IoT Malicious Traffic Identification Using Wrapper-Based Feature Selection Mechanisms

Muhammad Shafiq, Zhihong Tian, *Member, IEEE,* Ali Kashif Bashir, *Senior Member, IEEE,*
Xiaojiang Du, *Fellow, IEEE,* and Mohsen Guizani, *Fellow, IEEE,*

***Abstract*—Machine Learning (ML) plays very significant role in the Internet of Things (IoT) cybersecurity for malicious and intrusion traffic identification. In other words, ML algorithms are widely applied for IoT traffic identification in IoT risk management. However, due to inaccurate feature selection, ML techniques misclassify a number of malicious traffic in smart IoT network for secured smart applications. To address the problem, it is very important to select features set that carry enough information for accurate smart IoT anomaly and intrusion traffic identification. In this paper, we firstly applied bijective soft set for effective feature selection to select effective features, and then we proposed a novel CorrACC feature selection metric approach. Afterward, we designed and developed a new feature selection algorithm named Corracc based on CorrACC, which is based on wrapper technique to filter the features and select effective feature for a particular ML classifier by using ACC metric. For the evaluation our proposed approaches, we used four different ML classifiers on the BoT-IoT dataset. Experimental results obtained by our algorithms are promising and can achieve more than 95% accuracy.**

***Index Terms*—Feature Selection, Internet of Things, Cybersecurity, Attacks, Classification, Idntification, Machine Learning.**

I. Introduction

OWING to Smart Internet of Things (SIoT), the world becomes more convenient and more efficient as compared to the last decade [1]. In 2021 the connected devices in the SIoT network will reached to 27 million [2], which will be a huge change in technology era. As the smart applications growing day by day, the cyber-attacks will become more upsurge and more challenging. Nowadays, cybersecurity systems are widely used to protect information and IoT applications from attacks and unauthorized access in SIoT network environment [3][4]. From last few years IoT gaining a lot of attention in the area of IoT network anomaly and intrusion detection and researchers endeavor hard to overcome this problem. Similarly, several different kinds of cybersecurity systems are proposed and applied to protect information, computers and SIoT applications from attacks and unauthorized access in IoT network environment. For instance, in 2017, the number of IoT Denial of Service (DDoS) attacks grew up to 172% [2] [5]. Likewise, in 2017 numbers of malware attacks have increased by up to a numbers of times as compared to numbers of malware attacks in 2013, in which huge numbers of attacks of them are extremely hazardous such as Botnet attacks etc., as indicated by Kaspersky lab report [6]. To overcome the problem of cyber-attacks, In 1980 the first Intrusion Detection System was proposed by Anderson [7]. Then in 1987 Denning [8] introduced a real-time intrusion detection expert systems model, which was able to detect break-ins, penetrations such as Trojan horses, viruses and leakage, etc. However, their model used hypothesis to detect malicious attacks in a network. Moreover, their study especially focused on user behavior to identify abnormal operations. Recently, man-in-the-middle (MITM) threats are becoming more dangerous threats with distributed denial of service (DDoS) [9], but these are widespread hazardous threat to the Internet of Thing, and many researchers endeavor hard to accurately identify, detect and carry out a scheme to protect IoT network against such hazardous intrusion. Similarly, in 2018, Salem et al. in [10]introduced a new system named Fog Computing Based Security (FOCUS). This method mainly used to prevent the IoT network against malware cyberattacks. However, their proposed model consists of Virtual Private Network (VPN), which is used for the protection [11] of IoT communication devices channels [12]. Furthermore, their proposed protection system can send alerts during DDoS attacks in IoT network environment [13][14]. For the evaluation of results, their study confirmed proof of concept, and for the proposed system performance evaluation they conducted the experiment. However, their experimental results showed that their proposed model is efficient to percolate malicious attacks with a little low feedback time and with small bandwidth consumption. For effective performance, Machine Learning (ML) and Artificial Intelligence (AI) techniques are the most effective and mostly applied methods that can be applied to SIoT for cyberattacks detection [15], [16], [17]. From the last few decades ML methods have become popular in many areas such as from biology to telecommunications. ML technique uses attributes mean features as an input that are derived features set. Furthermore, ML techniques uses training and testing features sets for the evaluation of a model performance. ML techniques are more powerful for malicious traffic identification, cyberattacks detection [18], and the computing tools are more sophisticated as compare to other tools. Nevertheless,

Muhammad Shafiq, Zhihong Tian, are with the Department of Cyberspace Insitute of Advanced Technology, GuangZhou University, GuangZhou,China, 510006.
E-mail: srsshafiq@gmail.com,

Ali Kashif Bashir is with the Department of Computing and Mathematics, Manchester Metropolitan University, Manchester, UK.

Xiaojiang Du is with the Department of Computer and Information Sciences, Temple University, Philadelphia, USA

Mohsen Guizani is with the Department of Computer Science and Engineering , Qatar University, Qatar.

Correspondence: Zhihong Tian (tianzhihong@gzhu.edu.cn).

applying the ML technique to IoT introduces new constraints such as computation time and energy consumptions. Nowadays, computation time and energy consumptions are very emerging problems in the ML technique to IoT. However, several researchers endeavor hard to solve this issue. However, ML techniques are able to achieve accurate performance results in IoT malicious traffic identification, but when the input of the ML classifiers is optimal [19]. Thus, for optimum input to ML classifier, it is a good practice to remove unwanted features from the given features set, and feature selection techniques can do this task. Therefore, it is essential to focus on this issue and select effective features set for accurate anomaly and intrusion detection using ML algorithms so that we can manage security policy. Similarly, Zhang H et al. [20] studied the problem of feature selection and proposed a feature selection techniques using high dimensional datasets, such as imbalanced data for Internet traffic classification. However, their proposed techniques are effective and give optimum performance results. For the experimental evaluation results TPR and FPR metrics are used and as well as the authors evident that their proposed approaches are able to achieve high accuracy results. Likewise, in 2018 Koroniotis et al. in [21] address the problem of identifying malicious attacks in IoT network and then they develop and proposed online a new BoT-IoT dataset which incorporates the law and rules and simulate IoT network traffic including different types of attacks traffic usually used by botnets. However, the dataset is established in a realistic testbed with defined attributes, which includes on different types of attacks and normal traffic flow in the IoT network [22]. Using statistical analysis, they select ten best features set from the given set of features that they are extracted. Similarly, for the performance evaluation, they used ML classifiers to show the effectiveness of the selected features and showed that the selected feature set is optimum with reference to Accuracy, Recall, Precision, and Fall-out metrics. Nevertheless, it is important to find out and choose a features set that carry enough information for anomaly and intrusion in the IoT network to identify malicious attacks effectively. Similarly, in our previous research study [23], [24], [25], [26], [27], we classify Instant Messaging (IM) applications messages services using different IM classifiers by selecting 50 different statistical flow-based features set and achieve very effective performance results. Likewise, in [23], [28], we proposed different approaches and classify different traffic applications for accurate Internet traffic classification and produced an efficient feature set for internet traffic identification using ML algorithms. Nevertheless, in these research studies, we concluded that selecting more than fifty features set are not a good experience, which leads to computational complexity and decrease ML classifiers accuracy results. Thus it is important to study more in depth and propose efficient identification model for features selection anomaly and intrusion to IoT traffic identification.

In this research paper, we introduce a new feature selection technique to find out effective features set for Botnet IoT attacks in SIoT network using ML algorithm and to optimize the performance of machine learning methods. However, our main contribution in this paper are includes the following:

- To overcome the problem of Botnet attacks to the Internet of Things (IoT) and with effective feature selection in Smart IoT network anomaly and intrusion traffic identification. Firstly bijective soft set technique are used and define with details and then through bijective soft set dataset features are filter and compared with other flow set feature to select effective set.
- Then, a hybrid feature selection approach named CorrACC is proposed to deal with effective feature selection problem for anomaly and intrusion in SIoT network identification. Our proposed approach includes on two different metrics for accurate feature selection: Correlation Attribute Evaluation (CAE) metric and specific ML classifier accuracy (ACC) metric.
- Afterward, we proposed an algorithm Corracc based on CorrACC technique. Firstly Corracc algorithm assigns values to features based on Corr metric and then the algorithm select the features which have high ACC metric values of a particular ML classifier. Then, by using wrapper technique the algorithm select the features set which has significant information. However, it is the first research study where the Corr and ACC metrics are put forward in IoT Botnet attacks identification.
- Then, we put forward the selected features that are effective and choose by the proposed approach and described their values with details. Experimental results showed that seven features selected from given features set are discriminative power for identification of anomaly and intrusion IoT traffic.

This paper is arranged as follows: Section 2 demonstrate the related works. While in Section 3 we explains our proposed techniques. In Section 4 we demonstrate the evaluation methodology, experimental work, and datasets. While in Section 5 we discuss analysis and discussions. Finally, Section 6 includes the conclusions and future works.

