EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Enhancing IoT Botnet Detection through Machine Learning-based Feature Selection and Ensemble Models

Ravi Sharma[1,*], Saika Mohi ud din[2], Nonita Sharma[2] and Arun Kumar[3]

[1]Department of Computer Science and Engineering, Dr. B. R. Ambedkar NIT, Jalandhar, Punjab, India
[2]Department of Information Technology, Indira Gandhi Delhi Technical University for Women, Kashmere Gate, Delhi, India
[3]School of Computer Science & Engineering (SCOPE), VIT-AP University, Amaravati, Andhra Pradesh, India

Abstract

An increase in cyberattacks has coincided with the Internet of Things (IoT) expansion. When numerous systems are connected, more botnet attacks are possible. Because botnet attacks are constantly evolving to take advantage of security holes and weaknesses in internet traffic and IoT devices, they must be recognized. Voting ensemble (VE), Ada boost, K-Nearest Neighbour (KNN), and bootstrap aggregation are some methods used in this work for botnet detection. This study aims to first incorporate feature significance for enhanced efficacy, then estimate effectiveness in IoT botnet detection using traditional model-based machine learning, and finally evaluate the outcomes using ensemble models. It has been demonstrated that applying feature importance increases the effectiveness of ensemble models. VE algorithm provides the best botnet traffic detection compared to all currently used approaches.

Keywords: IoT, Botnet, Botnet Detection, Ensemble Model, Voting Ensemble, Ada Boost, KNN, Bootstrap Aggregation

Received on 17 June 2023, accepted on 05 September 2023, published on 25 September 2023

doi: 10.4108/eetsis.3971

1. Introduction

Technology that relies on machine learning and the IoT is used in every facet of modern life [1]. As information-driven infrastructure spreads, there is an increase in research being done on machine learning (ML) based software for the IoT. Today, internet access is considered an essential requirement for everyone [2].

Because the data used in the IoT framework is so vulnerable, privacy measures must be used very carefully [3]. Unwanted vulnerabilities are being introduced because of the complexity of IoT systems increasing. IoT devices are a more apparent subject for attack since they communicate data through a wireless channel [4]. Unlike ordinary transmission attacks within the local system, limited to the nearby nodes or the boundaries of a local realm, IoT system assaults cover a more excellent range and have disastrous effects on IoT sites [5]. Specific data must be kept confidential and classified for government and private organizations. An attacker may access sensitive data from any major corporation due to flaws in IoT nodes [6].

Millions of linked devices might be under the control of a botnet simultaneously, launching devastating attacks that pose severe risks to the web [7]. IoT botnets are connected gadgets infected by malware [8]. One of the most significant cybersecurity threats is the use of botnets [9].

Since they serve as an essential base for many online crimes like malware distribution, phishing attacks, click stealing, and Distributed Denial of Services (DDoS) attacks against significant targets, botnets pose a severe and growing threat to cyber security. A handful of investigations in botnet studies have investigated the botnet issue despite the long history of fraudulent botnets [10].

*Corresponding author. Email: ravis.cs.19@nitj.ac.in

As a result, a secure IoT structure is needed for defense against cybercrime. This study uses ensemble models and conventional machine learning to find botnet assaults on IoT devices.

2. Related Work

Jullian et al. recommended an evolving distributed system utilizing deep learning (DL) for cyberattack detection [11]. The structure is based on assessing the Long Short-Term Memory (LSTM) and Feed Forward Neural Network (FFNN) computational models for the NSL-KDD and BoT-IoT data sets. FFNN achieves more excellent discovery rates for both samples.

Lee et al. [12] proposed an autonomous defensive system that can notice the existence of DDoS attacks on an IoT information server and identify the attack employing edge computing that incorporates a two-dimensional Convolutional Neural Network (CNN). The two-dimensional CNN's efficiency can achieve 99.5% for packet traffic and 99.8% for packet feature training.

