2022 IEEE 11th International Conference on Communication Systems and Network Technologies (CSNT) | 978-1-6654-8038-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/CSNT54456.2022.9787583

A Productive Feature Selection Criterion for Bot-IoT Recognition based on Random Forest Algorithm

R. Pavaiyarkarasi[1], T. Manimegalai[2], S Satheeshkumar[3], K. Dhivya[4], G. Ramkumar[5]
[1]Assistant Professor, Department of ECE, R.M.K. Engineering College, Thiruvallur, Chennai
[2]Associate Professor, School of Computer Science and Engineering, Vellore Institute of Technology, Chennai.
[3]Assistant Professor, Department of ECE, Excel Engineering College, Komarapalayam.
[4]Assistant Professor, Department of ECE, R.M.K. College of Engineering and Technology, Puduvoyal, Chennai.
[5]Associate Professor, Department of ECE, Saveetha School of Engineering, SIMATS, Chennai.
[1]rpi.ece@rmkec.ac.in, [2]megalasen@gmail.com, [3]mariarubiston@saec.ac.in, [4]dhivyakece@rmkcet.ac.in,
[5]ramkumarg.sse@saveetha.com

Abstract—For IoT security to function properly, it is necessary to identify anomalies and suspicious activities in the Internet of things (IoT) network in order to keep an eye on things and stop undesired traffic flows in the IoT network. A large number of machine learning (ML) approach models have been suggested by many scholars to restrict fraudulent traffic flows in the Internet of Things network in order to achieve this goal. However, as a result of insufficient feature selection, several machine learning models are vulnerable to misclassifying mainly malicious traffic flows. Nonetheless, a key topic that should addressed in greater depth, and that is how to choose useful features for reliable mischievous traffic identification in an Internet of Things network, which is now being investigated. A framework is designed in order to deal with the issue. After developing and designing a novel feature selection metric strategy that relies on wrapper method to precisely filter the features, we then utilised a random forest algorithm for harmful traffic detection in an Internet of Things network to identify malicious traffic. On the basis of the Bot-IoT database, we assess the effectiveness of our suggested strategy. The examination of exploratory findings proofed that our suggested strategy is efficient and can produce output in excess of 96 percent of cases.

Index Terms — Internet of Things, Malicious, Identification, Machine Learning, Random forest algorithm, Feature selection.

I. INTRODUCTION

With each passing day [1] the Internet of Things (IoT) technology is becoming increasingly popular, with a rising number of devices being linked to it every minute. Everyday life becomes more comfortable and well-organized as a result of the use of this technology. For example, initially, Internet of Things (IoT) technology was restricted to tiny organizations and residences; but, today, IoT technology is being blended into industries to improve dependability and save time. However, Internet of Things (IoT) technology is quickly becoming a necessary component of our daily lives. In 2021, the IoT technology will mature, and more than 27 million IoT devices will be connected, resulting in a significant shift in the world of IoT technology [2]. Although IoT technology is improving with each passing day, cyber-attacks are becoming more difficult to detect and more frequent. In order to do this, a large number of researchers in the field of Internet of Things technology offered several different cyber security systems, and the recommended cyber security system was extensively used in order to safeguard their data from cyber-attacks and illegal access. It has currently become a popular topic in IoT cyber security and has received a great deal of media attention. For the purpose of overcoming the challenge of Internet of Things cyber-attacks, scholars have attempted to devise a variety of cyber security measures. In a similar vein, several cyber security systems for Internet of Things networks are offered and implemented for the protection of sensitive data and the prevention of illegal access to the IoT network. Attacks against IoT, such as Denial of Service (DDoS), have been increasingly prevalent in recent years, with an increase of up to 172 percent in 2017 [2], indicating a significant attention in IoT networks.