II. Related Works

The security and trust problem have been researched in many related computing paradigms, including wireless sensor networks [29], [30], IoVs[31], the future Internet [32], [33] and Smart IoT Cities. In this section, some studies related to IoT anomaly and Intrusion attacks in smart cities are demonstrated. In our previous work [34][28], we applied different Machine Learning algorithms in flow-based Internet traffic classification such as Instant Message application traffic classifications, we got encouraging results and heightened the performance of ML classifier of the employed classifiers. In this studies [28], we have focus on feature selection with different proposed approaches which are effective to minimize the computational complexity of applied classifiers. Though, our studies were only limited to feature selection and Internet applications traffic classification using machine learning [35] algorithms such as Instant Messaging (IM) application, etc. In numerous studies, feature selection technique has been proved effectively. In reality, the feature selection technique is vital and essential in data processing stage. However, feature selection includes on selecting effective features out of numbers of features and removing redundant features, which don't provide information related to the identification.

Similarly, In 2018 S Egea et al. [36] reviews some effective features selection techniques based on correlation measurement techniques and produced a new technique for functionalities to the Fast Based Correlation Features FCBF algorithm to enhance IoT network facilities in an industrial environment. However, in their studies they change the FCBF algorithm into FCBFiP algorithm. The essential purpose was to divide the feature space into parts with equal size. By proposing this approach, they improved the correlation and machine learning applications that are running on every node. However, their proposed model gives improved results with respective model accuracy and execution time. In 2018 Meidan Yair at el. [37] develop a new method for detecting attacks initiated from IoT devices and proposed and empirically evaluate the method anomaly detection which extracts the performance of the network and utilized autoencoders for the detection of anomalies network traffic from IoT devices. However, for the evaluation of the proposed method, they used two well-known IoT-based botnets attacks Bashlite and Mirai and infected some commercial devices in IoT network. Experimental results showed that their proposed technique can identify attacks in IoT devices.

Similarly, Shen Su in [38] proposed a features selection approach to increase the performance of IoT anomaly identification equipment. They firstly cluster IoT sensors together to identify the identical deployed sensors and then they controle the data correlation variation in actual time to pick the sensors with correlation variations as the attributes for anomaly identification. They applied curve alignment for clustering and discussed the window size for data calculation. Afterward, they applied MCFS (Multi-Cluster attributes Selection) to select the online feature selection scenario. They proved that the proposed give effective performance results with respect to minimize the FN (Flse Negative) of IoT equipment anomaly detection. Besides above, some subsequent security technologies, such as the attack detection [39], [40], the key management [41], [42], the evidence management [43] can also be used for IoT security. However, In the above given literature review, it is essential to find out the robust and stable feature set for anomaly and intrusion detection to IoT network traffic classification. In Figure 1, have shown the key idea of the attributes selection method, which are includes on four necessary steps such as subset generation, in which a feature set is will generate, subset evaluation, in this step feature are evaluated by analysis, decision maker, in which decisions are taken accepted or rejected with particular rules and validation of subset. Only those features will be choose, which have the desired information, otherwise will be discard. Figure 1.

III. Proposed Method

In this segment, we demonstrated the proposed technique in details. We use two methods to get a useful feature selection idea as presented in Fig. 2. Initially, we applied a bijective soft set technique which examines the flow features of Botnet attacks dataset and then by utilizing soft set concept we achieve

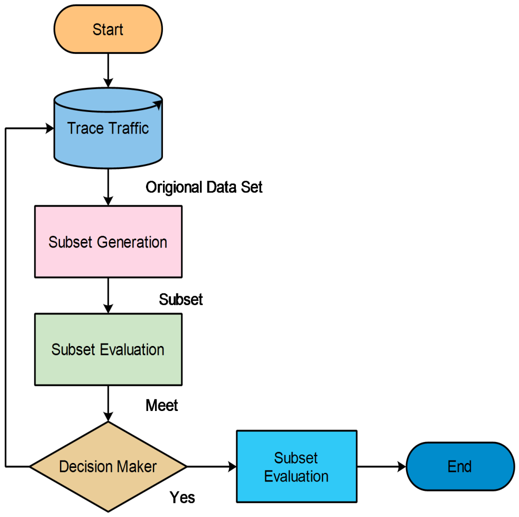


Fig. 1: Fundamental Steps of Feature Selection Process

the final idea. This technique is very effective and gives very clear numerical method to the anomaly, and intrusion detection flows to IoT network in smart cities. Then, we proposed a new feature selection approach called CorrACC to achieve with effective feature selection problem in IoT network. It consist on metrics for effective feature selection: Correlation Attribute Evaluation (CAE) and accuracy (ACC) metrics of the selected classifier. Afterward, we proposed an algorithm Corracc based on CorrACC technique. Firstly the algorithm CorrACC assigns Corr values to the features. Then allocating the Corr values, CorrACC choose the effective features which have high values for the particular classifier. We believe that, it is the first study where the Corr and ACC metrics are put forward in IoT anomaly and intrusion attacks identification. However, we present the features that are have much information and choose by the algorithm and presents their high dimensional values with metric values.

A. Bijective Soft-Set Approach

To overcome the problem of feature selection a mathematical operation is used to select effective feature for anomaly and intrusion detection in IoT traffic identification. The tool named Soft Set, which is firstly introduced by Molodsov in 1999 [44] and Maji [45] and Ali [46]. Soft sets are effective to used for decision making [47], and its fuzzy soft set model, [48]. However, to solved the problem of uncertainties bijective soft set [49] is very good choice as well as typ-2 soft sets [50] [51] can be also used for this type problem. Numerous researcher have been utilized Bijective soft sets for design concept analysis, selection and for decision makings. For instance, Tiwari [52] proposed selection idea which is based on the bijective soft to select items in several given items. Similarly, MF khan [53] also used the same technique to select best Wi-Fi frequency in a collapsed structure. Studying the above effectiveness of the soft set, we also adopt the same technique in our effective feature selection problem for anomaly and intrusion to IoT. However, we used the same technique to show the relationship between the statistical features and then select effective feature which have enough information values for anomaly and intrusion detection in IoT network traffic identification. Using bijective soft set technique, correlation table between features are constructed and then union operations are conducted between that column and rows. We used union operation for both row and column and also intersection for both row and column [53]. Correlation table gives evaluation of the entire best selection which is effective in the features selected. After union operation, intersection operation are conducted in the same way as we applied the union operations for the identification of effective features which leads to us effective feature selection.

1. Introductory definitions: However, there are many introductory definitions in the literature. But we describe soft set and of it's developing process with details. This can make more suitable subsections . In this paper, mostly definitions are taken from Manji and Roy [54].

Definition 1: (Soft Set) [54]: Suppose U is the universal set and it's numerical parameters is S. Suppose U be Q(U) and Y will subset of S, for example,$Y \subset S$. At that point, couple (L, Y) will be soft set over U, and function L will $L : Y \rightarrow Q(U)$. Thus, group of universal subset can likewise viewed as a soft set.

Definition 2: (AND Product) [54], [55] If (L, K) and (M, D) be 2 soft sets, then And-product will be '(L,K) AND (M, D)' of the two soft sets, denoted by $(L, K) \wedge (M, D)$ $is\ defined\ by$ $(L, K) \wedge (M, D) = (I, XD), where\ I(\beta, \phi) = L(\beta) \cap M(\phi), \forall(\beta, \phi) \in K \times D.$

Definition 3: (OR Product) [54], [55] If (L, Y) and (M, N) are sets, then "(L,Y) OR Product (M, N)" soft sets, will be $(L, Y) \vee (M, N)$ $is\ defined\ by$ $(L, Y) \vee (M, N) = (G, YN),\ where\ G(\beta, \phi) = L(\beta) U M(\phi), \forall(\beta, \phi) \in YN.$

Definition 4: (Bijective Soft Set) [49] Suppose (L,S) be a soft set and U is the Universe and S is a none empty parameter set, then we can see that (L,S) is a bijective soft set if the (L,S) soft set over U set and if the bellow given conditions meet exact.

i. $\bigcup_{\beta \in s} L(\beta) = U$

ii. If there are more then 1 mean 2 attributes; $\beta_i, \beta_j, \beta_j \in S, \beta_i = \beta_j, F(\beta_i) \bigcap F(\beta_j =) \oslash$.

2. Bijective soft algorithm: In this subsection we will discussed with detail the algorithm procedure, which lead us to effective feature selection. For instance, the input to the algorithm will be a feature set and the output will be effective features set.

a. Identification of attributes based on IoT dataset made a set X of values.

b. After identification of feature set, the algorithm will develop a soft set from every feature of X set with dependencies per classified dominions flows.

c. After completing the second step the algorithm will goes to step C and will make correlation table between AND and OR product of nxn. However, here in the algorithm the features values are indicated by n for better understanding.

d. Afterward, in this step the algorithm will perform the union operation on the table row or column for the minimization to $1 \times n$ or $n \times 1$.

e. The same step d will follow the algorithm in this step but instead of Union the algorithm will perform the intersection operation to 1 ×1.

f. And in the final step, selected features set, if the table is minimize to 1×1.

We apply concept approach on our proposed model feature selection for anomaly and intrusion in IoT traffic identification. Fig.2 shows the details illustration of our proposed technique through a flowchart.

