Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 8864301, 10 pages
https://doi.org/10.1155/2020/8864301

Research Article

SoftSystem: Smart Edge Computing Device Selection Method for IoT Based on Soft Set Technique

Muhammad Shafiq[1], **Zhihong Tian**[1], **Ali Kashif Bashir**[2], **Korhan Cengiz**[3] and **Adnan Tahir**[4]

[1]*Department of Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou, China 510006*
[2]*Department of Computing and Mathematics, Manchester Metropolitan University, UK*
[3]*Department of Electrical-Electronics Engineering, Trakya University, 22030 Edirne, Turkey*
[4]*College of Information and Communication Engineering, Shenzhen University, Shenzhen, China*

Correspondence should be addressed to Zhihong Tian; tianzhihong@gzhu.edu.cn

Received 22 August 2020; Revised 15 September 2020; Accepted 30 September 2020; Published 9 October 2020

Academic Editor: Rahul Yadav

The Internet of Things (IoT) is growing day by day, and new IoT devices are introduced and interconnected. Due to this rapid growth, IoT faces several issues related to communication in the edge computing network. The critical issue in these networks is the effective edge computing IoT device selection whenever there are several edge nodes to carry information. To overcome this problem, in this paper, we proposed a new framework model named SoftSystem based on the soft set technique that recommends useful IIoT devices. Then, we proposed an algorithm named Softsystemalgo. For the proposed system, three different parameters are selected: IoT Device Security (IDSC), IoT Device Storage (IDST), and IoT Device Communication Speed (IDCS). We also find out the most significant parameters from the given set of parameters. It is evident that our proposed system is effective for the selection of edge computing devices in the IoT network.

1. Introduction

Recently, more and more services are changed from cloud to edge device in the IIoT network because of saving processing time and ensuring the processing data in a short time response [1]. Similarly, edge device in a network ensures the reliability and saved bandwidth with dealing a large portion of data. On the other hand, the Industrial Internet of Things (IIoT) got very important in IoT technology. IoT is the technology used to interconnect Device-to-Device (D2D). Due to interconnected intelligent sensors in the IoT network environment, life becomes very convenient. As in this technology, numerous smart IoT devices are interconnected with each other for communication, generating and exchanging data for different purposes such as decision making and providing better services for better lives. More in-depth, due to IoT technology, life becomes more convenient, and it became an essential part of our daily life. However, this technology has some issues that should study more in-depth and proposed a useful model for communication from one node to another node, especially in the edge computing network environment. The critical issue is the effective IIoT device recommendation or selection, whenever there are several IoT devices to carry a task. In Figure 1 is shown the fundamental IoT five layers as (1) Perceptional Layer, (2) Network Layer, (3) Middleware Layer, (4) Application Layers, and (5) Business Layer. In the IIoT network, the connected smart devices are connected through wireless communication between intelligent nodes. However, the interconnected intelligent nodes are temporally connected with each other, and mostly the developed topology of this network changed from time to time whenever need. The question arises here, which is why the connection between node to node or machine to machine temporally is due to

the activation and deactivation of smart nodes. The essential thing in the network is node discovery functionality. It means a network can be easily detected or discovered in other network environments for a specific task, or this network can support One-hop functionality, a functionality, which supports sending and receiving a job from accessing other networks [2] and environments [3]. However, in other words, such kind of network is known as Delay Tolerant Networks (DTNS), or it can say Opportunistic Network (ON).

Similarly, in 2018, Cuka at el. [4] studied the IoT device selection in the opportunistic network environment, and it is evident that due to the wireless connection between smart devices in an opportunistic network, the routing task is a very challenging problem in this network. However, their study showed that the base station is carried great for long-distance routing in this network environment. Recently, this network got very important because of their different network nature as compared to other network nature environment, and due to these big differences of this network, these networks are overgrowing compared to other networks. As we mentioned earlier, the opportunistic network is spreading rapidly, but on the other side, the security problem is also rapidly growing with the development of this network. In an opportunistic network, the IoT system collects the information for effective communication between smart. Thus, the end-user should keep an eye on the flow of data and should filter the flow traffic of IoT devices in the opportunistic network [5, 6]. However, in an opportunistic network environment, when communication is not possible between two smart devices or there is no path, the secure communication to carry information from one smart device to another smart device, or we can say when the communication between two smart devices is no longer available than in this situation, the network requires the decision of IoT device to overcome the problem and make a secure connection between two different smart devices. However, sometimes it is not possible due to the low storage of IoT devices to support information. In the opportunistic network, the storage capacity of the selected devices is the main challenging issue in these networks.

