INTERNATIONAL RESEARCH JOURNAL ON ADVANCED SCIENCE HUB
e-ISSN : 2582 - 4376
Open Access
RSP SCIENCE HUB
(The Hub of Research Ideas)
Available online at www.rspsciencehub.com

Special Issue of First International Conference on Information Technology, Computing & Applications (ICITCA 2021)

Malicious Traffic Flow Detection in IOT Using Ml Based Algorithms

V Sri Vigna Hema[1], S Devadharshini[2], P Gowsalya[3]
[1]Assistant Professor, Information Technology, Bannari Amman Institute of Technology, Sathyamangalam, Erode, India.
[2]Information Technology, Bannari Amman Institute of Technology, Sathyamangalam, Erode, India.
[3]Information Technology, Bannari Amman Institute of Technology, Sathyamangalam, Erode, India.
srivignahemav@bitsathy.ac.in[1]. devadharshini.it17@bitsathy.ac.in[2], gowsalya.it17@bitsathy.ac.in[3]

Abstract

Identifying the malicious traffic flows in Internet of things (IOT) is very important to monitor and avoid unwanted errors or the unwanted flows in the network. So, for a security to this network various machine learning algorithms (ML) has been introduced by various analyst to avoid this flow of error in the network. But, owing to the unsuitable selection of features, the ML models which introduced previously suffer from misclassify errors. So, there arises a need to study the problem of feature selection more depth to predict the accurate traffic flow observation in the network. To overcome this problem, a new structure in machine learning (ML) is introduced. So, for thisa novel features selection metric CorrAUC is suggested. So, based on this metric approach, a new feature selection algorithm CorrAUC is develop and design, it is based on wrapper technique to get features accurately by filtering to predict flow of traffic is suggested. Then, we applied multicriteria decision method called VIKOR which is used for validating the features selected for recognition the flow of traffic errors in the network. We estimate our approach by using the NSL-KDD dataset and three different ML algorithms.

Keywords: **Machine learning, IOT security, attacks, Malicious, Identification.**

1. Introduction

Nowadays, our daily life is being well organized by using internet of things (IOT) technology. The internet of things (IOT) technology is interconnected with our daily needs such as vehicles and other home appliances. In some cases the technology is restricted to small industries and homes. However, now due to vast development of this technology the data collection, transferring and retrieving are getting numerous in various fields. So, IOT has become more essential for our life which saves time and gives more reliability. However, in 2021 the IOT will bring tremendous changes in connection with several IOT devices and grows up faster. Even though the technology is enlarging day by day we also face more dangerous cyber-attacks in the IOT technology which been challenging to secure the devices. Hence, many researchers in this IOT technology field introduced numerous cyber security systems and have implemented these methods to protect their data's and information from the cyber-attacks. At recent time maintaining security in the internet has become a trending topic and also gained more attention in IOT cyber security .For this purpose, many analyzer tried finest of their own and presented various cyber security systems. These cyber security systems are deploy for the safety of important details to protect it from prohibited access in the network. In 2017, denial of services (DDOS) attacks in internet of things grew by 172 percent, sparking a lot of interest in the technology. The attacks in malware were increased in IOT environment in 2017 contrast to 2013 given by the Kaspersky lab report in 2019. In this numerous attacks mostly