Kaspersky Lab published a paper in 2019 [3] stating that malicious attacks in the IoT network which rose in 2017 when contrasted to malicious traffic assaults in the IoT network environment . Nevertheless, among these constant attacks, the majority of them are very destructive strikes such as Botnet attacks and other similar attacks [4]. Man in the middle (MITM) significant threats with distributed denial-of-service (DDoS) are currently the most serious and challenging pervasive hazardous threats in the Internet of Things (IoT) [5][6]. However, a huge number of scholars in the research community made every effort to identify and propose a solution that would be effective in combating

978-1-6654-8038-3/22/$31.00 ©2022 IEEE
DOI: 10.1109/csnt.2022.94

these widespread and dangerous risks in the IoT environment.

Earlier this year, Alharbi S et al. [7] suggested a fresh technique for the detection of malicious cyber-attacks and the protection of the IoT from cyber-attacks, which they termed the FOCUS. It was discovered that their suggested intrusion detection system [8] made use of a VPN service for secure communication among IoT devices. However, their suggested approach is productive in terms of protecting against prospective cyber threats and is capable of safeguarding the Internet of Things system. Furthermore, they train and test system in fog computing and were able to achieve positive outcomes. They demonstrated that their designed system is successful for the identification of dangerous cyber-attacks while operating at a low reaction time and with limited bandwidth availability. Machine Learning (ML) and Artificial Intelligence (AI) techniques, on the other hand, are useful and frequently used for achieving the best outcomes and most subsequent detection possible.

The significant characteristics selected for the ML model is quite critical for proper identification in the ML model. Effective features are precise features or qualities that retain relevant data for machine learning techniques, and this set of effective features contains both training and a testing set of effective features. A machine learning model cannot be evaluated unless it has been trained on and tested on a large number of data points. As a result, for the evaluation of the ML model, it is necessary to have a meaningful features set of training and testing sets. The machine learning model is commonly used in computer science, particularly in the detection of network traffic [9]. Techniques such as machine learning can be extremely beneficial in recognising or categorising hostile, incursion, and cyber-attacks in Internet of Things networks. When it comes to the identification and categorization of harmful traffic from cyber-attacks, implementing the machine learning method is useful; nevertheless, when contrasted to other computer tools, the ML methodology tool can be highly difficult. Despite the fact that machine learning is extremely useful in the areas of identification and classification, it is not always the case. Although there are certain benefits to IoT malicious and intrusion detection, there are also some limitations, such as issues with computation time and usage of energy. These two problems are recently a big topic in the Internet of Things sector, and various academics are working hard to find solutions to these issues that keep cropping up in the industry. The accuracy of recognition ML model for raw datasets is critical for improving outcomes and overcoming the issues highlighted in this section. It is not impossible to obtain high-performance outputs and to accurately implement the machine-learning methods for Bot Detection.

As part of our prior research [11], [12], and [13], we looked at feature selection difficulties for Instant Message traffic classification and assault traffic recognition, and we proposed several different sorts of methodologies for selecting robust features. Likewise, in [9], multiple feature selection strategies are suggested for the efficient identification of network traffic using machine learning techniques in order to address the difficulty of feature selection issue. In the above study, we found that choosing a bigger number of attributes sets is inefficient for precise recognition when using machine learning techniques. We also discovered that picking over 50 features sets can reduce the precision of the ML classifier and enhance the complexity of the algorithm. The recognition of Bot in the IoT network, on the other hand, has yet to be solved using an effective machine learning model. As a result, it is critical to investigate the problem of reliable in the Internet of Things network and to develop a novel method for overcoming this challenge.

For cyber-attacks on Wireless network activity, a reliable attribute selection mechanism has been developed in this study, which is based on the Bot-IoT dataset, and it is shown to increase the efficiency of machine learning algorithms in the process. However, the following are the most significant contributions made in this paper:

- In order to deal with the right attribute selection difficulty in IoT, cyber threats must be recognised in the IoT environment. A strategy to feature selection using metrics is first developed to tackle the issues of appropriate attribute selection for cyber attacks recognition, which is addressed in the following sections. However, a combo of correlation feature assessment metric and particular ML AUC resulted in the most successful feature selection in the recognition of IoT assaults in the IoT environment.
- Following that, we used Shannon Entropy to validate the attributes for suspicious network recognition in the Internet of Things network. Because of the choosing of appropriate features to improved recognition of brutal attacks in the IoT network, it is based on the IoT network. Also included are comparisons between the results of Shannon Entropy and the results performance of proposed approach.
- In the end, we came to a decision and offered the best possible feature set for identifying dangerous Bots in the network based on our recommended strategy. Results showed that using machine learning to identify hazardous attacks on IoT networks; the five best selected features provide enough data and discriminative strength.