Similarly, in mobile cloud computing, the electric energy is the main issue; for this purpose, the authors in [7] introduced an adaptive heuristic algorithm to overcome the problem of electric energy of the data center. Likewise, to overcome the problem of energy consumption, the authors in 2020 [8] proposed adaptive heuristic algorithms for the Virtual Machine (VM) selection. In their study, they showed that their proposed algorithm is effective for reducing energy consumption and validate the proposed approach by using the CloudSim simulator. As we discussed in the above lines that nowadays energy consumptions is a very big issue in cloud computing; similarly, numerous researchers try their best to solve the emerging problems as in [9, 10] studied the emerging issue in cloud computing related to energy consumption problem and proposed different method algorithms. However, their proposed approaches are very effective and they showed that the proposed approaches overcome the problem of energy consumption in cloud computing. In their study, they implemented the CloudSim simulator for the validation of their proposed approaches. Similarly, for the Quality of Service (QoS) and energy-saving problem in cloud and IoT technology, the author in [11] studied the details of energy-saving and QoS issues and gave a very brief survey. Their survey mainly focuses on the optimizations of QoS and energy saving. Likewise in 2018, the authors in [12] present a survey to summarize bit IoT and fog challenges. For this purpose, the authors try their best to summarize the challenges related to fog and big IoT challenges and also present the most significant applications related to fog and IoT technologies.

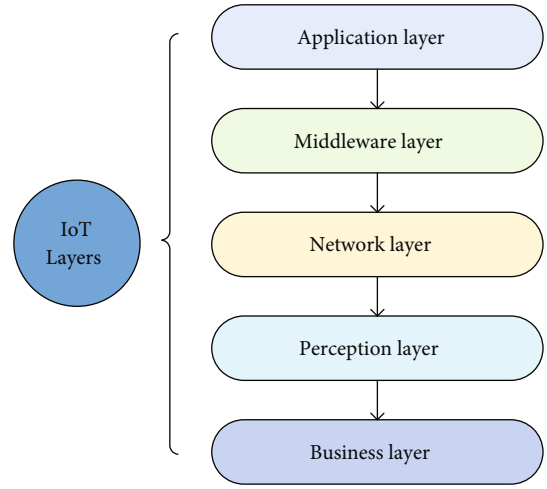

Figure 1: Basic IoT technology layers.

For the effective communication and recommendation of IoT devices in the opportunistic network, it is necessary to keep an eye on the storage capacity parameter of the device before to be recommended. Thus, due to this factor, in this paper, we considered the storage parameter of IoT devices for the recommendation of IoT devices in the IoT network. In this study, we used a soft set technique to overcome the problem of IoT devices' recommendation in the network. This method is based on the mathematic function process, firstly introduced by Molodtsov in 1999 [13]. Later, the soft set is updated by Maji et al. [14, 15] and Hayat et al. [16].

In the research community, numerous researchers used this technique for selection and decision-making problems [16, 17]. The soft set technique is a very effective technique for decision making and recommendation systems. Several researchers used a soft set for the concept design analysis problems. Based on the soft set, Roy and Maji in [18] proposed a new soft set technique called a bijective soft set for the problems of decision making and concept analysis. Similarly, in our previous study, we used a bijective soft set based on soft set to over the problem of effective machine learning (ML) algorithms and malicious attack traffic identification. We studied and found out the ML algorithm and selected the effective feature set by using a bijective soft set. However, the proposed method in our research study gives very promising results by using a bijective soft set [19]. Similarly, in this study, we also adopted the soft set method to overcome the problem of effective IoT devices' recommendation in the opportunistic network.

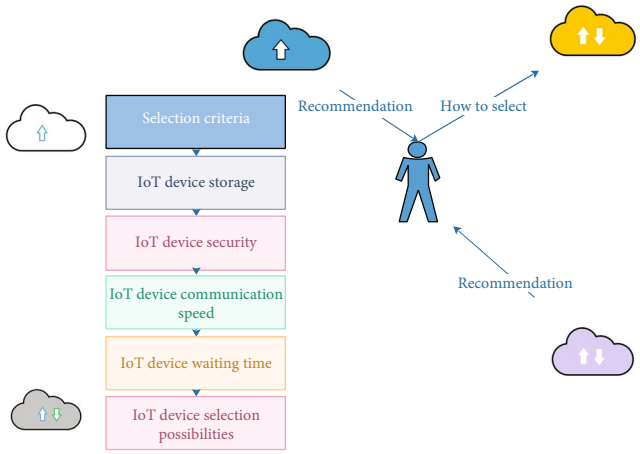

Figure 2: IoT device selection problem.