3. Algorithm main applications: The core application of the algorithm that we used in this section are defined with details are given below;

a. For the purpose of features requirement, we defined ten Selections of features (SFs) to form a SF set as: $SF = [SF_1, SF_2, SF_3, SF_4, SF_5, SF_6, SF_7, SF_8, SF_9, SF_{10}]$, where for the test case, suppose the following features.
$SF_1 = Mean, SF_2 = Stddev, SF_3 = Min,$
$SF_4 = Max, SF_5 = Ar\_p\_proto\_DstIP,$
$SF_6 = Pksts\_P\_Protocol\_P\_DestIP,$
$SF_7 = Pksts\_P\_Protocol\_P\_SrcIP, SF_8 = Seq, SF_9 = N\_inn_conn\_p\_dsttip, SF_{10} = N\_inn_conn\_p\_srcip.$

b. Each SF target requirement identified for effective feature selection. We denote these values with Ω

$$SF_1 = \{\Omega_{11}, \Omega_{12}, \Omega_{13}\} = \{Higher, High, Low\}$$
$$SF_2 = \{\Omega_{21}, \Omega_{22}, \Omega_{23}\} = \{Higher, High, Low\}$$
$$SF_3 = \{\Omega_{31}, \Omega_{32}, \Omega_{33}\} = \{Higher, High, Low\}$$
$$SF_4 = \{\Omega_{41}, \Omega_{42}, \Omega_{43}\} = \{Higher, High, Low\}$$
$$SF_5 = \{\Omega_{51}, \Omega_{52}, \Omega_{53}\} = \{Higher, High, Low\}$$
$$SF_6 = \{\Omega_{61}, \Omega_{62}\} = \{High, Low\}$$
$$SF_7 = \{\Omega_{71}, \Omega_{72}, \} = \{High, Low\}$$
$$SF_8 = \{\Omega_{81}, \Omega_{82}, \Omega_{83}\} = \{Better, Good, Low\}$$
$$SF_9 = \{\Omega_{91}, \Omega_{92}, \Omega_{93}\} = \{Better, Good, Low\}$$
$$SF_{10} = \{\Omega_{101}, \Omega_{102}\} = \{Good, Low\}$$

c. We generate ten features selection concept by suitable combination of feature set.

$$\cup = \vartheta_1 + \vartheta_2 + \vartheta_3 + \vartheta_4 + \vartheta_5 + \vartheta_6 + \vartheta_7 + \vartheta_8 + \vartheta_9 + \vartheta_{10}$$

Identified features selection concept are given as;

$$\vartheta_1 = \{\Omega_{11}, \Omega_{21}, \Omega_{31}, \Omega_{41}, \Omega_{51}, \Omega_{61}, \Omega_{71}, \Omega_{81}, \Omega_{91}, \Omega_{102}\}$$
$$\vartheta_2 = \{\Omega_{11}, \Omega_{21}, \Omega_{31}, \Omega_{41}, \Omega_{51}, \Omega_{61}, \Omega_{71}, \Omega_{81}, \Omega_{92}, \Omega_{101}\}$$
$$\vartheta_3 = \{\Omega_{11}, \Omega_{21}, \Omega_{31}, \Omega_{41}, \Omega_{51}, \Omega_{61}, \Omega_{71}, \Omega_{82}, \Omega_{91}, \Omega_{101}\}$$
$$\vartheta_4 = \{\Omega_{11}, \Omega_{21}, \Omega_{31}, \Omega_{41}, \Omega_{51}, \Omega_{61}, \Omega_{72}, \Omega_{83}, \Omega_{92}, \Omega_{101}\}$$
$$\vartheta_5 = \{\Omega_{11}, \Omega_{21}, \Omega_{31}, \Omega_{41}, \Omega_{51}, \Omega_{61}, \Omega_{72}, \Omega_{81}, \Omega_{91}, \Omega_{101}\}$$
$$\vartheta_6 = \{\Omega_{11}, \Omega_{21}, \Omega_{31}, \Omega_{41}, \Omega_{51}, \Omega_{61}, \Omega_{71}, \Omega_{81}, \Omega_{91}, \Omega_{101}\}$$
$$\vartheta_7 = \{\Omega_{11}, \Omega_{21}, \Omega_{31}, \Omega_{41}, \Omega_{51}, \Omega_{61}, \Omega_{71}, \Omega_{82}, \Omega_{92}, \Omega_{101}\}$$
$$\vartheta_8 = \{\Omega_{13}, \Omega_{23}, \Omega_{33}, \Omega_{43}, \Omega_{53}, \Omega_{62}, \Omega_{72}, \Omega_{83}, \Omega_{93}, \Omega_{102}\}$$
$$\vartheta_9 = \{\Omega_{13}, \Omega_{23}, \Omega_{33}, \Omega_{43}, \Omega_{53}, \Omega_{62}, \Omega_{72}, \Omega_{83}, \Omega_{91}, \Omega_{103}\}$$
$$\vartheta_{10} = \{\Omega_{13}, \Omega_{23}, \Omega_{33}, \Omega_{43}, \Omega_{53}, \Omega_{62}, \Omega_{72}, \Omega_{81}, \Omega_{91}, \Omega_{101}\}$$

d. For the representation of each feature we form a soft set. Similarly, we directly present feature specification using selection concept.

$(H_1, SF_1) = \{H_1(\varOmega_{11}), H_1(\varOmega_{12}), H_1(\varOmega_{13})\}$
$(H_2, SF_2) = \{H_2(\varOmega_{21}), H_2(\varOmega_{22}), H_2(\varOmega_{23})\}$
$(H_3, SF_3) = \{H_3(\varOmega_{31}), H_3(\varOmega_{32}), H_3(\varOmega_{33})\}$
$(H_4, SF_4) = \{H_4(\varOmega_{41}), H_4(\varOmega_{42}), H_4(\varOmega_{43})\}$
$(H_5, SF_5) = \{H_5(\varOmega_{51}), H_5(\varOmega_{52}), H_5(\varOmega_{53})\}$
$(H_6, SF_6) = \{H_6(\varOmega_{61}), H_6(\varOmega_{22})\}$
$(H_7, SF_7) = \{H_7(\varOmega_{71}), H_7(\varOmega_{72})\}$
$(H_8, SF_8) = \{H_8(\varOmega_{81}), H_8(\varOmega_{82}), H_8(\varOmega_{83})\}$
$(H_9, SF_9) = \{H_9(\varOmega_{91}), H_9(\varOmega_{92}), H_9(\varOmega_{93})\}$
$(H_{10}, SF_{10}) = \{H_{10}(\varOmega_{101}), H_{10}(\varOmega_{102})\}$

Now we can further explained the bijective soft sets as below with selection concept.

$H_1(\varOmega_{11}) = \{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$,$H_1(\varOmega_{12}) = \{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$,$H_1(\varOmega_{13}) = \{\vartheta_8, \vartheta_9, \vartheta_{10}\}$,$H_2(\varOmega_{21}) = \{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$,$H_2(\varOmega_{22}) = \{\vartheta_{10}\}$,$H_2(\varOmega_{23}) = \{\vartheta_8\}$,$H_3(\varOmega_{31}) = \{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$,$H_3(\varOmega_{32}) = \{\vartheta_8\}$,$H_3(\varOmega_{33}) = \{\vartheta_9, \vartheta_{10}\}$,$H_4(\varOmega_{41}) = \{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$,$H_4(\varOmega_{42}) = \{\vartheta_{10}\}$,$H_4(\varOmega_{43}) = \{\vartheta_8, \vartheta_9\}$,$H_5(\varOmega_{51}) = \{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$,$H_5(\varOmega_{52}) = \{\vartheta_7\}$,$H_5(\varOmega_{53}) = \{\vartheta_8, \vartheta_9, \vartheta_{10}\}$,$H_6(\varOmega_{61}) = \{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$,$H_6(\varOmega_{62}) = \{\vartheta_8\}$,$H_7(\varOmega_{71}) = \{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$,$H_7(\varOmega_{72}) = \{\vartheta_8, \vartheta_9, \vartheta_{10}\}$,$H_8(\varOmega_{81}) = \{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$,$H_8(\varOmega_{82}) = \{\vartheta_9\}$,$H_8(\varOmega_{83}) = \{\vartheta_8, \vartheta_9\}$,$H_9(\varOmega_{91}) = \{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$,$H_9(\varOmega_{92}) = \{\vartheta_8, \vartheta_9, \vartheta_{10}\}$,$H_{10}(\varOmega_{101}) = \{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$,$H_{10}(\varOmega_{102}) = \{\vartheta_8, \vartheta_9, \vartheta_{10}\}$

Now the conditions for bijective soft set are true. Suppose that (E2, SF2), union of the soft sets (E2, SF2) concept source, that is universal set U or $\bigcup_{\beta \in s} L(\beta) = U$. For instance, 2 SF values,$\varOmega_{11}, \varOmega_{12} \in SF_1, \varOmega_{11} \neq \varOmega_{12}(\varOmega_{11}) \bigcap (\varOmega_{12}) = \oslash$.

e. Desired statistical flow should have the following features as SF;
$[SF] = \{Ar\_p\_DTTIp, pkr\_p\_p\_pro\_p\_destip, Max, stddv, pkr\_p\_p\_pro\_psrcip, Min, Mean, seq, N\_inn\_conn\_p\_dsttip, N\_inn\_conn\_p\_srcip\}$. The features values should be as follow for effective feature selection for anomaly and intrusion in IoT traffic identification. $[SF] = \{Higher, High, Low, Better, Good, Low, \}$, Then the corresponding representation could be as given; $[SF] = \{\varOmega_{11}, \varOmega_{21}, \varOmega_{31}, \varOmega_{41}, \varOmega_{51}, \varOmega_{61}, \varOmega_{71}, \varOmega_{81}, \varOmega_{91}, \varOmega_{10}\}$ However, we select these features for effective anomaly and intrusion IoT traffic identification. **f**. Soft set representation for each features values from the statistical flow; $H(\varOmega_{11}) = \{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$;
$H(\varOmega_{21}) = \{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$;
$H(\varOmega_{31}) = \{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$;
$H(\varOmega_{41}) = \{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$;
$H(\varOmega_{51}) = \{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$;
$H(\varOmega_{61}) = \{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$;
$H(\varOmega_{71}) = \{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$;
g. After soft set representation, then we make correlation table form that bijective soft sets conducting and operation as we explained in Table 1.

h. After construction of correlation, we conduct correlation based on AND-Product as shown in Table. But due to page table size we are unable to show the complete table, so for this reason, we decompose the table with some function. For instance, suppose $\psi_1 = \{\psi_1, \psi_2, \psi_3, \psi_4, \psi_5, \psi_6, \psi_7\}$, with this assignment we can draw easily table as shown in Table2.

i. Similarly, we apply R-Union on AND Product Correlation as shown in Table 3.
g. After applying R-Union, then we conducted C-Intersection to achieve the final result. $\cap_{i=1\rightarrow 10 j=1\rightarrow 10}\{\bigcup rij\} = \{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$,
We get the above desired selected features using bijective soft set for anomaly and intrusion in IoT traffic identification.