The following is how the following section is organised: Section 2 contains works that are related to the Methods. In Section 3, we describe the techniques that have been offered. While in Section 4, we go into the experimentation work, and dataset that was used in this study in depth. Section 5 provides analysis and debate, in the same way as Section 4.

Finally, Section 6 summarises the paper's findings and provides suggestions for future research.

II. Related Study

Since the previous decade, security and privacy issues have become a hot concern, and many researchers have worked tirelessly to find solutions. They have offered various viable models, including the future Internet [14], and IoT [15,16]. A few of the most widely-viewed and quoted papers relating to attribute selection for harmful Bot's in networks are reviewed in this part, as are some of its implications. Recent research [9] proposes a feature selection strategy based on mutual information (MI) assessment for the maximum feature selection challenge in IM applications traffic categorization. In contrast, the suggested approach produces favourable performance outcomes by utilising the selected attributes set for the recognition of IM traffic, according to the findings of the experimental studies conducted. More specifically, the research was restricted to selecting feature for a variety of applications, as well as the reduction of the computational burden of the ML algorithms that were used. The proposed approach is capable of being applied to a data collection with imbalance or high dimensionality. The experimental results demonstrated that the suggested method may obtain favourable results for the identification of IM application when used to real-time messaging applications. The approach of feature selection comes in help when it comes to improving the performance of machine learning algorithms. However, selecting feature is a process that involves selecting the best set of features from a bigger number of features sets and deleting the characteristics that do not carry sufficient identification information that are redundant. It can be done manually or automatically. IN 2018 [17], SEgea et al. researched the majority of the scientific related studies to feature selection (FS) method, specifically the correlation coefficient technique, and proposed FCBF algorithm for the betterment of IoT network's performance in the industrial environment. One of the most important contributions of their research is to divide the feature space into numerous equal portions of equal size, which is their primary contribution. They demonstrated improved correlation ML results for every running node in the Internet of Things network by employing this approach. In their experiments, they demonstrated that their results were effective, and that the proposed approach was capable of achieving reliable performance output in terms of accuracy and executing time, both of which are critical for correct identification results. In a similar vein, in 2018, MeidanYair at el. [18] investigated the tracking of attacks in networks and announced a method to solve the challenges of attacks that are started by IoT devices. They deployed autoencoder as a data compression algorithm. However, the datasets that were used are also present on a number of compromised devices that are part of the IoT network. Additionally, for Internet of Things devices, performance enhancement, and anomaly detection, Shen Su and colleagues [19] investigated the most frequently mentioned feature selection methods and developed a feature selection method. In order to identify the sensors that have been deployed, they first combine the IoT sensors together as a group in their study. After that, in order to detect anomalies, they regulate the correlation fluctuation of data in order to select the appropriate sensors. More specifically, they used the curve alignment technique for the clustering of sensors, and the size of the calculation window for the data is explored in further detail. MCFS approach is then used to pick the features that will be used in the final product. According to their experimental findings, their suggested method is reliable for BoT detection in the networks, and they want to further develop it. Numerous IoT security techniques can be used to achieve precise cyber security goals in an IoT security environment, for example cyber-attack recognition in [20, 21], an appropriate management scheme, an evidence framework and other techniques. In any case, while the different methodologies recommended by numerous scholars are beneficial, it is critical to select the attribute set that contains reliable data for the Bot attack recognition.