To overcome the problem of effective IoT device recommendation of edge computing IoT devices in the IIT, in this study, the soft set is adopted and applied [20]. However, it is important to deeply study the problem of IIoT device selection in the opportunistic network environment. To deal with this problem, a graphical presentation is shown in Figure 2. Based on the soft set, a new framework is proposed named SoftSystem. Then based on our proposed SoftSystem, a new algorithm called Softsystemalgo is proposed for the IoT device recommendation to select IoT devices in the network effectively. In this study, three different parameters are used for the effective IoT device recommendation in an opportunistic network such as Device Security (IDSC), IoT Device Storage (IDST), and IoT Device Communication Speed (IDCS). For better communication and IoT device recommendation, we find out the most useful parameters from the given set of parameters [21]. Our proposed system is effective for the recommendation, decision making, and selection of IoT devices in several devices to carry information tasks for the IoT network. However, the main contributions are given below:

(1) To tickle the problem of effective edge computing devices and with effective parameter selection in the IIoT network environment, three different parameters of edge computing IIoT devices are identified: IoT Device Security (IDSC), IoT Device Storage (IDST), and IoT Device Communication Speed (IDCS)

(2) Then, by using the selected different parameters, a new framework model named SoftSystem based on the soft set technique that recommends useful IIoT devices from several edge computing IIoT devices in the IIoT network is proposed. The proposed system consists of three steps: (1) selection of three different parameters, (2) Applying the soft set technique with details step by step process, (3) and then the final results. Step number two has several substeps, as discussed in Section 3, with more information

(3) Then, based on SoftSystem, an algorithm named Softsystemalgo is proposed to effectively select edge computing devices in the IIoT network. Initially, the proposed algorithm assigns the values of selected parameters based on the edge computing devices, and the algorithm goes to the next step in which the proposed SoftSystem is conducted. However, the algorithm selected the device which carries enough information for the effective communication between two edge computing nodes in the IIoT network environment. Based on our study knowledge, it is the first time to integrate a soft set technique for the selection of IoT devices in the IoT network

(4) Afterward, we put forward the results and selected edge computing devices in the IIoT network selected by our proposed system and algorithm. It is evident in the analysis of the experimental results that the selected device by our proposed system and algorithm carry enough information to be selected in the IIoT network

The rest of the paper is organized as follows: In Section 2, related works are discussed with details. While in Section 3, we demonstrate our proposed methods. Then in Section 4, the proposed algorithm is discussed, and in Section 5 is the experimental result analysis. Finally, Section 6 includes the conclusions.

2. Related Works

Internet of Things (IoT) is getting very important in every field, for instance, edge computing devices in the IIoT. IoT is the technology used to interconnect Machine-to-Machine (M2M). Due to interconnected intelligent sensors in the IoT network environment, life becomes very convenient. As in this technology, numerous smart IoT devices are interconnected with each other for communication and generate and exchange data for different purposes such as decision making and providing better services for better lives. However, IoT technology still needs to be improved from the perspective of security, etc. Lately, security and trust issues are also a scorching topic in the research community and even been studied Wireless Sensor Network (WSN) [22, 23], future Internet [24], and Smart IoT Cities.

Recently, the researcher tries its best to propose an efficient model for the communication between smart edge nodes in the IIoT network. However, the network recommendation of IoT devices is a very challenging task. In this study, to overcome the problem of the recommendation of IoT devices in the network, the most cited studies related to recommendation techniques are discussed with details. Recently, in our study, we used the bijective soft set for the selection of machine learning algorithms, and IoT attacks traffic identification. We used a bijective soft set based on soft set to over the problem of effective machine learning (ML) algorithms and malicious attack traffic identification. We studied and find out the ML algorithm and select the effective

feature set by using a bijective soft set. However, the proposed method in our research study gives auspicious results by using a bijective soft set [19, 25].

Similarly, in our previous studies, several different feature selection techniques are proposed for the selection of effective features in network traffic classification using different machine learning algorithms [26]. However, from the result analysis, our proposed selections are effective for the selection of effective feature set in a number of given feature set [27, 28]. Similarly, besides effective feature selection, we proposed a new framework for the selection of effective packet numbers in several different packets. In the above-given studies, the proposed methods are effective with respective feature selection and packet selection and got very promising results in terms of accuracy, recall, specificity, and specificity metrics.

In the research community, numerous studies have been proved that the selection technique is very efficient for the identification of selection problems and very important in every field, especially in IoT device recommendation and data processing problems. The selection technique is based on filtering and removes redundant items from several different given items. Similarly, In 2017, Jin et al. [29] proposed a new technique for the selection of Internet of Things services and named Physical Service Model (PSM). They applied the proposed technique and got very promising results. They showed that the proposed technique is able to satisfy user requirement in terms of IoT services. However, their proposed model is based on a conceptual technique to describe the various IoT physical services [29], [?], [30]. Their proposed model includes three subconcept as device, resource, and service. Also, in their research study, they proposed a new technique named Physical Service Selection (PSS) for the evaluation of Quality of Service (QoS) service [31, 32]. However, they made it evident in their research study that the proposed approaches are effective for the selection of IoT services. However, the method of selection in IoT technology, whenever a need, is effective for the effective performance results and always give auspicious results. Similarly, [4] studied and proposed a new technique to overcome the problem of multiobjective optimization in the IoT network. However, their study is mainly based on the selection technique for the selection of QoS aware service in the IoT network environment. In their study, they evidenced that the proposed approach is efficient and gives very promising result in terms of the selection of QoS service. Likewise, Chen et al. [33] studied the problem of Internet of Things [34] device management in terms of social network and proposed a new approach for the given problem.