Botnet attacks is considered as very harmful attack. The harmful attacks were emerging as man-in-the-middle (MITM) which is the distributed denial of service (DDOS) threat. Alharbiset et al. proposed a new structure called fog computing based security (FOCUS) for the observation of malware cyber-attacks. It is used in virtual private network (VPN) to provide secure communication between the IOT. Devices and uses dare responses verified to keep the VPN server protected from malware attacks. It gives good result in low reaction time and bandwidth. So, artificial intelligence (AI) and machine learning (ML) are widely applied to get perfect and better outcomes. The ML model's significant features set are crucial for successful identification. Without a training set and a testing set, evaluating the machine ML model is difficult. Simultaneously a consequence, a valuable range of training and testing sets is available. It is needed for the ML model to be evaluated. Malicious, intrusion, and cyber-attacks in IOT networks can all be detected and categorized using machine learning methods. Using Machine Learning as a strategy for identifying and classifying malicious software Cyber-attack traffic is successful, but when compared to other forms of traffic, it is inefficient because the ML technique method is a complex computing tool. Though, in the field of recognition or classification, using a machine learning approach is very successful. However, there are several drawbacks to IOT malicious and intrusion detection such as concerns with computing time and energy usage. This two issues become currently trending in the IOT area, and numerous researchers are attempting to solve them using machine learning methods. For better performance results, there should be perfect data sets for ML model identification to resolve the above problems. [1-5].It is possible to produce high-performance outcomes by using machine learning technique for detecting cyber-attacks reliably in the Internet of Things (IOT) network environment. To solve problem of selecting effective features zhang h etal.suggested two separate algorithms. Their newly introduced method is effective to select features from imbalance datasets. Similarly, Doroniotis et al. implemented Bot-IoT, a new data collection for detecting cyber-attacks in the IOT network, in 2018. In their view, they based their research on attacks which are malicious in IOT networks. These different types of hazards attacks are included in the generated data collection. Especially cyber-attacks involving Botnets. However, based on the findings of the report, we concluded that selecting a larger collection of features is ineffective for accurate identification by employing machine learning techniques. The accuracy of ML classifiers can be lowered if more than 50 features are used it can make computations more difficult. However, no efficient machine learning model for detecting cyber-attacks on IOT networks has yet been suggested. As a result, it's crucial to research the effective features for malicious and anomaly traffic in the Internet of Things (IOT) network and implements the proposed technique that solves the problem.[6-10].

2. Literature Review

Since from the last century, trust issues and privacy issues seems to be a major topic and many experts already worked very hard to improve the situation and developed number of effective models. The most successful and documented survey on selecting features for malicious attacks in network of IOT environment are detailed clearly in this section. Anderson[1] has comes with a novel detection method called first Intrusion detection in 1980 .And In 1987 Denning created a new model in order to detect intrusion based on actual intrusion detection .This identified system has an ability to find break-ins, perforations and other intrusion Trojan Horse and also system-related intrusion that cause to affect the computer. However their developed framework was based on the premise that any security breach can be tracked using tracking. Further Access control mechanism is suggested by[2] Qiu,Tain used this method to prevent the flow of information that is not permitted, but this mechanism has a defect of giving security issues to access the control systems ,so to overcome this they introduced next method. Then IbbadHafeez [3] has proposed a new method to detect the malicious IoT network using online Traffic analysis as IoT-KEEPER .IoT-KEEPER immediately restricts network access to the IoT system that is causing the issues, preventing it

from attacking other devices or services. But also this method face issues in time consumption and some more problem. so that effective method to select the effective features are developed that is Effectiveness of Statistical Features for Early Stage Internet Traffic Identification[5].In this method Packet sizes and statistical features have shown to be useful features in Traffic Detection at the early stages .To overcome this problem Alharbi S [4]proposed a new system as FOCUS Fog Computing based Security system ,To secure communication channels to IoT computers the conceptual FOCUS system uses a virtual private network (VPN).FOCUS sometimes utilize challenge-response authentication to safe the VPN server from the malicious attack like DDoS attack, which can further increase the protection of the IoT framework. Such a dual protection scheme is successful in quashing a number of malicious attacks and can provide High-level protection for the Iot system. Besides that FOCUS is used in fog computing which is close to end users, resulting in a quick response and efficient network use. FOCUS is demonstrated in a proof-of-concept framework and experiments are conducted to assess its efficiency .But this also has some limitation that critical to have accurate network classification and also has difficulties in getting effective features , so that we goes to the proposed system for effective results and better performance. **Inference:** From the above survey, many methods are driven to detect the traffic flow attacks but it is critical to select effective features. This proposed method select effective features from the NSL-KDD dataset.

3. Proposed Method

In this chapter we detailed the proposed method line by line. Our proposed approach involves four measures for the effective feature selection in the IOT network. To begin, a novel feature selection method called CorrAUC is designed and implemented, which choses features that carry sufficient data and then applies it. Whereas CorrAUC a new metric method to extract a effective feature from the NSL-KDD dataset. CorrAUC is proposed and designed ,to access the feature comes from the filter process called wrapper technique ,and select the effective features for the chosen algorithm of machine learning using AUC method and NSL-KDD dataset. To address the issues, in effective feature selection for the IoT attack detection the Proposed approach combines Correlation Attribute Evaluation (CAE) with Area Under Roc Curve (AUC), a distinct machine learning algorithm is used. The Selected features of Iot attacks are validating using multi criteria decision method called VIKOR method. Effective results are produced by this technique in terms of selecting effective feature for Iot attacks in IoT environment network. [11-15].To the best of our knowledge, in this paper this is the first research to combine Correlation and AUC metric method for the purpose of detection of attacks using machine learning algorithm in Iotnetwork. Furthermore our proposed approach chooses the feature set that contains sufficient data for the IOT attacks in network of IOT. For the detailed understanding, In the next part, we will go over the methodology in more detail for the effective feature selection in IOT network environment in terms of IOT malicious attacks detection.[16-21].