On records like NSL-KDD along with UNSW-NB15, in which they assessed the binary and multiple classes attack groups using a neural network as well as machine learning approaches, Janardhana et al. [13] indicated different ML and deep learning methods for determining the presence of reliability and privacy-related obstacles in the IoT. The Recurrent Neural Network (RNN) model outperforms other models with high accuracy in recognizing threats with its efficacy in binary categorization (99.4%) and multiclass categorization (96.2%).

In their investigation, Alissa et al. [14] evaluated a range of ML algorithms for botnet identification, but the decision tree (DT) outscored them all with 94% accuracy.

Using the Bot-IoT and UNSW datasets, Alshamkhany et al. [15] used various models for attack detection, with the DT outperforming them all with a 99.89% accuracy rate.

To identify unusual network traffic, the ELBA-IoT ensemble learning approach, created by Haija & Al-Dala'ien [16], assesses the behavioral features of IoT networks. According to the study's findings, their proposed ELBA-IoT can identify botnet assaults conducted from impacted IoT devices with a high probability of identification (99.6%) and a low inference overhead (40 s).

Afrifa et al. [17] employed quantitative and qualitative methodologies in their investigation. They applied three core ML techniques— generalized linear model, random forest (RF), DT, and stacking ensemble model to detect botnets in computer network data. The results demonstrated that random forests performed best, with an R2 rating of 0.9977.

Srinivasan and Deepalakshmi [18] suggested an ensemble classifier coupled with a stacking procedure to choose the best attributes to be supplied to machine learning algorithms as input to assess the success of botnet identification. The advised method yields positive results with a 78.24% F-value, 86.5% sensitivity, 94.08% efficiency, and 85.68% specificity.

3. Proposed Methodology

This study uses ensemble models and ML to detect botnet attacks on IoT devices. The dataset's top 10 features are selected, and several machine learning algorithms are used. After trained on training datasets, the models are assessed on testing datasets. Feature significance has been applied to this dataset, and several ensemble models are utilized to increase productivity to reach the highest efficiency. In Figure 1, each step taken throughout the current investigation is described in detail. The BoT-IoT dataset was created at the UNSW Canberra Cyber Range Lab using a realistic network environment [19]. The network environment had both botnets and regular activities. The dataset includes keylogging, DDoS, Denial of Services (DoS) attacks, service scanning, and attacks on data exfiltration. The DDoS, as well as DoS attacks, are further organized based on the protocol used. In the study, models are applied and evaluated using the top 10 features from the dataset. The test and train sets of data are prepared, and a standard scaling is utilized for data scaling during the data preparation process. Different ML methods were suggested and evaluated for varying assault types. After feature significance is integrated into the dataset, ensemble models are applied to the processed data for even better efficacy.