III. Methodology

In this section, we will go over the novel approach in depth and step by step demonstrations. Our proposed strategy, as seen in Fig.1, consists of four steps that are essential for effective selection in an IoT network. Initially, selecting feature is performed, which selects features that contain sufficient amount of information to be useful. To precisely filter the features, the wrapper technique is utilised, and the random forest algorithm is applied to the Bot-IoT dataset. After that, we used Shannon Entropy to check the features selected for Bot assaults in the network, which was then used to identify Bot-IoT attacks traffic. Bot - IoT attack detection in the IoT network environment is made possible by using this method, which yields extremely successful outputs in terms of reliable feature selection. Furthermore, our suggested method selects a feature set that has sufficient identity data for Bot assaults in an IoT network, which is important. In order to provide a clear understanding, the specific approaches for the selecting feature in IoT networks, taking into consideration Bot-IoT malicious assaults detection, are addressed in the following section.

In this subsection, the proposed methods are described in depth, as seen in Figure.1. As a first step, the correlation-based metric scheme utilizes a correlation method to refine the feature set and determine the connection among attributes and class which will use the random forest technique, to filter out the attributes which have better AUC metric values. To put it another way: in an IoT network, the proposed method identifies the useful features that include sufficient information for Bot-IoT identification. Bot attacks

are detected in IoT networks using a combined selection in feature method and area under the curve metric. The algorithm selects features that have sufficient data for recognition of Bot assaults in IoT networks.

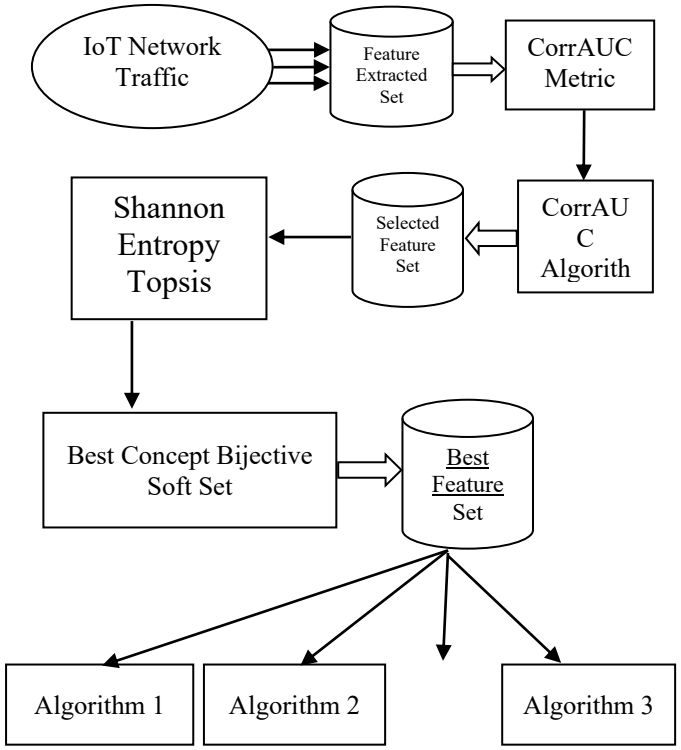

Fig. 1: Suggested Framework for Selecting features

The suggested methodology, on the other hand, first calculates the relation among features and then selects those features that have a strong correlation among them. Further in-depth, the system will initially compute the relation between features, after which the features will be arranged in ascending order according to their correlation values. After that, the programme looked at the relationship between each feature. After that, a fixed value is designated, and if the correlation values are better than the set threshold value, it indicates that the attribute is reliable, and the feature is then placed first in the descending order of effectiveness. The random forest approach will be implemented after the correlation coefficients have been calculated and the threshold values have been set. When it comes to IoT network Bot assaults, the algorithm examines each parameter using the AUC metric, then choose attributes AUC values. In this scenario, the Swapper approach will delete an attribute from the collection if its AUC values fall below a certain threshold.

Shannon Entropy is used to identify Bot assaults in IoT network environments, and it is used to choose the most effective features for detection. After the suggested selection methods of features, a decision-making method is deployed to address the problems of effective selection in feature, which helps to solve the difficulty. It is critical to validate the developed feature selection strategy before using it. So we utilize a technique called CDM to choose a strong attribute set for Bot-IoT threat detection in the Internet of Things network environment. Likewise, we employ the similar strategy for selecting reliable features from a large number of features in this study.