In 2018, Van der Elzen and van Heugten [35] studied the problem of IoT device selection and presented a new technique for the selection of IoT devices in the opportunistic network. Their study is based on the Fuzzy Logic [18] method and showed that the selection of IoT devices in the opportunistic network is very effective whenever there are several IoT devices for the communication between two nodes. Nevertheless, for their study, they used only three effective parameters as Device Storage (IDST), IoT Device Waiting Time (IDWT), and IoT Device Security (IDSC). As they showed that the selected parameters carry enough information for the selection of IoT devices; thus, we also adopted these parameters for our study. However, their proposed technique is effective for the selection of the IoT device in the opportunistic network [36, 37]. However, this problem still needs to study more in-depth for effective performance results.

3. Proposed SoftSystem

To overcome the problem of the recommendation of effective IoT devices in the opportunistic network, in this section, we explained the proposed technique named SoftSystem based on the soft set technique. The detailed methodology of our model is shown in Figure 3. The proposed system for the recommendation of effective IoT devices in the opportunistic network includes different phases. Initially, the proposed system SoftSystem identified the IoT smart devices in the opportunistic network, which are available for consideration. In this study, only five intelligent IoT devices are considered for the study. However, the recommendation of smart IoT devices [38] depends on the opportunistic network operator. In the next step, the most useful parameters are identified carefully. In 2018, Van der Elzen and ven Huegten [35] studied the problem of IoT device selection and presented a new technique for the selection of IoT and used only three IoT device parameters for their study. However, in this study, three different parameters are utilized for the edge computing devices selection in the IIoT network as IoT Device Security (IDSC), IoT Device Storage (IDST), and IoT Device Communication Speed (IDCS). Then, the soft set technique is applied. The soft set portion included on several subportions. The details are discussed in the next subsection. After using the soft set technique, then we proposed a new algorithm named Softsystemalgo based on our proposed system SoftSystem for IoT device recommendation in the opportunistic network.

Though the proposed algorithm works the same as our proposed SoftSystem, the developed algorithm is effective for the real-time IoT device recommendation. However, the output of our proposed algorithm includes the final result of the IoT device recommendation in the network environment. The graphical presentation of our proposed SoftSystem for effective IoT device recommendation in the opportunistic network is shown in Figure 3. In the next subsection, the detailed methodology of our proposed approaches is discussed.

3.1. SoftSystem Metrics. In this section, the applied selection metrics are explained with details, as shown in Figure 3. Initially, the soft set method is discussed, and its algorithm then the proposed Softsystemsalgo. However, the detailed description is given below.

3.2. Soft Set Method. In this section, the applied soft set method is adopted for the recommendation of effective IoT devices in the opportunistic network environment. Soft set is a mathematical tool used for selection and decision-

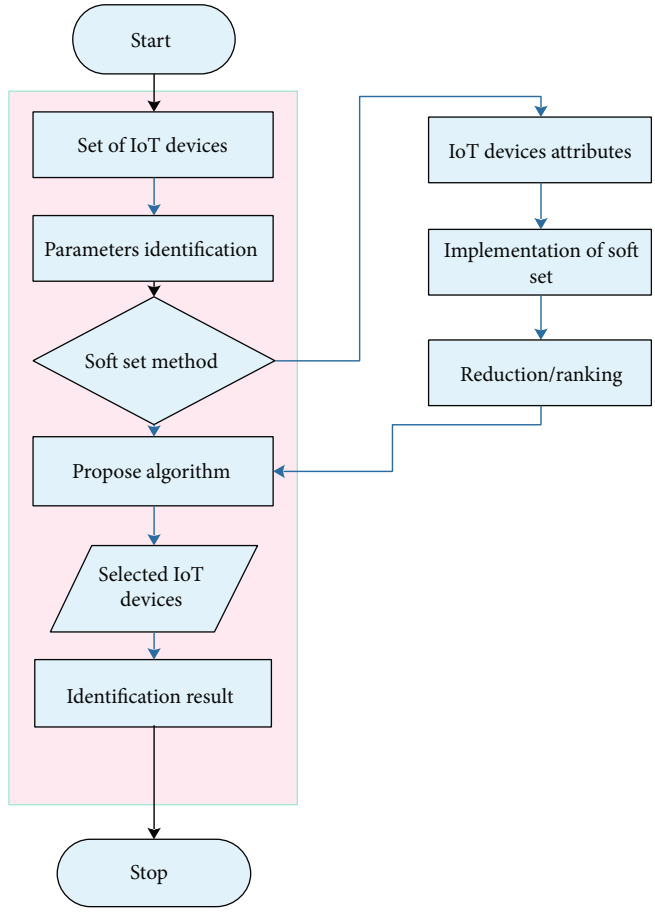

Figure 3: SoftSystem model.