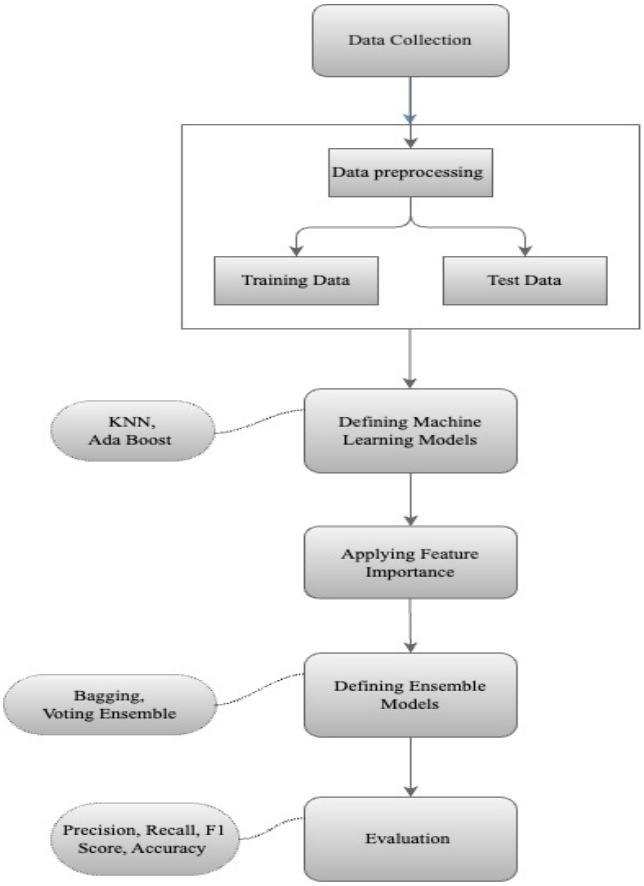

Figure 1. Proposed Methodology

3.1. Data Collection

The BoT-IoT dataset is used in this study to identify botnets. The top 10 features from the data set are used in this study to construct and test ML techniques. On various networks, there were 1541315 DDoS assaults, 1320148 DoS attacks, 72919 reconnaissance attacks, 370 ordinary data attacks, and 65 stealing attacks. Figure 2 shows the information regarding the data, where "pkSeqID" stands for row identifier, "proto" stands for network traffic, "sport" stands for source port number, "daddr" stands for destination IP address, "dport id" stands for destination port number, and "seq" stands for argus sequence number. The aggregated records' standard deviation is "stddev". "N_IN_Conn_P_SrcIP" represents the number of connections received per source IP, "min" is the minimum aggregate record duration, and "state_number" is the feature's numerical representation.

```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 733705 entries, 0 to 733704
Data columns (total 19 columns):
 #   Column             Non-Null Count   Dtype
---  ------             --------------   -----
 0   pkSeqID            733705 non-null  int64
 1   proto              733705 non-null  object
 2   saddr              733705 non-null  object
 3   sport              733705 non-null  object
 4   daddr              733705 non-null  object
 5   dport              733705 non-null  object
 6   seq                733705 non-null  int64
 7   stddev             733705 non-null  float64
 8   N_IN_Conn_P_SrcIP  733705 non-null  int64
 9   min                733705 non-null  float64
 10  state_number       733705 non-null  int64
 11  mean               733705 non-null  float64
 12  N_IN_Conn_P_DstIP  733705 non-null  int64
 13  drate              733705 non-null  float64
 14  srate              733705 non-null  float64
 15  max                733705 non-null  float64
 16  attack             733705 non-null  int64
 17  category           733705 non-null  object
 18  subcategory        733705 non-null  object
dtypes: float64(6), int64(6), object(7)
memory usage: 106.4+ MB
```

Figure 2. Data Information

4. Ensemble model

This study used a variety of ensemble and machine learning models, such as VE, Ada Boost, KNN, and Bagging, to identify the botnet attack on IoT devices. Some evaluation metrics used are accuracy, recall, precision, and F1 Score.

4.1. Evaluation Metrics

This research used the evaluation metrics below to identify botnets in an IoT network.

- Precision: Precision calculates how many favorable events were anticipated correctly. Equation 1 represents the accuracy.

$$\frac{TP}{TP + FP} \tag{1}$$

- Recall: Recall quantifies the percentage of exceptional events in the data the classifier accurately anticipated. The recall is represented by equation 2.

$$\frac{TP}{TP + FN} \tag{2}$$

- F1 Score: This measurement combines accuracy and recall. The F1 score is represented by equation 3.

$$2 * \frac{(Recall * Precision)}{(Recall + Precision)} \tag{3}$$

- Accuracy: Accuracy is the ratio of correctly classified data instances to all. Equation 4 stands for precision.

$$\frac{TP + TN}{TP + FP + FN + TN} \tag{4}$$

where, TP= True Positive, TN= True Negative,
FP= False Positive, FN= False Negative.

5. Experimental Results

This section will discuss the findings from the various approaches used to detect botnet attacks on the IoT network. Ensemble learning techniques are used to identify botnets in IoT based on the target traits of attack, category, and subcategory. It was found that ensemble models outperformed other models. VE put on outstanding performances. The class assault, category, and subcategory accuracy of the voting ensemble were all judged to be 0.99 and above. The multiple ML techniques are shown in Tables 1, 2, and 3, along with the outcomes for three distinct classes: Attack, Category, and Subcategory.

