, Huy-Trung Nguyen, Hoang-Anh Tran, and Doan-Hieu Nguyen. "IoT botnet detection based on the integration of static and dynamic vector features." In 2020 IEEE Eighth International Conference on Communications and Electronics (ICCE), pp. 540-545. IEEE, 2021. https://doi.org/10.1109/ICCE48956.2021.9352145
18. Alkahtani, Hasan, and Theyazn HH Aldhyani. "Botnet attack detection by using CNN-LSTM model for Internet of Things applications." Security and Communication Networks 2021 (2021): 1-23. https://doi.org/10.1155/2021/3806459
19. Yang, Changjin, Weili Guan, and Zhijie Fang. "IoT Botnet Attack Detection Model Based on DBO-Catboost." Applied Sciences 13, no. 12 (2023): 7169. https://doi.org/10.3390/app13127169
20. Gharehchopogh, Farhad Soleimanian, Benyamin Abdollahzadeh, Saeid Barshandeh, and Bahman Arasteh. "A multi-objective mutation-based dynamic Harris Hawks optimization for botnet detection in IoT." Internet of Things 24 (2023): 100952. https://doi.org/10.1016/j.iot.2023.100952