Algorithm 1: Selecting feature based on correlation along with AUC:

Input: E (G_1, G_2, G_3, …… G_n)//training data set,
Output: feature [ ]

1. begin
2. For j = 1 to L
3. Finding correlation value;
4. Finish for
5. for j = to L;
6. calculate Corr (G_i);
7. if (Corr(G) > δ);
8. arrange G_i into descending order;
9. finish if
10. finish for
11. G_p = get initial attribute (list);
12. finish until (G_p== Null);
13. Y is a sample value of dataset
14. Last_AUC ← classify Y;
15. Load the attribute into Swrapper;
16. attribute = get next attribute;
17. For attribute!= Null
18. Load the feature into Swrapper;
19. Y is a dataset sample for Swrapper;
20. AUC ← classify Y with a classifier;
21. if (AUC <= last_AUC)
22. Eliminate attribute from Swrapper;
23. else
24. attribute = find Next attribute (list, attribute);
25. finish if
26. finish for

Return Swrapper;

Fig 2: Proposed Corrauc algorithm

IV. RESULTS AND DISCUSSIONS

DataSet

A newly developed dataset [10], [22] is used for relative selection of feature and precise Bot assaults recognition in the Internet of Things network environment. The database includes information on the Internet of Things, as well as typical traffic flows, as well as a large number of cyber-attacks issues, such as botnets attacks, among other things [23]. The construction of this database with useful information features is carried out on a realistic test bed, which allows for the correct tracking of traffic and the implementation of an effective dataset. In a similar vein, in order to enhance the performance of machine learning

models and the effectiveness of prediction models, extracting new features and combined with the features set which is extracted. However, labelling the extracted features is done in order to achieve better performance results. There are three sub-components to the testbed that are used. In a similar vein, five Internet of Things devices are used to simulate IoT devices, such as an Internet of Things device that develop meteorological data every minute, allowing users to know the present temperature, humidity, and pressure of atmosphere, among other things.

Performance Measurements

Confusion metrics is based on the assessment of achievement, are extensively used for the evaluation of the identification effectiveness of a machine learning model outcome. Various measurement measures, based on the metrics described above, can be developed in order to better analyse a machine learning model, as seen in the following example. Machine learning classifiers strive to decrease the number of false positive and false negative metrics values in order to achieve accurate detection. Nevertheless, the following are the metrics selected that were employed in this research, as explained in greater detail below:

- **Accuracy**: In the context of assaults identification, it can be defined as the proportion of successfully identified samples of traffic in the total amount of successfully identified samples traffic. Accuracy can be mathematically defined as follows, however, when performance assessment metrics are utilised:

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

- **Precision:** The properly recognised sample expressed as a percentage of all those which classified rightly as belonging to Class A. The mathematical formula that was employed in this study investigation is shown in the following section.

$$Precission : \frac{TP}{(TP + FP)}$$

- **Sensitivity:** It can be described as the no of successfully detected traffic samples divided by the total no of traffic samples in the dataset. For the sensitivity metric, we employed the mathematical formula that was provided to us, as shown below.

$$Sensitivity : \frac{TP}{(TP + FN)}$$

- **Specificity:** Specifically, we used specificity measures in our research project, which may be described as the potential of a machine learning classifier to identify negative results.

$$Specificity : \frac{TN}{(FP + TN)}$$

Nevertheless, for the suggested concept's evaluation process, we employed the indicators listed above.

The comprehensive outcomes and evaluation of the proposed methodology are explained in more detail in this section. In this research, we suggested a new approach for recognising Bot assaults in the IoT network environment, which we tested in the real world. For the purpose of selection in feature, our suggested technique chose only 5 reliable characteristics, each of which contains adequate data for the identification of Bot attacks in the network. A total of four distinct ML techniques are deployed for the analysis of the proposed technique, including the DT, SVM, NB, and RF algorithms. This is done in order to choose the most effective features. When using the features set chosen by our suggested methodology, the accuracy, precision, sensitivity, and specificity of the methodologies vary. Nevertheless, when employing the given features set for Bot attack recognition, the effectiveness of Naive Bayes is inferior to that of other machine learning techniques, as measured by the accuracy metric. As demonstrated in Fig. 4, the performance result of SVM classifiers is marginally better than that of Nave Bayes classifiers in terms of efficiency when contrast to the latter. Random Forest method, on the other hand, produce favourable performance results in terms of accuracy. Because of this, the Random Forest algorithm outperforms the competition when employing the selected characteristics set for the recognition of Bot assaults by 99.7%, which is extremely effective in terms of overall performance. The comprehensive results chart for accuracy, on the other hand, is provided in Fig.4.