B. Metrics On Feature Selection

1) Correlation Based Metric: To deal with effective features selection problem for anomaly and intrusion in Smart IoT network traffic identification, in this we adopted Pearson's product moment correlation to study in depth the relationship among independent features with target classes for prediction. In the 1880s, Francis Galton [56] proposed the product moment correlation, then later in 1896 Karl Pearson modified product moment correlation and then call as Pearson product moment correlation coefficient and based on statistical operation used to analyze the relation every two attributes, For instance, two variable X and Y. Then the Pearson's Correlation Coefficient between X and Y can be deliberate by the following given formula.

$$C_{X,Y} = \frac{Covariance(A, B)}{\sigma_x \sigma_y} \tag{1}$$

Here $C_{X,Y}$ is the correlation coefficient, and (X,Y) is the covariance, while $\sigma_x \sigma_y$ is the standard deviations of X and Y. Similarly in dataset, which have 2 sets, then the correlation coefficient can be calculated as;

$$C_{X,Y} = \frac{Covariance(A, B)}{\sigma_x \sigma_y} \tag{2}$$

Here n is the number of sample size and ai, bi is the ith data values. While A and B are the means. In this way, the coefficient values range to -1 and +1. if the value is near to +1 shows a strong relation between features, while values that are close to -1 show negative correlation mean the weak relationship between attributes, while the values that are close to 0 show no relation between attributes or features. Thus, to deal with effective features for anomaly intrusion in IoT traffic classification, we adopted Correlation attribute evaluation to rank and weight the feature based on Pearson's product moment correlation. The key idea behind this technique to the significance of the features set can be calculated correlation of the a set in a dataset with reliant feature and correlation between the features. However, in the machine learning model, a feature is considered effective, if the feature is highly correlated to class not related with each other. Through this idea a feature could be rank and analyze as follows:

$$Corr = \frac{kavg(corr_{fc})}{\sqrt{k + k(k-1)avg(corr_{ff})}} \tag{3}$$

TABLE I: Correlation Table

Feature Set	r_m1	r_m2	r_m3	r_m4	r_m5	r_m6	r_m7	r_m8	r_m9	r_m10
r_1	$H(\Omega_{11})\wedge H(\Omega_{11})$	$H(\Omega_{11})\wedge H(\Omega_{21})$	$H(\Omega_{11})\wedge H(\Omega_{31})$	$H(\Omega_{11})\wedge H(\Omega_{41})$	$H(\Omega_{11})\wedge H(\Omega_{51})$	$H(\Omega_{11})\wedge H(\Omega_{61})$	$H(\Omega_{11})\wedge H(\Omega_{71})$	$H(\Omega_{11})\wedge H(\Omega_{81})$	$H(\Omega_{11})\wedge H(\Omega_{91})$	$H(\Omega_{11})\wedge H(\Omega_{101})$
r_2	$H(\Omega_{21})\wedge H(\Omega_{11})$	$H(\Omega_{21})\wedge H(\Omega_{21})$	$H(\Omega_{21})\wedge H(\Omega_{31})$	$H(\Omega_{21})\wedge H(\Omega_{41})$	$H(\Omega_{21})\wedge H(\Omega_{51})$	$H(\Omega_{21})\wedge H(\Omega_{61})$	$H(\Omega_{21})\wedge H(\Omega_{71})$	$H(\Omega_{21})\wedge H(\Omega_{81})$	$H(\Omega_{21})\wedge H(\Omega_{91})$	$H(\Omega_{21})\wedge H(\Omega_{101})$
r_3	$H(\Omega_{31})\wedge H(\Omega_{31})$	$H(\Omega_{31})\wedge H(\Omega_{21})$	$H(\Omega_{31})\wedge H(\Omega_{31})$	$H(\Omega_{31})\wedge H(\Omega_{41})$	$H(\Omega_{31})\wedge H(\Omega_{51})$	$H(\Omega_{31})\wedge H(\Omega_{61})$	$H(\Omega_{31})\wedge H(\Omega_{71})$	$H(\Omega_{31})\wedge H(\Omega_{81})$	$H(\Omega_{31})\wedge H(\Omega_{91})$	$H(\Omega_{31})\wedge H(\Omega_{101})$
r_4	$H(\Omega_{41})\wedge H(\Omega_{41})$	$H(\Omega_{41})\wedge H(\Omega_{21})$	$H(\Omega_{41})\wedge H(\Omega_{31})$	$H(\Omega_{41})\wedge H(\Omega_{41})$	$H(\Omega_{41})\wedge H(\Omega_{51})$	$H(\Omega_{41})\wedge H(\Omega_{61})$	$H(\Omega_{41})\wedge H(\Omega_{71})$	$H(\Omega_{41})\wedge H(\Omega_{81})$	$H(\Omega_{41})\wedge H(\Omega_{91})$	$H(\Omega_{41})\wedge H(\Omega_{101})$
r_5	$H(\Omega_{51})\wedge H(\Omega_{11})$	$H(\Omega_{51})\wedge H(\Omega_{21})$	$H(\Omega_{51})\wedge H(\Omega_{31})$	$H(\Omega_{51})\wedge H(\Omega_{41})$	$H(\Omega_{51})\wedge H(\Omega_{51})$	$H(\Omega_{51})\wedge H(\Omega_{61})$	$H(\Omega_{51})\wedge H(\Omega_{71})$	$H(\Omega_{51})\wedge H(\Omega_{81})$	$H(\Omega_{51})\wedge H(\Omega_{91})$	$H(\Omega_{51})\wedge H(\Omega_{101})$
r_6	$H(\Omega_{61})\wedge H(\Omega_{11})$	$H(\Omega_{61})\wedge H(\Omega_{21})$	$H(\Omega_{61})\wedge H(\Omega_{31})$	$H(\Omega_{61})\wedge H(\Omega_{41})$	$H(\Omega_{61})\wedge H(\Omega_{51})$	$H(\Omega_{61})\wedge H(\Omega_{61})$	$H(\Omega_{61})\wedge H(\Omega_{71})$	$H(\Omega_{61})\wedge H(\Omega_{81})$	$H(\Omega_{61})\wedge H(\Omega_{91})$	$H(\Omega_{61})\wedge H(\Omega_{101})$
r_7	$H(\Omega_{71})\wedge H(\Omega_{11})$	$H(\Omega_{71})\wedge H(\Omega_{21})$	$H(\Omega_{71})\wedge H(\Omega_{31})$	$H(\Omega_{71})\wedge H(\Omega_{41})$	$H(\Omega_{71})\wedge H(\Omega_{51})$	$H(\Omega_{71})\wedge H(\Omega_{61})$	$H(\Omega_{71})\wedge H(\Omega_{71})$	$H(\Omega_{71})\wedge H(\Omega_{81})$	$H(\Omega_{71})\wedge H(\Omega_{91})$	$H(\Omega_{71})\wedge H(\Omega_{101})$
r_8	$H(\Omega_{81})\wedge H(\Omega_{11})$	$H(\Omega_{81})\wedge H(\Omega_{21})$	$H(\Omega_{81})\wedge H(\Omega_{31})$	$H(\Omega_{81})\wedge H(\Omega_{41})$	$H(\Omega_{81})\wedge H(\Omega_{51})$	$H(\Omega_{81})\wedge H(\Omega_{61})$	$H(\Omega_{81})\wedge H(\Omega_{71})$	$H(\Omega_{81})\wedge H(\Omega_{81})$	$H(\Omega_{81})\wedge H(\Omega_{91})$	$H(\Omega_{81})\wedge H(\Omega_{101})$
r_9	$H(\Omega_{91})\wedge H(\Omega_{11})$	$H(\Omega_{91})\wedge H(\Omega_{21})$	$H(\Omega_{91})\wedge H(\Omega_{31})$	$H(\Omega_{91})\wedge H(\Omega_{41})$	$H(\Omega_{91})\wedge H(\Omega_{51})$	$H(\Omega_{91})\wedge H(\Omega_{61})$	$H(\Omega_{91})\wedge H(\Omega_{71})$	$H(\Omega_{91})\wedge H(\Omega_{81})$	$H(\Omega_{91})\wedge H(\Omega_{91})$	$H(\Omega_{91})\wedge H(\Omega_{101})$
r_10	$H(\Omega_{101})\wedge H(\Omega_{11})$	$H(\Omega_{101})\wedge H(\Omega_{21})$	$H(\Omega_{101})\wedge H(\Omega_{31})$	$H(\Omega_{101})\wedge H(\Omega_{41})$	$H(\Omega_{101})\wedge H(\Omega_{51})$	$H(\Omega_{101})\wedge H(\Omega_{61})$	$H(\Omega_{101})\wedge H(\Omega_{71})$	$H(\Omega_{101})\wedge H(\Omega_{81})$	$H(\Omega_{101})\wedge H(\Omega_{91})$	$H(\Omega_{101})\wedge H(\Omega_{101})$