3.1. System Architecture

The proposed framework of malicious traffic flow detection using ml-based algorithm.

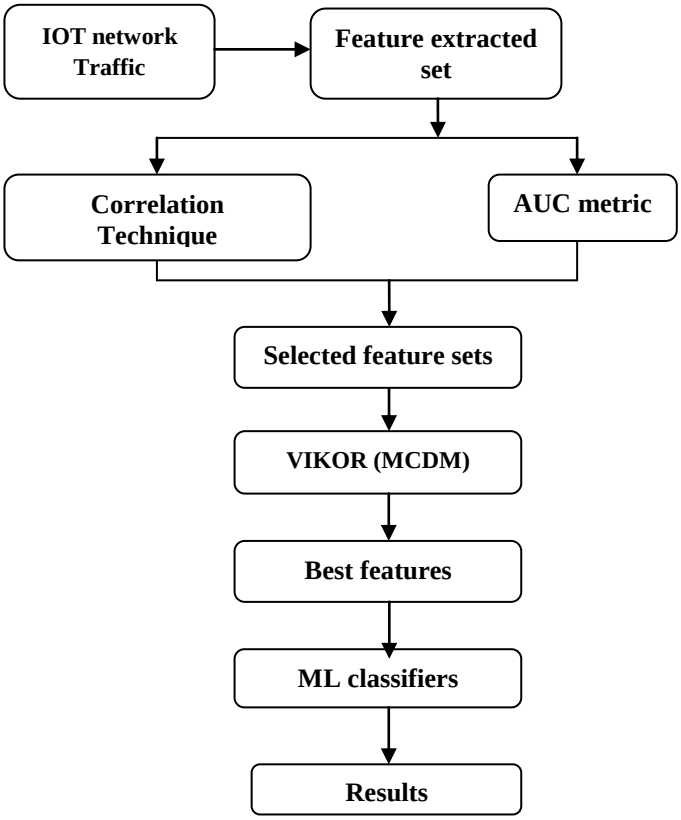

Fig.1. Proposed framework of malicious traffic flow detection using ml-based algorithms.

4. Feature Selection Metrics

The observed features selection metrics is detailed discussed in this section. We begin with correlation-based metric is explained and then we goes to AUC metrics. The details are listed in the next section.

4.1. Correlation Based Metrics

In process to overcome the IoT attack detection problem of selecting effective features in IoT network Galton has proposed a simple idea as Pearson Moment Correlation in his year of 1880's .This technique is detailed more for the identification of relationship between class features and independent. Then K Pearson in 1896 has introduced a new Pearson moment correlation with some changes and defined as Pearson Product moment correlation. This method used in this is project is a Statistical method operation, used for the relationship identification among different attributes and features. Formulas are used for correlation coefficient. For the different A and B attribute, the formula is used to calculate Pearson Correlation Coefficient between A and B attributes.

$$\text{CM, N} = \frac{\text{Covaraince}\quad (X,Y)}{\sigma_m\,\sigma_n}$$

In this first equation Cx,y, is correlation coefficient and (X,Y) shows the covariance. And also standard deviation for the X and Y attribute of xy is$\sigma_x\sigma_y$. More specifically equation number 2 can be used to measure the correlation coefficient for the sets of two features.

$$C = \frac{\sum_{n-1}^{i}(x_n - \bar{x})(y_n - \bar{y})}{\sqrt{\sum_{n-1}^{i}(x_n - \bar{x})^2}\sqrt{\sum_{n-1}^{i}(y_n - \bar{y})^2}}$$