making problems [39]. Soft set is firstly introduced by Molodtsov in 1999 [13] and Maji et al. [14] for the solution of decision-making problems. However, it is lately expended by Gong et al. [17] and Hayat et al. [16]. However, to overcome the problem of decision making, concept design and selection is a very effective method when there are several given items. Recently, numerous researchers applied the soft set method and achieved very efficient performance results in [17, 40]. The soft set method is similar to the type-2 soft set method and applied in several research studies for the effective performance results in [41]. In our previous research study, we applied a bijective soft set approach for the effective ML algorithm and feature selection and got auspicious results in terms of accuracy, recall, specificity, and specificity metrics.

Similarly, several researchers applied a soft set method to overcome the problem of decision making and selection problem [35, 38]. Likewise, Tiwari et al. [40] introduced a new method based on the soft set method for the selection of items from several given items. It is evident that the proposed technique is effective and efficient. Similarly, Khan et al. in 2019 [42] applied a bijective soft set based on the soft set technique for the best Wi-Fi frequency selection problem. However, it is a very good decision to apply a soft set method for the decision making and selection problem. From the above literature reviews and effectiveness of the soft set method, we adopted a soft set method for our desired selection problem. However, in this study, we applied a soft set method for the best IoT device selection problem [35]. The introductory definitions and implementations are given below with details.

3.2.1. Preliminary Definitions. To define soft set theory, suppose that a universal set U and the parameters of universal set U is P. More in-depth, the U indicates the universal set, and P indicates the parameters of the universal set. Then, the power will be $P(U)$, and R will be subset S such as $R \subset S$. Then, the pair (F, R) will be a soft set over U. Then, the mapping function of a soft set will be $F : R \to P(U)$. For instance, if

(1) X is relative null soft set: $(F, X) = \varnothing_x$ if for all $\{\lambda\lambda, \lambda\lambda\} \in X$

(2) X is relative null soft set: $(F, X) = U_x$ if $F(\lambda\lambda, \lambda\lambda) = U$ for all $\{\lambda\lambda, \lambda\lambda\} \in X$

(3) A soft subset: $(F,X) \subseteq^{\sim} (G, Y)$ if for all $\lambda\lambda \in X$, $F(\lambda\lambda, \lambda\lambda) = G(\lambda\lambda, \lambda\lambda)$

(4)The soft set equal: $(F, X) \approx (G, Y)$ if for all $\lambda\lambda \in X \cup Y$, $\lambda\lambda \in X \cap Y$ implies $F(\lambda\lambda) = G(\lambda\lambda)$; $\lambda\lambda \in X - Y$ or $\lambda\lambda \in Y - X$ imply $F(\lambda\lambda, \lambda\lambda) = \varnothing$ or $G(\lambda\lambda, \lambda\lambda) = \varnothing$

Table 1: Binary information system.

B	r_1	r_2	r_3
$\lambda\lambda 1$	0	1	1
$\lambda\lambda 2$	1	1	1
$\lambda\lambda 3$	0	1	1
$\lambda\lambda 4$	1	0	1
$\lambda\lambda 5$	0	1	1

Table 2: Binary information system.

B	r_2	r_3	Δ_i
Δ_1	0	1	1
Δ_2	1	0	1
Δ_3	0	1	1
Δ_4	1	0	1
Δ_5	0	1	1

(5)The union set $(F,X)\tilde{\cup}(G,Y) = (H,D)$, here $D = A\ U\ B$, and for all $\lambda\lambda \in$ D, if $\lambda\lambda \in$ X − Y, and $H(\lambda\lambda) = F(\lambda\lambda)$; if $\lambda\ \lambda \in$ Y − X, then $H(\lambda\lambda) = G(\lambda\lambda)$; $\lambda\lambda \in X \cap Y$, then $H(\lambda\lambda) = F(\lambda\lambda) \cup X(\lambda\lambda)$

(6)The restricted union: $(F,A) \cup (G,X) = (H,D)$, here $D = G \cap X$, and for all $\lambda\lambda \in D$,$H(\lambda\lambda) = F(\lambda\lambda) \cup G(\lambda\lambda)$

(7)Intersection operations:$(F,X) \sqcap (G,Y) = (H,D)$, here $D = X \cup Y$, and for all $\lambda\lambda \in D$, if $\lambda\lambda \in X - Y$, then $H(\lambda\lambda) = F(\lambda\lambda)$; If $\lambda\lambda \in Y - X$, then $H(\lambda\lambda) = G(\lambda\lambda)$; $\lambda\lambda \in X \cap Y$, then $H(\lambda\lambda) = F(\lambda\lambda) \cap G(\lambda\lambda)$