TABLE II: AND Product Correlation Table

Feature Set	r_1m	r_2m	r_3m	r_4m	r_5m	r_6m6	r_7m	r_8m	r_9m	r_10m
r_1n	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1
r_2n	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1
r_3n	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1
r_4n	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1
r_5n	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1
r_6n	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1
r_7n	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1
r_8n	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1
r_9n	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1
r_10n	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1	ψ_1

TABLE III: R-Union of Table 2.

	R-Union
$\bigcup_{m\longrightarrow 10} r_{1m}$	$\{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$
$\bigcup_{m\longrightarrow 10} r_{2m}$	$\{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$
$\bigcup_{m\longrightarrow 10} r_{3m}$	$\{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$
$\bigcup_{m\longrightarrow 10} r_{4m}$	$\{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7$
$\bigcup_{m\longrightarrow 10} r_{5m}$	$\{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$
$\bigcup_{m\longrightarrow 10} r_{6m}$	$\{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$
$\bigcup_{m\longrightarrow 10} r_{7m}$	$\{\vartheta_1, \vartheta_2, \vartheta_3, \vartheta_4, \vartheta_5, \vartheta_6, \vartheta_7\}$

Where Corr is the correlation between the features and kavg ($corr_{fc}$) is here the average of the correlation between attributes and reliant class, while average ($corr_{ff}$) is used for the average correlations among the attributes and here k indicate the number of features. While corr indicate to evaluate the attributes set in the attribute selection algorithm. Using the given mathematical equation the attribute set could be analyze below given factor. 1. The more correlation between the attributes set indicates the weak correlation among the features set and reliant class. 2. The more correlation among the attribute set and reliant class shows the more correlation among the features and reliant class. 3. Similarly, the more attributes shows a high correlation among the features and reliant class. Through these statistical method for effective features selection, we conduct this technique by Weka application.

2) Accuracy (ACC) Based metric: Subsequentlyvapplying Correlation, it is utmost important to find out effective features for a Machine Learning (ML) classifier. For this objective, we used the wrapper technique based on the accuracy ACC metric. Even though the ROC curve (AUC) metric is more effective to use, but the AUC metric is useful for imbalance internet traffic classification [34][57][58]. However, we are attentiveness to predict the best attributes which give more information for IoT anomaly and intrusion identification using ML algorithms; thus we apply ACC metric. The highest ACC values show the ML classifier could give a high-performance result [59]. ACC metric is important for the ranking of a feature. As we discuss, we will rank the feature by ACC metric, for this purpose we also employ this method and achieved better results to select the features whose values are very high.

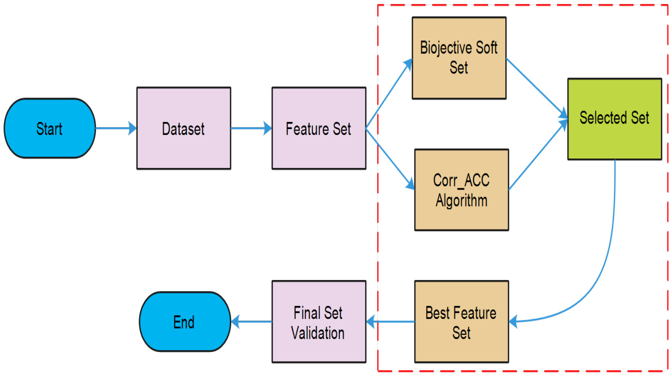


Fig. 2: Proposed Frame Work For Feature Selection

C. Proposed Feature Selection Algorithm

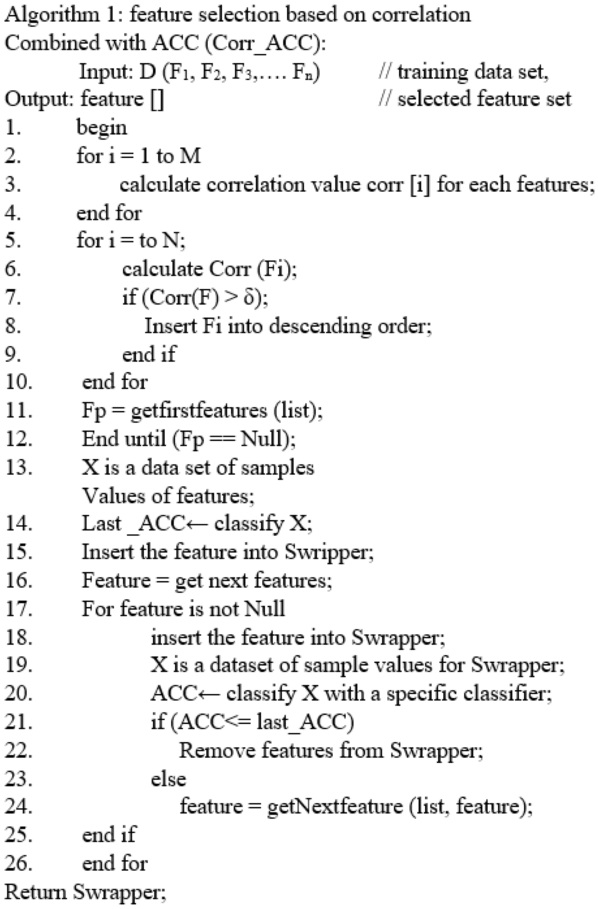
In this section, we delineate the submitted feature selection algorithm named Corracc. Corracc in the first phase filters the attributes with Correlation and then filtrate the selected attributes with high ACC metric a particular machine learning classifiers. The Corracc algorithm select the optimal feature set out from the selected features set. The details is in the following section.

1) Corracc algorithm: In this subcategory, we demonstrate the proposed Corracc approach and pseudo code of the proposed algorithm as shown in the Figure 3. In the related work section that, selection effective feature is very important in term of IoT anomy and intrusion traffic identification. Then the algorithm filter all the feature with Corr metric to choose optimum attributes that are associated to one another. However, the algorithm consists of 2 phases. In the first phase, line 1-10 in Fig. 3. Suppose, given dataset is D and m classes and n attributes of the dataset. In the fig.3 Corracc filter the features with Corr metric values. The Corr metric value of each features is determined as shown an algorithm in line 3. Corracc then compute the correlation values among each attribute in line 6. Moreover, if the correlation value is higher than threshold value then the algorithm place features in the list in descending row. More in depth, the greater the threshold value the higher speed up the attributes selection method. However, it will decrease identification of a particular ML classifier [60].

Similarly, the algorithm will get the correlated attributes set in the 11. In the second phase from 13 to 27 line, the algorithm will filter the features set by using ACC metric of a utilized and selected machine learning classifier and then the algorithm will select the features from a feature list filtering one by one feature ACC metric value whose value is high with respect to ACC metric. Similarly, in the remaining steps the algorithm will first used the wrapper technique to filter the feature and then take a decision to remove or not. If the selected feature value are very low then the algorithm will remove otherwise forward to Swrapper.

IV. Evaluation Methodology

In this section, we delineate the dataset and evaluation criteria used for anomaly and intrusion IoT traffic identification.



```
Algorithm 1: feature selection based on correlation
Combined with ACC (Corr_ACC):
        Input: D ($F_1$, $F_2$, $F_3$,…. $F_n$)          // training data set,
Output: feature []                            // selected feature set
1.      begin
2.      for i = 1 to M
3.          calculate correlation value corr [i] for each features;
4.      end for
5.      for i = to N;
6.          calculate Corr (Fi);
7.          if (Corr(F) > $\delta$);
8.             Insert Fi into descending order;
9.          end if
10.     end for
11.     Fp = getfirstfeatures (list);
12.     End until (Fp == Null);
13.     X is a data set of samples
        Values of features;
14.     Last _ACC← classify X;
15.     Insert the feature into Swripper;
16.     Feature = get next features;
17.     For feature is not Null
18.            insert the feature into Swrapper;
19.            X is a dataset of sample values for Swrapper;
20.            ACC← classify X with a specific classifier;
21.            if (ACC<= last_ACC)
22.               Remove features from Swrapper;
23.            else
24.               feature = getNextfeature (list, feature);
25.     end if
26.     end for
Return Swrapper;
```

Fig. 3: Proposed Corracc algorithm

A. Bot-IoT Data Set

In this paper, we used a new Bot-IoT dataset [21][61]. Bot-IoT dataset incorporate both IoT and normal traffic as well as traffic with different types of attacks which is usually used by botnets attacks. However, Bot-IoT dataset is developed in a realistic testbed and then generate its features with labeled. Moreover, additional attributes were also generated to improve the prediction performance capabilities of the ML classifiers model. Labeled features indicate an attacks flow traffic, its categories, and subcategory for multiclass purposes. The testbed consists of three main components: Simulated Internet of Things (IoT) services, network platform, and extraction features and Forensics analytics. However, for the IoT scenarios, they applied five Internet of Things (IoT) such as: 1. A weather checking IoT device, which generates time to time information such as temperature, humidity and atmosphere pressure. Smart Phone or Weather Station. 2. A smart cooling fridge, which produces or measures the fridge temperature and adjustment of fridge temperature when necessary. 3. Smart Lights, it is a motion activated lights based on the pseudo-random general signal, e.g. Motion lights. 4. Smart Door, it is a remotely activated door, which opens and closes based on a probabilistic input. 5. A smart thermostat, which controls the temperature of the house by starting the Air-conditioning system.