For example two sets of features X and Y with their respective features can be written as x1;x2;x3;;;;xn and y1;y2;y3;;;;;yn,respectively .Similarly, n denoted the number of size cases. Where xn and yn are the data values. Similarly if the values of the C coefficient are reached to plus one +1 and minus one -1 in equation 2, x bar and y bar are the mean values. It implies that if the coefficient values are greater than one, the relationship between the features is strong and if the coefficient values are zero, there is no relationship between the features. From the other hand if the coefficient values are negative indicates a very weak relationship between features .The technique called Pearson correlation technique is very useful for ranking and detailed selection of features. As a result, the correlation was used to overcome the problem of selecting strong and robust features for IoT malicious attacks detection in IoT network. To ranking the effectiveness of several given set the correlation attribute evaluation technique is used. The basic idea behind using these ranking attributes is to use the correlation between features to rank the performance of a dataset's features collection. Nonetheless, this feature will be successful for detecting IoT malicious attacks in an IoT network using machine learning .If the relationship is high between feature and class, not correlated to selected feature. Similarly, feature performance can be calculated and studied in the following way for the accurate detection.

$$\text{Cor} = \frac{\text{lavg}(\text{cor}_{dc})}{\sqrt{l + l(l-1)\text{avg}(\text{cor}_{dd})}}$$

From the above equation Cor denotes the correlation between features, while lavgcordc denotes the average of the correlation between features and their class. Avg (cordd) denotes the average of correlation between features and L denotes numbers of features.Nevertheless,by using the above equation to identify correlation relationships between attributes , the major factors are: if the correlation between the feature set is high, the correlation between the features set and the features class is weak .Accordingly , a strong correlation between the features set and the reliant class implies a strong correlation between the features set and the class, if there is large number of attributes that indicates a strong correlation between features and reliant class.

4.1.1 Area under the Curve (AUC) Based Metric:

After filtering from the corr metric, it is important to select the effective feature which has full of accurate information for the IoT attacks detection in IoT network. In this case, a wrapper technique is used, which is based on the area under ROC curve (AUC) metric. The accuracy metric is the most optimal for the classification of network traffic using machine learning technique. But in this case, we're looking for the most important collection of features for detecting IoT attacks in the IoT network environment. As a result, the AUC metric is an important metric for detecting malicious attacks in IoT networks as well as a

useful metric for ranking features in large range of features. However there are two distinct facts on using AUC metric in this study: the model will provide successful output results if the AUC metric values are strong and high. This process will not provide successful performance results in terms of detecting IoT attacks in the IoT network environment, if the AUC metric values are small or not high enough. More specifically, the AUC metric is very useful for evaluating efficiency and ranking features. As a result, we used the AUC metric in this research study to rank successful features and choose those that contain enough information and have good high metric values for detecting malicious IoT attacks in IoT networks.

4.1.2 The Proposed Algorithm

In this part we have discussed about the step by step work of combination of correlation and AUC metric method. Two parts are included in the proposed CorrAUC. To filter the feature set and determine the relationship between the feature and class, correlation algorithm is used. Then to the next step, which is to use a machine learning based algorithm to filter the features with high AUC metric values. Likewise our proposed method picks the features which carry useful information for IoT detection in network environment. However, the following are the detailed step-by-step phases: As discussed in the above part, the combined feature of correlation and Area under Roc Curve metric in our proposed method is to select feature which carry only useful information for the benefits of IoT network environment to detect IoT attack detection. However, the proposed method selects a feature which has high correlation relationship among features to calculate correlation between them. Firstly, this method calculates the correlation values between features and placed the respective values in ascending order. After that comparison of correlation goes between the every feature. Then a value is assumed as threshold value, if the value of feature correlation is greater than the threshold value, it mean the feature as highly effective and placed that in the descending order. More specifically ,the higher the threshold value, the faster the proposed model is, but it is ineffective for the machine learning algorithm because high threshold values reduces machine learning algorithm detection and efficiency. The proposed algorithm then filters each feature using the AUC metric of a particular machine learning algorithm after determining the correlation and filtering with threshold values. However, the proposed algorithm filters each feature one by one using AUC metric and selects those features that give high AUC metric values for detecting IoT attacks in IoT network environment as if the AUC values of feature are low, the algorithm will remove the feature from the list and proceed to the Swapper stage.

4.2Vikor Method

To make a feature selection effective, VIKOR method which is also known as multi criteria decision making is used to find the attacks in the environment of IOT.