(8)Restricted intersection: $(F,X) \circledcirc (G,Y) = (H,D)$, where $D = X \cup Y$, and for all $\lambda\lambda \in D, H(\lambda\lambda) = F(\lambda\lambda) \cap G(\lambda\lambda)$

(9)The complement: $(F,X) = (F,X)$, where for every $\lambda\ \lambda \in X$, $F(\lambda\lambda) = \cup - F(\lambda\lambda\ ;\ )$

However, parameter reduction is important for the accurate implementation of the soft set. In the soft set technique, parameter reduction indicated the removing redundant parameter, which does not carry information for the identification. Similarly, in binary information system, soft set reduction is very important. For instance, in binary information system if (U,X,B), Where B indicates the binary relation, the detail is discussed in the next section, and $R_{\lambda\lambda}$ is equal to the relation on U and parameter $\lambda\lambda \in X$. Similarly, $R\lambda\lambda = \cap\ \lambda\lambda \in XR\lambda\lambda$ for soft set (F,X) over U.

(i) Then, the parameter reduction of a soft set is (F,Y) of a (F,X), if $\overset{\hat{E}}{A}B \subseteq X$, $R_Y = R_X$ and $R_{Y-\lambda\lambda}$, R_x for any $\lambda\lambda B$

(ii) Similarly, the intersection of the soft set reduction parameters (F,X) will be soft set core (F,X) and the soft set core (F,X) will be $(F, \cap B \subseteq X \mid (F,B))$of (F,X)

For instance, if a universe of housed $U = \{\lambda\lambda_1, \lambda\lambda_2, \lambda\lambda_3, \lambda\lambda_4, \lambda\lambda_5\}$ and its parameters are $R = \{(r_1),(r_2),(r_3))\}$ or $(r_1 = \text{cheap})$, $(r_2 = \text{modern})$, and $(r_3 = \text{beautiful})$, then the soft set can represent (F,R) if $F(r_1) = \{\lambda_2, \lambda_4\}$, $F(r_2) = \{\lambda_1, \lambda_3, \lambda_5\}$, and $F(r_3) = \{\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5\}$, then the binary information system can be like this if (F,R) is $(\{\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5\}), (\{(r_1),(r_2),(r_3)\}, B)$ Where B is the binary relation, and the table for the binary relation is shown in Tables 1 and 2, respectively, $U = \{\{\lambda\lambda_2\}, \{\lambda\lambda_4\}, \{\lambda\lambda_1, \lambda\lambda_3, \lambda\lambda_5\}\}$, and then the parameters are of a soft set will be like $(F, \{r_1, r_2\})$ and $(F, \{r_1, r_2, r_3\})$ as $\{r_1, r_2\} \subset \{r_1, r_2, r_3\}$, $U/R_r = U/R_{r1}$, $r_2/ = \{\{\lambda\lambda_2\}, \{\lambda\lambda_4\}, \{\lambda\lambda_1, \lambda\lambda_3, \lambda\lambda_5\}\}$ and $U/R_r, U/R_{r1}$. However, in research community especially in decision making or selection problems numerous researchers contributed for the reduction of soft set technique for better performance results. As Cagman et al. [43] contributed in soft set and extended the soft set technique with uni-int operators. For instance, if there is two soft set over U then $T = (F,X)$ and $S = (G,Y)$ and $S\,T \wedge S = (P, X \times Y)$ is $\times -$ product of T and S. Then, we can say that uni-int operator $\times -$product of $T \times S$ are

$$\text{uni}_y\ \text{int}_x(T \wedge S) = U_{yex}\left(\underset{x \in y}{\cap} P(y,x)\right), \tag{1}$$

$$\text{uni}_y\ \text{int}_x(T \wedge S) = U_{y \in x}\left(\underset{y \in x}{\cap} P(y,x)\right). \tag{2}$$

Then, the $\times$-product can be as

$$\text{uni-int}\ (T \wedge S) = \text{uni}_x\ \text{int}_y(T \wedge S) U \text{uni}_x\ \text{int}_y(T \wedge S). \tag{3}$$

Cagman et al. [44] defined the whole operation as below.

(1) Parameters selection of subsets

(2) Then applying soft set on each parameters

(3) Identification of $\times$-product

(4) And then performing uni-int decision of the product

3.2.2. Implementation of SoftSystem. The most important and critical operation is the development and implementation of soft set based SoftSystem for the effective IoT device recommendation in the IoT network environment or the construction of soft set for the recommendation of effective IoT devices for the better communication between two IoT devices. However, in this paper, we adopted the soft set method for the development of SoftSystem. For this purpose, Let U be the set of IoT devices and R be set of parameters and D the interval IoT devices then D is a mapping from R to L, i.e.,

$$D : R \to L, L = \{[a,b]\}, \tag{4}$$

$$D_L(R)\{U|\text{set of interval}|U \text{ over } R\}, \tag{5}$$

$$F : U \to D_L(R). \tag{6}$$

Here the (F,U) is the dual soft set and as well as interval values of SoftSystem for IoT device recommendation. Suppose that a set of IoT devices $U = \{\Delta_1, \Delta_2, \Delta_2, \Delta_4\ \Delta_5,\}$ and

Table 3: Reduction of soft set.