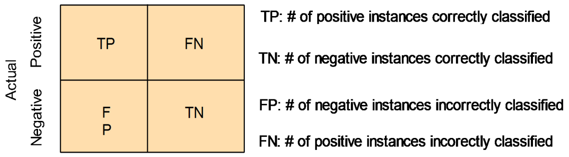

Actual
Positive
Negative
TP
FN
F P
TN
TP: # of positive instances correctly classified
TN: # of negative instances correctly classified
FP: # of negative instances incorrectly classified
FN: # of positive instances incorectly classified

Fig. 4: Confusion Matrix for Results Evaluation

B. Performance Measurements

To measure the identification or classification performance of classifiers results. The confusion metrics are the main and important base for performance measurement. Figure 4, the confusion matrix with details and graphical representation for performance measurement evaluation of a machine learning classifier. In the figure.4. Row shows the actual class's instance and column indicates the identified class instances. However, the measurement that mostly researchers used for their model performance evaluation are given below with details.

- True Positive (TP): It indicate that L attack is correctly identified as belong to L attacks group.
- True Negative (TN): It indicate that L attacks is correctly identified as not belong to L attacks group.
- False Positive (FP): Its Indicate that L attack is not correctly identified as belong to L attack group.
- False Negative (FN): It indicate that L attack is not correctly identified as not belong to L attack group.

Figure 4 shown the graphical representation of confusion matrix.

- Accuracy: It can be described as the correctly identified samples in overall identified samples. The details mathematical formula is given below.

$$Accuracy = \frac{(TP+TN)}{(TP+TN+FP+FN)} \tag{4}$$

  Using accuracy result a ML algorithm performance can be measure. It indicates the overall effectiveness of identification model.
- Precision: it can be describe as the percentage of sample correctly identified Class L in all those were identified class L.

$$Precission = \frac{TP}{(TP+FP)} \tag{5}$$

- Sensitivity: Sensitivity can be calculated as correctly identified samples divided by overall dataset sample. It can be also used as a recall in anomaly or intrusion attacks identification in IoT network. However, the detail mathematical formula is given below with details.

$$Sensitivity = \frac{TP}{(TP+FN)} \tag{6}$$

- Specificity: In simple words the machine learning (ML) classifier performance ability to identify the negative result. It can be explain as the True Negative divide by the sum of False Positive and True Negative.

$$Specificity = \frac{TN}{(FP+TN)} \tag{7}$$

However, we used the above given metrics for the ML classifiers performance evaluation.

V. Results And Analysis

In this section, we enlighten the results and analysis of our experiment with details and we proposed a new approach for effective feature selection for anomaly and intrusion IoT traffic identification. Our proposed method select seven best feature out of thirty-nine features, which carry enough information for accurate anomaly and intrusion detection in the IoT network environment. In this systematic investigation study, we applied four different machine learning classifiers for performance evaluation which are Decision Tree (C4.5), Support Vector Machine (SVM), Random Forest (RF) and NaÃŕve Bayes Machine Learning Classifiers. All the used machine learning (ML) identifiers achieve deeply promising outcome results for effective features selection for anomaly and intrusion in IoT traffic identification using the selected feature set, selected by our proposed approach with respective accuracy, precision, sensitivity, and specificity. However, using the selected features and given machine learning classifiers, support vector machine (SVM) algorithm achieve low accuracy results as compared to other applied ML classifiers accuracy results for IoT anomaly and intrusion identification. As shown in Figure 5, the NaÃŕve Bayes ML classifiers achieve lightly better accuracy results as compared to SVM classifier. But the remaining C4.5 and Random Forest gets very promising accuracy results and identify all the attacks and normal traffic very effectively with respect to accuracy metric. Thus, C4.5 ML classifier achieves the maximum accuracy result using Bot-IoT dataset and selected features set for the identification attacks in IoT network as 99.9%. More in depth, all the attacks and normal traffics are identified very effectively, but only two attacks SSR and Data Theft are identified slightly low with respect to accuracy as shown in Figure 5.

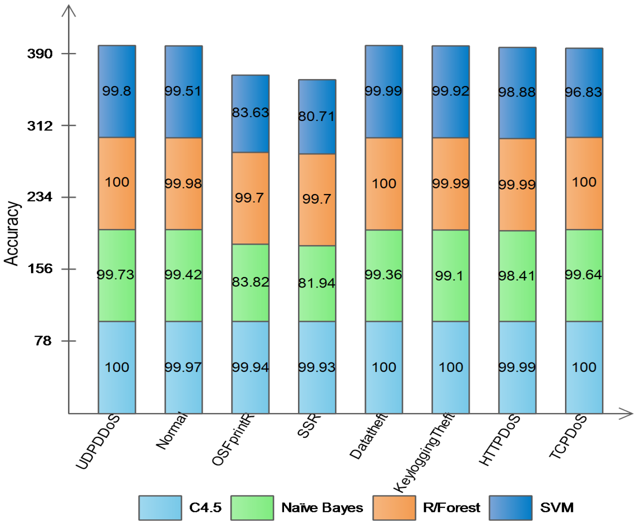


Fig. 5: Accuracy Results

Similarly, Figure 6 shows the precision result, in which it is clear that UDPDoS, TCPDoS, and SSR are attacks are classified effectively as compared to Data Theft and Keylogging attacks. Moreover, normal traffics are also classified very precisely with respect to precision metric, while the remaining