The motivations are discussed first and then preliminary definitions of feature selection which are effective and the mathematical operation are done for understanding. In operational science, decision making method becomes most difficult problem and many analyzers were worked to solve this problem and proposed successful structure for decision making. Molodsov's introduced soft set for decision making and attributes to select from a set of multiple criteria attributes, and then Gong’s introduced objective soft set. In a similar vein, a soft set which is type-2 is introduced for solving the problem of decision-making. This soft set is a usable technique for selecting successful attributes from a set of multiple attributes, as shown by the literature review above. However, after the proposed feature selection method, a decision-making technique is used to solve the issue of successful feature selection. It's critical to test the proposed feature selection method. As a result, the conceptual decision-making technique is used to choose balanced set for detecting attacks in IOT networks. We may use the same approach to pick effective features from a large number of features based on the findings of this analysis.

4.2.1Vikor Method Steps

Step 1: Find the best fi* and worst fi values for all criterion functions, I = 1,2,...,n; fi* = max (fij,j=1,...,J), fi = min (fij,j=1,...,J) if the i-th function is benefit; fi* = min (fij,j=1,...,J) if the i-th function is cost; fi* = min (fij,j=1,...,J).

Step 2: Using the following relationships, compute the values Sj and Rj, j=1,2,...,J:

Rj=max[wi(fi* - fij)/(fi*-fi),i=1,...,n], weighted and normalized Chebyshev distance; Sj=sum[wi(fi* - fij)/(fi*-fi),i=1,...,n], weighted and normalized Manhattan distance; where wi are the weights of parameters, reflecting the DM's choice as the relative value of the criteria.

Step 3: Calculate the values Qj, j=1,2,...,J, using the formula Qj = v(Sj – S*)/(S – S*) + (1-v)(Rj-R*)/(R-R*), where S* = min (Sj, j=1,...,J), S = max (Sj, j=1,...,J), R* = min (Rj, j=1,...,J), R* = max(Rj, j=1,....,J). Since the criterion (1 of n) relevant to R is also included in S, v = 0.5 is adjusted as = (n + 1)/ 2n (from v + 0.5(n-1)/n = 1) to protect these strategies.

Step 4: Order the options by the values S, R, and Q, starting with the lowest value. Three rating lists emerge as a result of the research.

Step 5: If the following two conditions are met, propose the alternative A(1) as a compromise solution, which is the best graded by the measure Q (minimum): C1. "Advantage Acceptable": Q(A(2) – Q(A(1)) >= DQ, where A(2) is the alternative that ranks second in the ranking list according to Q; DQ = 1/ (J-1). C2 "Acceptable Decision Stability": Alternative A(1) must also be the highest ranked by S or/and R. This compromise approach is stable within a decision-making phase, and may be the highest group utility strategy (when v > 0.5 is required), "by consensus" v about 0.5, or "with veto" v 0.5). If one of the conditions is not met, a set of compromise solutions is proposed, which includes: - Alternatives A(1) and A(2) if only condition C2 is met, or - Alternatives A(1), A(2),..., A(M) if condition C1 is met; A(M) is decided by the relation Q(A(M)) – Q(A(1)) DQ for maximum M (the positions of these alternatives are "in near proximity").

5.Experimental Analysis

In this process we discussed about the dataset of the proposed system, and then the performance analysis is discussed for the detection of malicious attacks in IoT network environment.

5.1. NSL-KDD Dataset

The proposed method uses NSL-KDD dataset. The dataset contains traffic flows which are normal and also has several attacks in IoT network. The NSL-KDD dataset is used to find accuracy of traffic and develop dataset which is effective to avoid cyber-attacks. Similarly, we extract many features which is applied to the extracted features collection to increase ML model efficiency for accurate prediction model. The attacks flow, categories, subcategories are labeled for better performance results. Additionally the dataset contains no redundant record in their train set so result will be non-biased .And also it does not contains duplicate record in the test set that will have better reduction rates. The training dataset contains 21 separate attacks, compared to 37 in the test dataset. The recognized attack styles are those that appear in the training dataset, while the novel attacks are those that occur in the test dataset but are not present in the training datasets. The styles of attacks are divided into four categories: DoS, Probe, U2R, and R2L are four different types of DoS.

5.2 Performance Analysis

Confusion metrics, which are based on the performance measurement, are commonly used to calculate the detection or recognition performance of a machine learning model test. Even so, the most commonly used metric for evaluating a machine learning model is as follows:

•True Positive (TP): In this TP indicates that Class A is correctly identified as belonging to class A during attack detection.