B	r_2	r_3	Δ_i
Δ_1	0	69.29	69.29
Δ_2	70.93	0	70.93
Δ_3	0	69.29	69.29
Δ_4	70.93	0	70.93
Δ_5	0	69.29	69.29

Algorithm 1: Selection of IoT devices:
Input: P (P_1, P_2, P_3, …. P_n) // set of Parameters,
Output: IoT devices [] // selected of IoT devices
1. begin
2. for i = 1 to N // IoT devices
3. calculate IoT devices [i];
4. end for
5. for i = 1 to N // Devise parameters
6. calculate parameters from each [i] for each parameters;
7. end for
8. for i = 1 to N // IoT devices
9. calculate soft set from each [i] for each parameters;
10. end for
11. for i = to N;
12. calculate ruduction and rank each parameters;
13. end for
14. Finally, obtain the effective IoT devices, if the table is Ruducted and rank to 1×1;
Return Algo;

Figure 4: Softsystemalgo.

R is a parameter set here in this research study, we used three fundamental parameters as IoT Device Security (IDSC), IoT Device Storage (IDST), and IoT Device Communication Speed (IDCS). Then, suppose that R is IoT Device Security (IDSC), IoT Device Storage (IDST), and IoT Device Communication Speed (IDCS). More in-depth, we defined the parameters as $R = \{r_1, r_2, r_3\}$. However, the mappings will be the following.

(i) $\Delta(\Delta 1) = r_1/[0.55], r_2/[0.15], r_3/[2]$, it can be defined as a number of IoT devices or a smart IoT device, which have the parameters of communication speed between 0 and 55, and the devices storage capacity is between 0 and 15 while the security level is of the IoT device between 2

(ii) $\Delta(\Delta 1) = r_1/[0.55], r_2/[55.105], r_3/[2, 10]$, it can be defined as a number of IoT devices or a smart IoT device, which have the parameters of communication speed between 0 and 55, and the devices storage capacity is between 55 and 105 while the security level is of the IoT device between 2 and 10

(iii) $\Delta(\Delta 1) = r_1/[0.55], r_2/[105], r_3/[0, 10]$, it can be defined as a number of IoT devices or a smart IoT device, which have the parameters of communication speed between 0 and 55, and the devices storage capacity is between 0 and 105 while the security level is of the IoT device between 0 and 10

Input:$P(P_1, P_2, P_3, \cdots P_n)$ //set of Parameters,
Output: IoT devices []//selected of IoT devices
1. begin
2. for i=1 to N // IoT devices
3. calculate IoT devices [i];
4. end for
5. for i=1 to N //Devise parameters;
calculate soft set from each [i] for each parameters
7. end for
8. for i=to N;
9. calculate soft set from each [i] for each parameters;
10. end for
11. for i=to N;
12. calculate ruduction and rank each parameters;
13. end for
14. Finally, obtain the effective IoT devices, if the table is Ruducted and rank to 1×1;
Return Algo.

Algorithm 1. Selection of IoT devices.

(iv) $\Delta(\Delta 1) = r_1/[0.55], r_2/[55.105], r_3/[0, 15]$, it can be defined as a number of IoT devices or a smart IoT device, which have the parameters of communication speed between 0 and 55, and the devices storage capacity is between 55 and 105 while the security level is of the IoT device between 0 and 15

(v) $\Delta(\Delta 1) = r_1/[0.55], r_2/[55.105], r_3/[1, 15]$, it can be defined as a number of IoT devices or a smart IoT device, which have the parameters of communication speed between 0 and 55, and the devices storage capacity is between 55 and 105 while the security level is of the IoT device between 1 and 15

Then, to get the interval value based on (F, U) as

$$\begin{aligned}(FU) &= \left\{\frac{r_1}{[0.55]}, \frac{r_2}{[0.15]}, \frac{r_3}{[2]}, \right\}\Delta \\ &= \left\{\frac{r_1}{[0.55]}, \frac{r_2}{[55.105]}, \frac{r_3}{[2, 10]}\right\}, \Delta \\ &= \left\{\frac{r_1}{[0.55]}, \frac{r_2}{[105]}, \frac{r_3}{[0, 10]}\right\}, \Delta \\ &= \left\{\frac{r_1}{[0.55]}, \frac{r_2}{[55.105]}, \frac{r_3}{[0, 15]}\right\}, \Delta \\ &= \left\{\frac{r_1}{[0.55]}, \frac{r_2}{[55.105]}, \frac{r_3}{[1, 15]}\right\}\end{aligned} \tag{7}$$