Table 1 presents the performance metrics of various machine learning algorithms when applied to classify attacks. These algorithms were evaluated using four important metrics: Precision, Recall, F1 Score, and Accuracy. Precision measures the proportion of true positive predictions among all positive predictions, emphasizing the model's ability to correctly identify attacks without making too many false alarms. Recall quantifies the model's ability to correctly capture all actual attack instances among all the true attacks. F1 Score combines both precision and recall into a single metric, providing a balanced measure of a model's

performance. Lastly, accuracy measures the overall correctness of the model's predictions. Ada Boost exhibited perfect precision among the algorithms evaluated, indicating it rarely misclassifies attacks, but its recall is relatively low. VE performed remarkably well across all metrics, particularly regarding precision and recall, suggesting a well-balanced trade-off between false positives and false negatives. KNN demonstrated respectable precision but lower recall. Bootstrap Aggregation displayed excellent precision and recall, implying it accurately identifies attacks while maintaining high precision.

Table 1. The outcome of different machine learning algorithms for class Attack

Models	Precision	Recall	F1	Accuracy
Ada Boost	1.00	0.68	0.76	1.00
Voting Ensemble	0.99	0.99	0.99	0.99
KNN	0.96	0.65	0.73	1.00
Bootstrap Aggregation	1.00	0.86	0.92	1.00

Table 2 displays the performance of different ML algorithms for classifying data, as assessed using key metrics: Precision, Recall, F1 Score, and Accuracy. Ada Boost balances precision and recall with an accuracy of 96%, indicating its reliability in classifying categories. VE outpaces other models with impressive precision, memory, and F1 scores of 98%, 99%, and 98%, respectively, proving its ability to identify categories appropriately. KNN shows moderate performance, with an accuracy of 78% and reasonably balanced precision and recall scores. Bootstrap Aggregation performs well in precision and recall, demonstrating its ability to categorize categories accurately while maintaining high precision. Generally, these results highlight the strengths and weaknesses of each algorithm in classifying categories, with VE and Bootstrap Aggregation demonstrating superior performance.

Table 2. The outcome of different machine learning algorithms for class Category

Models	Precision	Recall	F1	Accuracy
Ada Boost	0.78	0.63	0.66	0.96
Voting Ensemble	0.98	0.99	0.98	0.99
KNN	0.82	0.70	0.74	0.78
Bootstrap Aggregation	0.99	0.87	0.92	1.00

Table 3 highlights the performance of various ML algorithms when categorizing data into subcategories. The results show that Ada Boost attains a relatively high precision but lower recall, while VE shows exceptional performance with perfect precision, recall, F1 Score, and accuracy. KNN performs moderately, with a balanced F1 Score and accuracy but slightly lower precision and recall. Bootstrap Aggregation also performs well, with high precision, recall, F1 Score, and perfect accuracy. Overall, these results highlight each algorithm's varying strengths and weaknesses in classifying subcategories, with VE and Bootstrap Aggregation standing out as powerful performers.

Table 3. The outcome of different machine learning algorithms for class subcategory

Models	Precision	Recall	F1	Accuracy
Ada Boost	0.82	0.44	0.44	0.99
Voting Ensemble	1.00	1.00	1.00	1.00
KNN	0.73	0.67	0.70	0.81
Bootstrap Aggregation	0.97	0.94	0.95	1.00

The efficiency of several methods for identifying botnets is shown in Figure 3 for three distinct classes: attack, category, and subcategory. In identifying botnets, it was discovered that the ensemble approach, i.e., VE, performed better than other machine learning models.