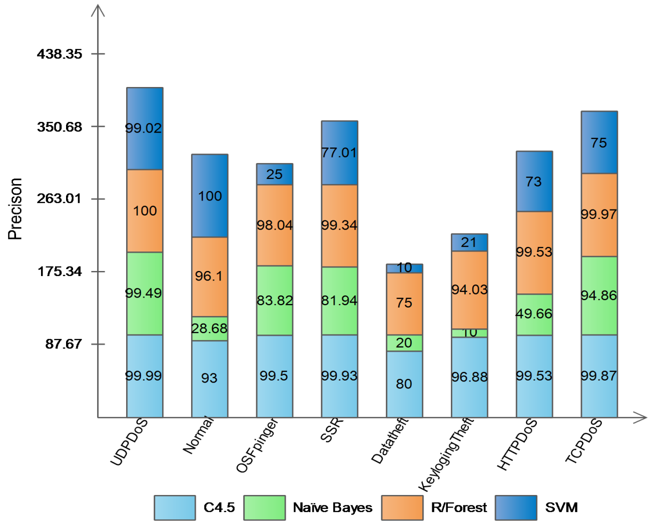


Fig. 6: Precision Results

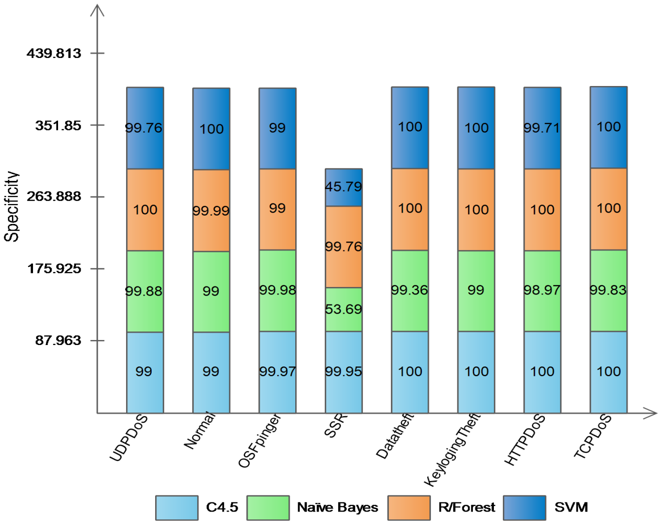


Fig. 8: Specificity Results

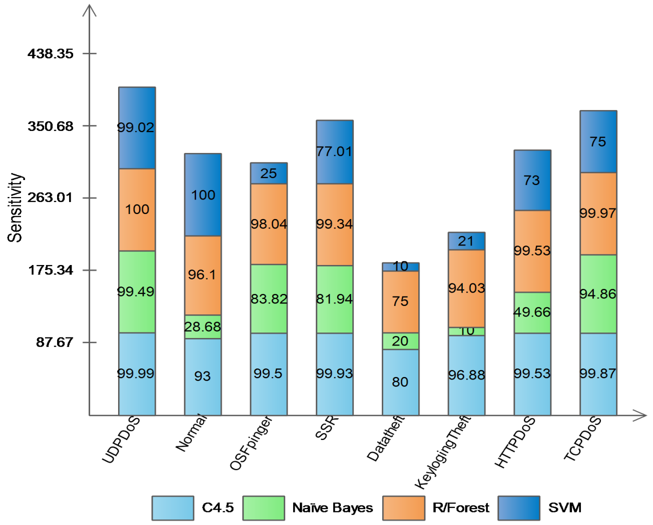


Fig. 7: Sensitivity Results

attacks are classified slightly low. However, C4.5 and Random Forest machine learning algorithms achieve very optimal precision results as compared to Naive Bayes and SVM. All the used machine learning classifiers achieve promising results with respective sensitivity. However, using the selected features set and given machine learning classifiers, support vector machine (SVM) algorithm achieve shallow sensitivity results as compared to other applied ML classifiers sensitivity results for IoT anomaly and intrusion identification. As shown in Figure 7, the Naive Bayes ML classifiers achieve better sensitivity results as compared to SVM classifier. However, C4.5 and Random Forest delivers absolutely useful sensitivity results and identify all the attacks and normal traffic very precisely with respect to the sensitivity metric. C4.5 ML classifier achieves enough good sensitivity result using Bot-IoT dataset and selected features set for the identification attacks in IoT network as 92.3%. However, all the attacks and normal traffics are identified effectively, but only two attacks Data Theft and Keylogging are identified slightly low with respect to sensitivity results as shown in Figure 7. For the specificity metric evaluation, all the machine learning classifiers gives promising results. But only SVM and NaÃŕve Bayes gives slightly low specificity results and give accurate results for identifying the attacks. However, comparing the specificity results of each applied machine classifier, C4.5 decision tree and Random Forest gives promising results as compared to NaÃŕve Bayes and SVM with respective 99.74%, 93.71%, 99.84%, and 93%. Similarly, all the attacks and normal traffics are identified effectively but only two attacks SSR and identified slightly low with respect to specificity results as shown in Figure 8.

VI. Analysis And Discussion

Although, the results that we achieve in this research paper by using our proposed approaches are effective by conducting Machine Learning (ML) algorithms with respective accuracy, precision, sensitivity and specificity by using Bot-IoT dataset. Nevertheless, after experimental analysis and study some insightful information that we learnt for effective feature selection for anomaly and intrusion in IoT traffic identification are given below.

- In this work, it is evident that the proposed approach select optimum features set for anomaly and intrusion in IoT traffic identification using Bot-IoT dataset with regard to accuracy, precision, sensitivity, and specificity metrics.
- In this study, it is clearly seen that the applied approach is enough efficient for the selection of efficient features and it is noticeable that the feature carry sufficient identification knowledge for IoT anomaly and intrusion attacks traffic classification such as (a) mean (b) stddev (c) min (d) max (e) AR_P_Proto_P_DstIP (f) Pkts_P_State_P_DestIP (g) Pkts_P_State_P_SrcIP.
- In the experimental results evaluation it is noticeable that the four Machine Learning (ML) classifiers gives very promising performance results by using Bot-IoT dataset

and it's selected features set. However, only Data Theft attacks is identified low comparing with other attacks and normal traffic. It's due to not sufficient instances of attacks. Nevertheless, it is clear in this study that the applied approach can select effective feature for intrusion attacks in IoT network.

- The ML algorithms that we used in this study gives very appropriate performance results for IoT attacks traffics identification. Nonetheless, we found that Random Forest ML and C4.5 classifiers results performance are encouraging using Bot-IoT by comparing with others applied ML classiïňĄers in anomaly and intrusion in IoT traffic identification.

VII. Conclusion

To address effective features selection problem, in this research study, we apply bijective soft set technique to choose effective features, and then a new feature selection metric called Corr_ACC is introduced. Afterward, we designed a new feature selection algorithm called Corracc based on Corr_ACC, which utilized wrapper technique to select effective features set for a specific classifier with ACC metric. Then, we analyze the approaches using four different machine learning classifiers using Bot-IoT traces captured dataset in smart cities IoT network environment. After experiment it clear that our approaches can get more than 95% accuracy, sensitivity, and specificity results respectively. In the experimental analysis, it is clear that the proposed approaches were able to effectively select best feature set and identify anomaly and intrusion attacks in IoT network. It is also clear that the ML classifiers are able to classify the attacks effectively and normal traffics in IoT without any altering the training dataset. Moreover, the features that is selected by the proposed approach gives very well results in term of accuracy, precision, sensitivity and specificity metric. The features set determined by our approaches are (a) mean (b) stddev (c) min (d) max (e) AR_P_Proto_P_DstIP (f) Pkts_P_State_P_DestIP (g) Pkts_P_State_P_SrcIP, which carry enough information for anomaly and intrusion in IoT traffic identification. The applied four ML algorithms achieve auspicious performance results, but in the experiment analysis, C4.5 decision tree and RandomForest classifiers performance are effective as compare to other applied ML classifiers. However, our proposed approaches are very effective for effective feature selection for anomaly and intrusion in IoT traffic identification.

Acknowledgment

This work is supported by the National Key research and Development Plan (Grant No. 2018YFB0803504), the Guangdong Province Key Research and Development Plan (Grant No. 2019B010137004) and the National Natural Science Foundation of China under Grant No.61871140, and Guangdong Province Universities and Colleges Pearl River Scholar Funded Scheme (2019).

References

[1] 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.

[2] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Implementing lightweight iot-ids on raspberry pi using correlation-based feature selection and its performance evaluation," in *International Conference on Advanced Information Networking and Applications*. Springer, 2019, pp. 458–469.

[3] S. Deep, X. Zheng, and L. Hamey, "A survey of security and privacy issues in the internet of things from the layered context," *arXiv preprint arXiv:1903.00846*, 2019.

[4] A. Jolfaei and K. Kant, "Data security in multiparty edge computing environments," Temple University Philadelphia United States, Tech. Rep., 2019.

[5] M. Li, Y. Sun, H. Lu, S. Maharjan, and Z. Tian, "Deep reinforcement learning for partially observable data poisoning attack in crowdsensing systems," *IEEE Internet of Things Journal*, 2019.

[6] 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

[7] J. P. Anderson, "Computer security threat monitoring and surveillance, 1980. lastaccessed: Novmeber 30, 2008."

[8] D. E. Denning, "An intrusion-detection model," *IEEE Transactions on software engineering*, no. 2, pp. 222–232, 1987.

[9] 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*, 2019.

[10] 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.

[11] X. Huang and X. Du, "Achieving big data privacy via hybrid cloud," in *2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2014, pp. 512–517.

[12] L. Xiao, Y. Li, X. Huang, and X. Du, "Cloud-based malware detection game for mobile devices with offloading," *IEEE Transactions on Mobile Computing*, vol. 16, no. 10, pp. 2742–2750, 2017.

[13] X. Du, M. Guizani, Y. Xiao, and H.-H. Chen, "Defending dos attacks on broadcast authentication in wireless sensor networks," in *2008 IEEE International Conference on Communications*. IEEE, 2008, pp. 1653–1657.

[14] R. Vinayakumar, M. Alazab, A. Jolfaei, K. Soman, and P. Poornachandran, "Ransomware triage using deep learning: twitter as a case study," in *2019 Cybersecurity and Cyberforensics Conference (CCC)*. IEEE, 2019, pp. 67–73.

[15] 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.

[16] R. Xue, L. Wang, and J. Chen, "Using the iot to construct ubiquitous learning environment," in *2011 Second International Conference on Mechanic Automation and Control Engineering*. IEEE, 2011, pp. 7878–7880.

[17] M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1996–2018, 2014.

[18] 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*, 2019.

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

[20] 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.

[21] 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:1811.00701*, 2018.

[22] A. Musaddiq, Y. B. Zikria, O. Hahm, H. Yu, A. K. Bashir, and S. W. Kim, "A survey on resource management in iot operating systems," *IEEE Access*, vol. 6, pp. 8459–8482, 2018.

[23] M. Shafiq, X. Yu, A. A. Laghari, and D. Wang, “Effective feature selection for 5g im applications traffic classification,” *Mobile Information Systems*, vol. 2017, 2017.

[24] M. Shafiq and X. Yu, “Effective packet number for 5g im wechat application at early stage traffic classification,” *Mobile Information Systems*, vol. 2017, 2017.

[25] M. Shafiq, X. Yu, A. A. Laghari, L. Yao, N. K. Karn, and F. Abdessamia, “Network traffic classification techniques and comparative analysis using machine learning algorithms,” in *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*. IEEE, 2016, pp. 2451–2455.

[26] M. Shafiq, X. Yu, and A. A. Laghari, “Wechat text messages service flow traffic classification using machine learning technique,” in *2016 6th International Conference on IT Convergence and Security (ICITCS)*. IEEE, 2016, pp. 1–5.

[27] M. Shafiq, X. Yu, A. A. Laghari, L. Yao, N. K. Karn, F. Abdesssamia *et al.*, “Wechat text and picture messages service flow traffic classification using machine learning technique,” in *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. IEEE, 2016, pp. 58–62.

[28] 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.

[29] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, “A survey of key management schemes in wireless sensor networks,” *Computer Communications*, vol. 30, no. 11-12, pp. 2314–2341, 2007.