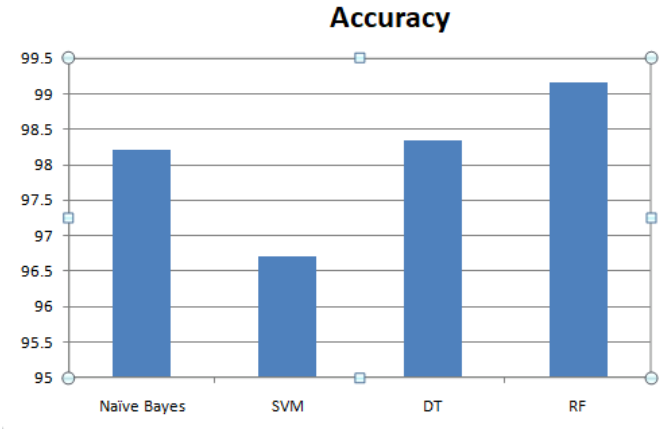

Fig. 4: Accuracy Results

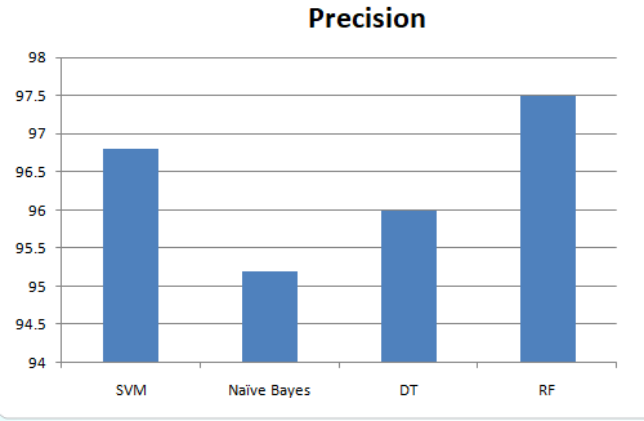

Fig. 5: Precision Results

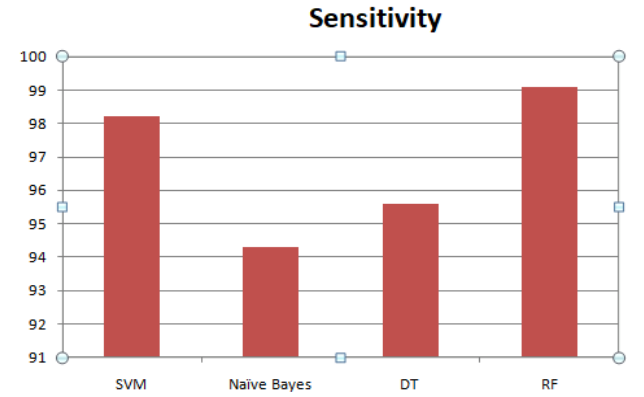

Fig. 6: Sensitivity Results

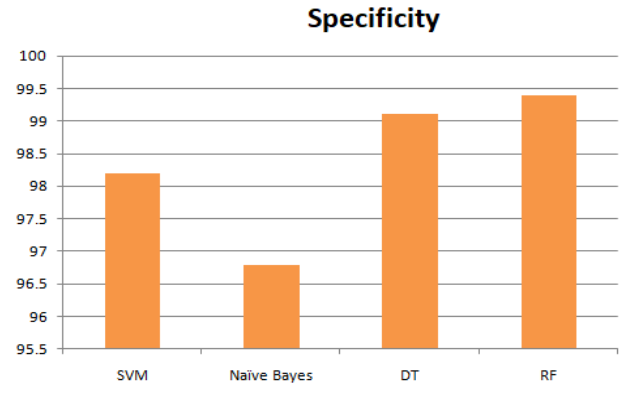

Fig. 7: Specificity Results

The comprehensive precision result is depicted in Figure 5. When comparing the Random Forest algorithm to the SVM and Naive Bayes algorithms, it is clear that the Random Forest approach achieves superior performance outcomes. When the performance of each ML classifier is averaged, the findings are quite different. In comparison to other regular and other attacks employing the features chosen and their related precision, only Key Logging Theft traffic was discovered at a low rate. Performance findings for all four of the applied machine learning classifiers are quite effective in terms of sensitivity metrics. By applying the selected features set, Random Forest, in comparison to other applicable ML classifiers achieves exceptionally high-performance results. As demonstrated in Fig.6, the SVM and Naive Bayes ML classifiers have poor outcomes when contrast to the DT and RF classifiers when using the sensitivity metric, which is the same as the accuracy and precision metrics. When it comes to specificity, the entire imposed machine learning algorithms produces very impactful results. For example, the decision tree and the Random Forest produce performance results of 98.95 percent and 99.99 percent, respectively, which are both very effective good results when it comes to the respective specificity metric. Additionally, by utilising the selected feature set, all assaults and routine traffic are recognised with high fidelity. As a result of the foregoing research, it is obvious that our suggested selection method is better for the selection of characteristics for the detection of Bot in the Internet of Things environment.

V. Conclusion and Future Scope

The identification of intrusions in the Internet of things (IoT) network is important for IoT security since it allows the network to keep an eye on things and restrict undesired data flows. Lot of academics have proposed a different machine learning (ML) approach models in order to restrict attack traffic flows in the Internet of Things network. However, as a result of insufficient feature selection, several machine learning algorithms are prone to misclassifying predominantly harmful traffic flows. Despite this, there is still