•True Negative (TN): In this it indicates that Class A is correctly identified as not belonging to Class A.

•False Positive (FP): In this matrix indicates that Class A is not correctly identified as belong to Class A during the attack detection.

•False Negative (FN): In this FN indicates that Class A is not correctly identified as belong to Class A during the attack detection

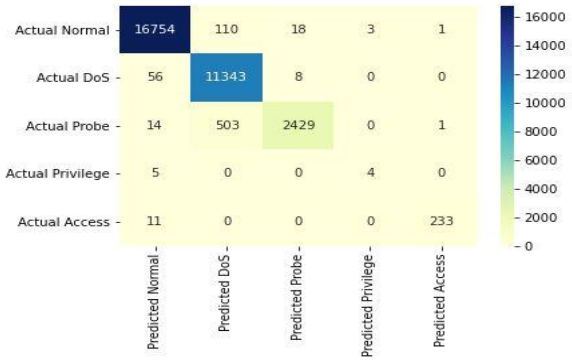

Fig.2.It shows the predicted normal & attacks and actual normal & attacks of NSL-KDD dataset

Using the metrics described above, however, different measurement metrics can be created to test a machine learning model. Machine learning classifiers reduce false positive and false negative metrics values for accurate identification. However, the following are the selected metrics that were used in this paper:

Accuracy: It can be described as the correctly identified samples of traffic in the overall identified samples traffic in the context of attacks detection. The accuracy, on the other hand, can be mathematically described using performance measurement metrics as follows:

$$\text{Accuracy} = \frac{(\text{T pos} + \text{T neg})}{(\text{Tpos} + \text{Tneg} + \text{Fpos} + \text{Fneg})}$$

In our research, we used equation 4 to assess the efficiency of machine learning classifiers. The efficacy of ML classifiers can be determined using these metrics.

Precision: It can be described as the percentage of correctly identified Class A samples in all those who were correctly identified in Class A. Below is the mathematical formula that was used in this research analysis.

$$\text{Precission} = \frac{\text{Tpos}}{(\text{Tpos} + \text{Tneg})}$$

However, for the proposed technique's performan ce evaluation, we used the metrics mentioned abo ve.

Table 1.This table shows the comparison of accuracy and precision using machine learning classifiers.

ML Algorithms	Accuracy	Precision
Random Forest	0.99	0.99
Logistic regression	0.82	0.68
KNeighbors classifier	0.98	0.98

6.Result and Analysis

The detailed findings and interpretation of the proposed method are discussed in this section. Using the NSL-KDD dataset, we proposed a new technique for detecting attacks in the IOT network. In the IOT network environment, there are four successful features for feature selection that provide enough information for attack detection. Three different machine learning algorithms, such as KNeighbour's Classifiers, Logistic Regression, and Random Forest ML algorithms, are used to evaluate the efficiency of the proposed technique with the goal of selecting successful features. Though the performance of all three implemented ML algorithms is successful for detecting attacks in the NSL-KDD dataset, there is a difference between the classifiers when using the proposed technique with accuracy and precision. However, when using the selected features set as accuracy metric for the NSL-KDD dataset, the performance of Logistic Regression is poor when compared to other machine learning classifiers. Similarly, as compared to other ML classifiers, the efficiency of Random Forest is marginally better in terms of accuracy, as shown in the fig.3.Random Forest and KNeighbour's ML algorithms, on the other hand, have better accuracy outcomes. However, when compared to other applied ML classifiers, the Random Forest gives successful results in terms of overall applied ML classifier efficiency. As a result, the Random Forest ML algorithm outperforms the selected features set by 99.5 percent in detecting attacks in the NSL-KDD dataset, which is a very effective output result.