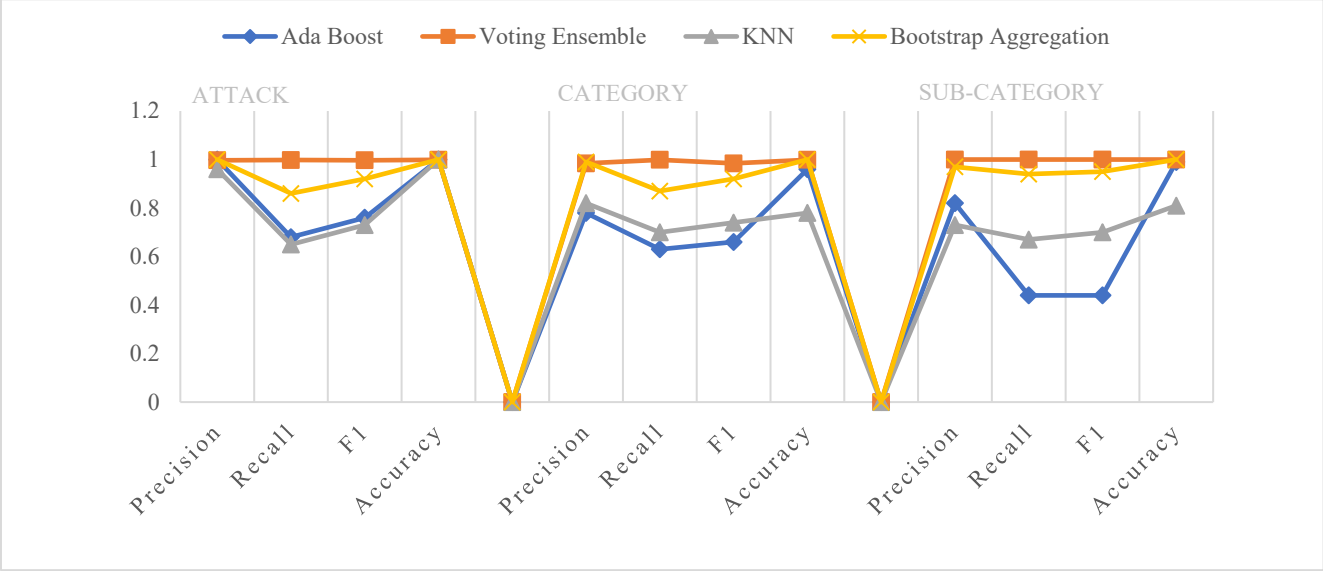

Figure 1. Comparison of different algorithms

6. Conclusion

In this study, botnet attacks on IoT devices are found using ensemble models and conventional machine-learning approaches. To improve effectiveness, feature importance analysis was used for the dataset. It was demonstrated that ensemble models surpassed traditional machine learning methods regarding efficiency and precision when characteristics were considered. Voting ensemble functions astonishingly effectively for botnet detection in IoT networks. As a result, the ensemble models used in this study were successful.

In the future, we plan to use additional datasets and algorithms in this work to evaluate the efficiency of identifying a botnet attack in IoT.

References

[1] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet of Things*, vol. 7, p. 100059, Sep. 2019, doi: 10.1016/J.IOT.2019.100059.

[2] A. Shahid, M. Z. Jasni, Z. Mohamad Fadli, and I. Zakira, "A Review Paper on Botnet and Botnet Detection Techniques in Cloud Computing," 2014, Accessed: May 03, 2023. [Online]. Available: https://www.researchgate.net/profile/Shahid_Anwar3/publication/283257776_A_Review_Paper_on_Botnet_and_Botnet_Detection_Techniques_in_Cloud_Computing/links/562f525308ae4742240abea7.pdf

[3] SharmaRavi and SharmaNonita, "Attacks on Resource-Constrained IoT Devices and Security Solutions," *International Journal of Software Science and Computational Intelligence (IJSSCI)*, vol. 14, no. 1, pp. 1–21, Oct. 2022, doi: 10.4018/IJSSCI.310943.

[4] X. Liu, Y. Liu, A. Liu, and L. T. Yang, "Defending ON-OFF attacks using light probing messages in smart sensors for industrial communication systems," *IEEE Trans Industr Inform*, vol. 14, no. 9, pp. 3801–3811, Sep. 2018, doi: 10.1109/TII.2018.2836150.

[5] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, and K. K. R. Choo, "A Two-Layer Dimension Reduction and Two-Tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks," *IEEE Trans Emerg Top Comput*, vol. 7, no. 2, pp. 314–323, 2019, doi: 10.1109/TETC.2016.2633228.

[6] I. K. Poyner and R. S. Sherratt, "Privacy and security of consumer IoT devices for the pervasive monitoring of vulnerable people," *IET Conference Publications*, vol. 2018, no. CP740, 2018, doi: 10.1049/CP.2018.0043.