[30] X. Du and H.-H. Chen, “Security in wireless sensor networks,” *IEEE Wireless Communications*, vol. 15, no. 4, pp. 60–66, 2008.

[31] 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.

[32] Y. Xiao, X. Du, J. Zhang, F. Hu, and S. Guizani, “Internet protocol television (IPTV): the killer application for the next-generation internet,” *IEEE Communications Magazine*, vol. 45, no. 11, pp. 126–134, 2007.

[33] 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.

[34] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, “Selection of effective machine learning algorithm and bot-iot attacks traffic identification for internet of things in smart city,” *Future Generation Computer Systems*, 2020.

[35] A. K. Bashir, R. Arul, S. Basheer, G. Raja, R. Jayaraman, and N. M. F. Qureshi, “An optimal multitier resource allocation of cloud ran in 5g using machine learning,” *Transactions on Emerging Telecommunications Technologies*, p. e3627, 2019.

[36] 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.

[37] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, “N-baiotâĂŤnetwork-based detection of iot botnet attacks using deep autoencoders,” *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12–22, 2018.

[38] 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.

[39] 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*, 2018.

[40] Z. Tian, W. Shi, Y. Wang, C. Zhu, X. Du, S. Su, Y. Sun, and N. Guizani, “Real time lateral movement detection based on evidence reasoning network for edge computing environment,” *IEEE Transactions on Industrial Informatics*, 2019.

[41] X. Du, Y. Xiao, M. Guizani, and H. Chen, “An effective key management scheme for heterogeneous sensor networks,” *Ad Hoc Networks*, vol. 5, no. 1, pp. 24–34, 2007.

[42] X. Du, M. Guizani, Y. Xiao, and H. Chen, “A routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks,” *IEEE Trans. Wireless Communications*, vol. 8, no. 3, pp. 1223–1229, 2009.

[43] Z. Tian, M. Li, M. Qiu, Y. Sun, and S. Su, “Block-def: A secure digital evidence framework using blockchain,” *Information Sciences*, vol. 491, pp. 151–165, 2019.

[44] D. Molodtsov, “Soft set theoryâĂŤfirst results,” *Computers & Mathematics with Applications*, vol. 37, no. 4-5, pp. 19–31, 1999.

[45] P. K. Maji, R. Biswas, and A. Roy, “Soft set theory,” *Computers & Mathematics with Applications*, vol. 45, no. 4-5, pp. 555–562, 2003.

[46] E. Türkmen and A. Pancar, “On some new operations in soft module theory,” *Neural Computing and Applications*, vol. 22, no. 6, pp. 1233–1237, 2013.

[47] X. Du, M. Zhang, K. E. Nygard, S. Guizani, and H.-H. Chen, “Self-healing sensor networks with distributed decision making,” *International Journal of Sensor Networks*, vol. 2, no. 5-6, pp. 289–298, 2007.

[48] P. K. Maji, R. Biswas, and A. R. Roy, “Intuitionistic fuzzy soft sets,” *Journal of fuzzy mathematics*, vol. 9, no. 3, pp. 677–692, 2001.

[49] 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.

[50] K. Hayat, M. I. Ali, B.-Y. Cao, and X.-P. Yang, “A new type-2 soft set: Type-2 soft graphs and their applications,” *Advances in Fuzzy Systems*, vol. 2017, 2017.

[51] K. Hayat, M. I. Ali, F. Karaaslan, B.-Y. Cao, and M. H. Shah, “Design concept evaluation using soft sets based on acceptable and satisfactory levels: An integrated topsis and shannon entropy,” *Soft Computing*, vol. 24, no. 3, pp. 2229–2263, 2020.

[52] V. Tiwari, P. K. Jain, and P. Tandon, “A bijective soft set theoretic approach for concept selection in design process,” *Journal of Engineering Design*, vol. 28, no. 2, pp. 100–117, 2017.

[53] M. Li, Y. Meng, J. Liu, H. Zhu, X. Liang, Y. Liu, and N. Ruan, “When csi meets public wifi: Inferring your mobile phone password via wifi signals,” in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016, pp. 1068–1079.

[54] 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.

[55] N. Çağman and S. Enginoğlu, “Soft set theory and uni–int decision making,” *European Journal of Operational Research*, vol. 207, no. 2, pp. 848–855, 2010.

[56] R. E. Fancher, “Galton on examinations: An unpublished step in the invention of correlation,” *Isis*, vol. 80, no. 3, pp. 446–455, 1989.

[57] S. Sebastio, E. Baranov, F. Biondi, O. Decourbe, T. Given-Wilson, A. Legay, C. Puodzius, and J. Quilbeuf, “Optimizing symbolic execution for malware behavior classification,” *Computers & Security*, p. 101775, 2020.

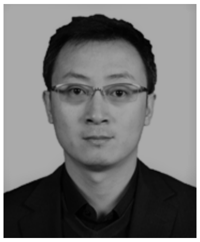
[58] O. Olukoya, L. Mackenzie, and I. Omoronyia, “Towards using unstructured user input request for malware detection,” *Computers & Security*, p. 101783, 2020.

[59] X. Du, M. Shayman, and M. Rozenblit, “Implementation and performance analysis of snmp on a tls/tcp base,” in *2001 IEEE/IFIP International Symposium on Integrated Network Management Proceedings. Integrated Network Management VII. Integrated Management Strategies for the New Millennium (Cat. No. 01EX470)*. IEEE, 2001, pp. 453–466.

[60] 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.

[61] I. Van der Elzen and J. van Heugten, “Techniques for detecting compromised iot devices,” *University of Amsterdam*, 2017.

Muhammad Shafiq was born in Pakistan. He received the B.S. degree with honor rank in computer science from the Faculty of Computer Science, Malakand University, Chakdara, Pakistan, in 2009, and the M.S. degree in computer science from Faculty of Computer Science, Malakand University, Chakdara, Pakistan, in 2011. He is received the Ph.D. degree at the School of Computer Science and Technology, Harbin Institute of Technology, Harbin, China, in 2018. He is currently pursuing the Post-Doctorate. at the Cyberspace Institute of Advance Technology, Guangzhou University, Guangzhou, China. His current research areas of interests include IoT Security, IoT anomaly and intrusion traffic classification, IoT management, Network Traffic Classification and Network Security, Cloud Computing.



Zhihong Tian Ph.D., professor, PHD supervisor. Dean of cyberspace institute of advanced technology, Guangzhou University. Standing director of CyberSecurity Association of China. Member of China Computer Federation. From 2003 to 2016, he worked at Harbin Institute of Technology. His current research interest is computer network and network security.

Ali Kashif Bashir is a Senior Lecturer at the Department of Computing and Mathematics, Manchester Metropolitan University, United Kingdom. His past assignments include Associate Professor of Information and Communication Technologies, Faculty of Science and Technology, University of the Faroe Islands, Denmark; Osaka University, Japan; Nara National College of Technology, Japan; the National Fusion Research Institute, South Korea; Southern Power Company Ltd., South Korea, and the Seoul Metropolitan Government, South Korea. He received his Ph.D. in computer science and engineering from Korea University, South Korea. MS from Ajou University, South Korea and BS from University of Management and Technology, Pakistan. He is supervising/co-supervising several graduate (MS and Ph.D.) students. His research interests include internet of things, wireless networks, distributed systems, network/cybersecurity, network function virtualization, etc. He has authored over 80 peer-reviewed articles. He has served as a chair (program, publicity, and track) on top conferences and workshops. He has delivered over 20 invited and keynote talks in seven countries. He is a Distinguished Speaker, ACM; Senior Member of IEEE; Member, ACM; Member, IEEE Young Professionals; Member, International Association of Educators and Researchers, UK. He is serving as the Editor-in-chief of the IEEE FUTURE DIRECTIONS NEWSLETTER. He is advising several startups in the field of STEM-based education, robotics, internet of things, and blockchain.

Xiaojiang(James) Du Xiaojiang Du is currently a Tenured Professor with the Department of Computer and Information Sciences, Temple University, Philadelphia, USA. He has authored over 260 journal and conference papers in these areas, and a book (Springer). His research interests are wireless communications, wireless networks, security, and systems. He has been awarded over 5 million U.S. dollars research grants from the U.S. National Science Foundation, Army Research Office, Air Force Research Laboratory, NASA, the State of Pennsylvania, and Amazon. He is a Life Member ACM. He serves on the editorial boards of three international journals.

Mohsen Guizani received the B.S. (with distinction) and M.S. degrees in electrical engineering, the M.S. and Ph.D. degrees in computer engineering from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively. He is currently a Professor at the Computer Science and Engineering Department in Qatar University, Qatar. His research interests include wireless communications and mobile computing, computer networks, mobile cloud computing, security, and smart grid. Throughout his career, he received three teaching awards and four research awards. He also received the 2017 IEEE Communications Society WTC Recognition Award as well as the 2018 AdHoc Technical Committee Recognition Award for his contribution to outstanding research in wireless communications and Ad-Hoc Sensor networks. He was the Chair of the IEEE Communications Society Wireless Technical Committee and the Chair of the TAOS Technical Committee. He served as the IEEE Computer Society Distinguished Speaker and is currently the IEEE ComSoc Distinguished Lecturer. He is a Fellow of IEEE and a Senior Member of ACM.