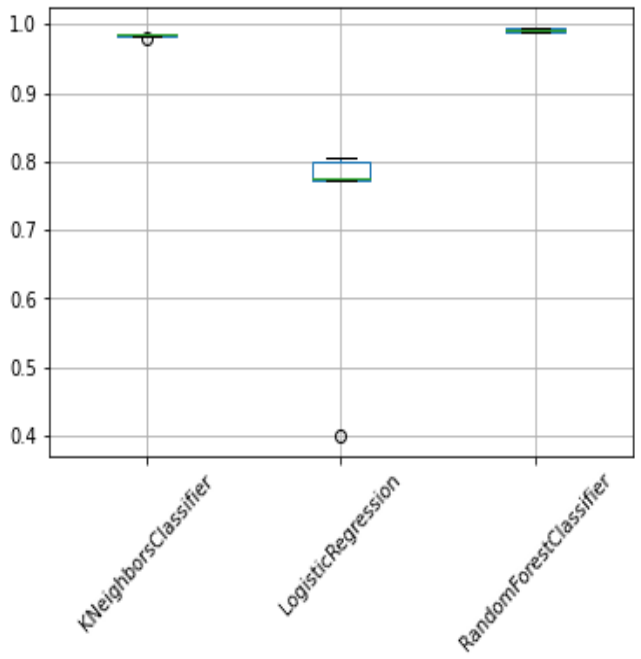

Fig 3.Results of comparing features with machine learning algorithms.

Conclusion

Attack detection in the Internet of Things (IOT) network is critical for IOT security, as it keeps an eye on and blocks unwanted traffic flows. Many researchers have presented a variety of machine learning (ML) technique models to block attack traffic flows in the IOT network. Several machine learning models, on the other hand, are susceptible to misclassifying mostly in malicious traffic flows due to insufficient feature selection. Nonetheless, the important problem of how to pick effective features for accurate malicious traffic detection in IOT networks needs to be researched further. A new system model is proposed for this reason. First, a novel feature selection metric called CorrAUC is proposed, and then, based on CorrAUC, a new feature selection algorithm called Corrauc is developed and designed, which is based on a wrapper technique to accurately filter features and pick effective features for the selected ML algorithm using the AUC metric. The Vikor or Multicriteria decision making tool, which is based on a bijective soft collection, was then used to validate selected features for malicious traffic detection in IOT networks. The NSL-KDD dataset and three separate ML algorithms are used to test our proposed solution. The analysis of experimental results revealed that our proposed method is efficient, achieving average results of >96%.

References

Journals

[1]. J. P. Anderson, "Computer security threat monitoring and surveillance, 1980. Last accessed: November 30, 2008."

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

[3]. 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.

[4]. J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, "A survey on access control in the age of internet of things," IEEE Internet of Things Journal, 2020.

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

[6]. 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.

[7]. M. Shafiq and X. Yu, "Effective packet number for 5g im we chat application at early stage traffic classification," Mobile Information Systems, vol. 2017, 2017.

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

[9]. D. Ventura, D. Casado-Mansilla, J. López-de Armentia, P. Garaizar, D. López-de Ipina, and V. Catania, "Ariima: a real iot implementation of a machine-learning architecture for reducing energy consumption," in International Conference on Ubiquitous Computing and Ambient Intelligence. Springer, 2014, pp. 444–451.

[10]. L. Peng, B. Yang, Y. Chen, and Z. Chen, "Effectiveness of statistical features for early stage internet traffic identification," International Journal of Parallel Programming, vol. 44, no. 1, pp. 181–197, 2016.

[11]. D. Molodtsov, "Soft set theoryâA˘Tfirst results," ˘ Computers & Mathematics with Applications, vol. 37, no. 4-5, pp. 19–31, 1999.

[12]. K. Gong, Z. Xiao, and X. Zhang, "The bijective soft set with its operations," Computers & Mathematics with Applications, vol. 60, no. 8, pp. 2270–2278, 2010.

[13]. V. Tiwari, P. K. Jain, and P. Tandon, "An integrated shannon entropy and topsis for product design concept evaluation based on bijective soft set," Journal of Intelligent Manufacturing, vol. 30, no. 4, pp. 1645–1658, 2019.

[14]. A. R. Roy and P. Maji, "A fuzzy soft set theoretic approach to decision making

problems," Journal of Computational and Applied Mathematics, vol. 203, no. 2, pp. 412–418, 2007.

[15].T.-C. Wang and H.-D. Lee, "Developing a fuzzy topsis approach based on subjective weights and objective weights," Expert systems with applications, vol. 36, no. 5, pp. 8980–8985, 2009.

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

[17]. M. Dash and H. Liu, "Feature selection for classification," Intelligent data analysis, vol. 1, no. 1-4, pp. 131–156, 1997.

[18]. H. Zhang, G. Lu, M. T. Qassrawi, Y. Zhang, and X. Yu, "Feature selection for optimizing traffic classification," Computer Communications, vol. 35, no. 12, pp. 1457–1471, 2012.

[19]. N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset," arXiv preprint arXiv.

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

[21].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.