[7] S. Al-mashhadi, M. Anbar, I. Hasbullah, and T. A. Alamiedy, "Hybrid rule-based botnet detection approach using machine learning for analysing DNS traffic," *PeerJ Comput Sci*, vol. 7, pp. 1–34, 2021, doi: 10.7717/PEERJ-CS.640/SUPP-4.

[8] A. Kumar *et al.*, "A Novel Decentralized Blockchain Architecture for the Preservation of Privacy and Data Security against Cyberattacks in Healthcare," *Sensors*, vol. 22, no. 15, Aug. 2022, doi: 10.3390/S22155921.

[9] R. A. Rodriguez-Gomez, G. Macia-Fernandez, and P. Garcia-Teodoro, "Survey and taxonomy of botnet research through life-cycle," *ACM Computing Surveys (CSUR)*, vol. 45, no. 4, Aug. 2013, doi: 10.1145/2501654.2501659.

[10] M. Feily, A. Shahrestani, and S. Ramadass, "A survey of botnet and botnet detection," *Proceedings - 2009 3rd International Conference*

on Emerging Security Information, Systems and Technologies, SECURWARE 2009, pp. 268–273, 2009, doi: 10.1109/SECURWARE.2009.48.

[11] O. Jullian, B. Otero, E. Rodriguez, N. Gutierrez, H. Antona, and R. Canal, "Deep-Learning Based Detection for Cyber-Attacks in IoT Networks: A Distributed Attack Detection Framework," *Journal of Network and Systems Management*, vol. 31, no. 2, pp. 1–24, Apr. 2023, doi: 10.1007/S10922-023-09722-7/FIGURES/8.

[12] C.-H. ; Cheng *et al.*, "Detection and Prevention of DDoS Attacks on the IoT," *Applied Sciences 2022, Vol. 12, Page 12407*, vol. 12, no. 23, p. 12407, Dec. 2022, doi: 10.3390/APP122312407.

[13] D. R. Janardhana, V. Pavan Kumar, S. R. Lavanya, and A. P. Manu, "Detecting Security and Privacy Attacks in IoT Network using Deep Learning Algorithms," *2021 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics, DISCOVER 2021 - Proceedings*, pp. 35–40, 2021, doi: 10.1109/DISCOVER52564.2021.9663586.

[14] K. Alissa, T. Alyas, K. Zafar, Q. Abbas, N. Tabassum, and S. Sakib, "Botnet Attack Detection in IoT Using Machine Learning," *Comput Intell Neurosci*, vol. 2022, 2022, doi: 10.1155/2022/4515642.

[15] M. Alshamkhany, W. Alshamkhany, M. Mansour, M. Khan, S. Dhou, and F. Aloul, "Botnet Attack Detection using Machine Learning," *Proceedings of the 2020 14th International Conference on Innovations in Information Technology, IIT 2020*, pp. 203–208, Nov. 2020, doi: 10.1109/IIT50501.2020.9299061.

[16] Q. A. Al-Haija and M. Al-Dala'ien, "ELBA-IoT: An Ensemble Learning Model for Botnet Attack Detection in IoT Networks," *Journal of Sensor and Actuator Networks 2022, Vol. 11, Page 18*, vol. 11, no. 1, p. 18, Mar. 2022, doi: 10.3390/JSAN11010018.

[17] S. Afrifa, V. Varadarajan, P. Appiahene, T. Zhang, and E. A. Domfeh, "Ensemble Machine Learning Techniques for Accurate and Efficient Detection of Botnet Attacks in Connected Computers," *Eng*, vol. 4, no. 1, pp. 650–664, Feb. 2023, doi: 10.3390/ENG4010039.

[18] S. Srinivasan and D. P, "Enhancing the security in cyber-world by detecting the botnets using ensemble classification based machine learning," *Measurement: Sensors*, vol. 25, p. 100624, Feb. 2023, doi: 10.1016/J.MEASEN.2022.100624.

[19] "The Bot-IoT Dataset | UNSW Research." https://research.unsw.edu.au/projects/bot-iot-dataset (accessed Apr. 16, 2023).