one important problem that has to be researched further: how to identify helpful attributes for efficient malicious traffic identification in Internet of Things networks. A new mechanism is developed in order to achieve this goal. The first stage is to design and build an attribute selection measurement that uses a wrapper approach to properly filter variables and choose relevant attributes for the ML algorithm, which is then assessed using the AUC metric. Once we had selected features for malicious traffic identification in IoT networks validated, we used Shannon Entropy to see if they were still valid. The Bot-IoT dataset, as well as four alternative machine learning methods, are used to test our suggested strategy. The results of the experiments demonstrated that our recommended technique is effective, and the Random Forest Algorithm achieved a 98 recognition rate utilising the data.

REFERENCES

[1] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, “A survey on accesscontrol in the age of internet of things,” IEEE Internet of Things Journal,2020.

[2] Anitha et al (2021) “Experimental Analysis of Secured Routing Protocol Establishments Over Wireless Sensor Network” 2021 5th International Conference on Trends in Electronics and Informatics

(ICOEI), 2021, pp. 691-698, doi: 10.1109/ICOEI51242.2021.9452857.

[3] K. Lab. (2019) Amount of malware targeting smart devices morethan doubled in. [Online]. Available: https://www.kaspersky.com/about/press-releases/2017_amount-of-malware

[4] Amirthalakshmi. et al. (2021). "A Novel Approach in Hybrid Energy Storage System for Maximizing Solar PV Energy Penetration in Microgrid", International Journal of Photoenergy, Volume 2022, Article ID 3559837, 7 pages, https://doi.org/10.1155/2022/3559837.

[5] L. Wu, X. Du, W. Wang, and B. Lin, "An out-of-band authentication scheme for internet of things using blockchain technology," in 2018 International Conference on Computing, Networking and Communications(ICNC). IEEE, 2018, pp. 769–773.

[6] Z. Tian, X. Gao, S. Su, and J. Qiu, "Vcash: A novel reputation framework for identifying denial of traffic service in internet of connected vehicles," IEEE Internet of Things Journal, vol. 7, no. 5, pp. 3901–3909, May 2020.

[7] S. Alharbi, P. Rodriguez, R. Maharaja, P. Iyer, N. Bose, and Z. Ye, "Focus: A fog computing-based security system for the internet ofthings," in 2018 15th IEEE Annual Consumer Communications &Networking Conference (CCNC). IEEE, 2018, pp. 1–5.

[8] Z. Tian, C. Luo, J. Qiu, X. Du, and M. Guizani, "A distributed deep learning system for web attack detection on edge devices," IEEE Transactions on Industrial Informatics, 2020. Vol 16(3): 1963-1971.

[9] M. Shafiq, X. Yu, A. K. Bashir, H. N. Chaudhry, and D. Wang, "A machine learning approach for feature selection traffic classification using security analysis," The Journal of Supercomputing, vol. 74, no. 10,pp. 4867–4892, 2018.

[10] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towardsthe development of realistic botnet dataset in the internet ofthings for network forensic analytics: Bot-iot dataset," arXiv preprintarXiv:1811.00701, 2018.

[11] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "Iot malicioustraffic identification using wrapper-based feature selection mechanisms," Computers& Security, p. 101863, 2020.

[12] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, "Selection ofeffective machine learning algorithm and bot-iot attacks traffic identification for internet of things in smart city," Future Generation Computer Systems, vol. 107, pp. 433–442, 2020.

[13] M. Shafiq, Z. Tian, A. K. Bashir, A. R. Jolfaei, and X. Yu, "Datamining and machine learning methods for sustainable smart cities traffic classification: A survey," Sustainable Cities and Society, 2020.

[14] Z. Tian, S. Su, W. Shi, X. Du, M. Guizani, and X. Yu, "A data-driven method for future internet route decision modeling," Future Generation Computer Systems, vol. 95, pp. 212–220, 2019.

[15] Z. Tian, X. Gao, S. Su, J. Qiu, X. Du, and M. Guizani, "Evaluating reputation management schemes of internet of vehicles based on evolutionary game theory," IEEE Transactions on Vehicular Technology,2019. 68(6): 5971-5980.

[16] Tripti Sharma, Brijesh Kumar, G.S. Tomar, "An Efficient Condensed Cluster Stable Election Protocol in Wireless Sensor Networks", International Journal of Smart Device and Appliance Vol.1, No.1 pp 17-28, Dec 2013.

[17] S. Egea, A. R. Mañez, B. Carro, A. Sánchez-Esguevillas, and J. Lloret,"Intelligent iot traffic classification using novel search strategy for fast based-correlation feature selection in industrial environments," IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1616–1624, 2018.

[18] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, "N-baiotâ˜A ˇ Tnetwork-based detection of iot botnet attacks using deep autoencoders," IEEE Pervasive Computing, vol. 17, no. 3, pp. 12–22, 2018.

[19] S. Su, Y. Sun, X. Gao, J. Qiu, and Z. Tian, "A correlation-change based feature selection method for iot equipment anomaly detection," Applied Sciences, vol. 9, no. 3, p. 437, 2019.

[20] Q. Tan, Y. Gao, J. Shi, X. Wang, B. Fang, and Z. H. Tian, "Towards a comprehensive insight into the eclipse attacks of tor hidden services," IEEE Internet of Things Journal, 2019. vol. 6, no. 2, pp. 1584-1593,April.

[21] L. Shrivastava, B.K. Chaurasia, GS Tomar, S.S. Bhadoria, "Secure Congestion Adaptive Routing using Group Signature Scheme", Trans. on Comput. Sci. Vol.17, LNCS 7420, pp. 101–115, 2013.

[22] Ramkumar, G. et al. (2021). "A Short-Term Solar Photovoltaic Power Optimized Prediction Interval Model Based on FOS-ELM Algorithm", International Journal of Photoenergy, Volume 2021, Article ID 3981456, 12 pages, https://doi.org/10.1155/2021/3981456.

[23] I. Van der Elzen and J. van Heugten, "Techniques for detecting compromised iot devices," University of Amsterdam, 2017.

[24] Padmakala S, Muthuchelvi P & Anandha Mala GS 2014, 'IVRSC: 'An Interactive and Intelligent Video Retrieval System for Cricket Videos Using Multi-Features', International Journal of Applied Engineering Research, ISSN 0973-4562, vol. 9, no. 24, pp. 27457-27491