The above-given equations defined soft set technique will produce the desired output of IoT device. More in-depth, suppose that a set of three parameters $R = \{r_1, r_2, r_3,\}$, it can be defined in more details if an IoT devices communication speed is 31 and storage capacity is 60 while security level is about 9. Here, the communication speed is satisfied by the network administrator hence r_3 is reduced and reduction soft

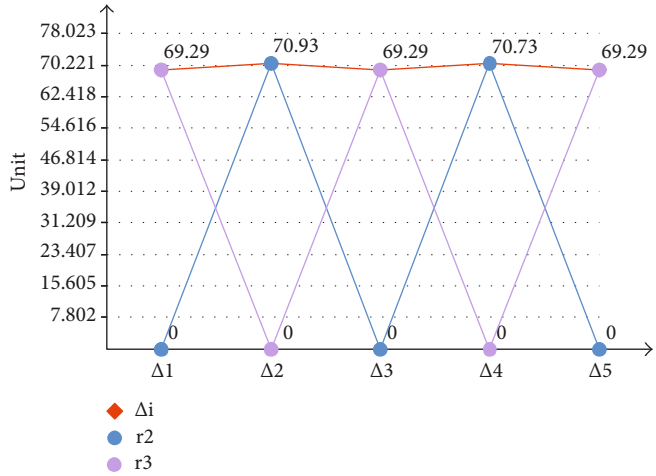

Figure 5: Reduction of soft set.

set is shown in the table. However, for reduction, a very useful method introduced by [4] is more effective for selection. In this paper, we adopted this technique for the reduction of soft set as $R = \{r_1, r_2, r_3,\}$ can be calculated by using a term weight: $w\_1 = 60/31 + 60 + 9 = 70.93$ and $w\_2 = 9/31 + 60 + 9 = 69.29$, then we can get the reduction by using the above equation as shown in Table 3.

Hence, it is clear from the reduction table that Δ_2 and Δ_4 are the effective IoT devices for effective communication in an opportunistic network environment. It is evident that the SoftSystem is efficient for the recommendation of effective IoT device in an opportunistic network when there are several different IoT devices for the selection.

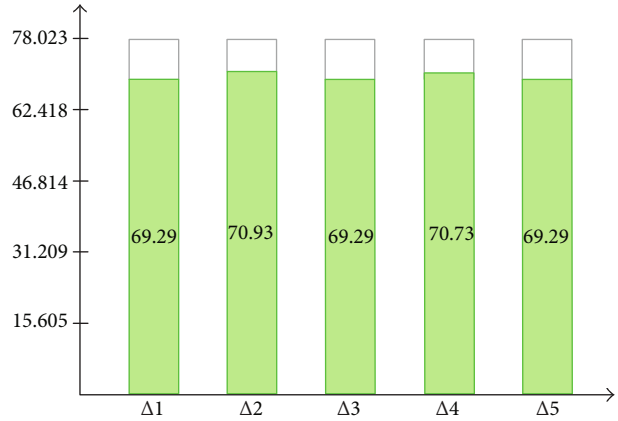

Figure 6: After reduction IoT device rank.

4. Proposed Softsystemalgo Algorithm

In this section, we demonstrate the proposed algorithm Softsystemalgo for the effective Internet of Things device recommendation in network as shown below.

However, the main process of the proposed Softsystemalgo is very simple as compared with others as shown in Figure 4. In the first step, the algorithm will calculate the available IoT devices and then the control goes to calculate the parameters. In this section, the algorithm will identify the available parameters and calculate. Then, after the identification of IoT devices parameters, the algorithm control will transfer to another step to calculate the soft set and then after calculation soft set the reduction operation will be conducted to reduce the parameters as required for effectiveness. After reduction operation, the proposed algorithm will rank the IoT devices with the help of identified parameters of IoT devices, and then finally the algorithm will produce the output IoT device, which will be effective in an opportunistic network. The proposed algorithm is very effective for the IoT device selection in an opportunistic network environment especially if there are several IoT devices, and it is difficult to select which IoT device is effective for efficient communication between two smart nodes in an opportunistic network environment. The idea and implementation of our proposed Softsystemalgo are very simple and easy for the selection and decision-making problem related to IoT devices, especially in an opportunistic network environment.

5. Results Analysis

To overcome the problem of the recommendation or selection of effective IoT devices in the opportunistic network, we explained the proposed technique named SoftSystem based on the soft set technique. The detailed methodology of our model is shown in Figure 3. The proposed system for the recommendation of effective IoT devices in the opportunistic network is very effective. In this section, we discuss the detailed results of our proposed system named SoftSystem and the proposed algorithm called Softsystemalgo as shown in Figure 5, reduction of soft set, and Figure 6, after reduction IoT device rank, respectively. In the previous section, from our proposed system output, it is evident that our proposed system and algorithm are able to recommend effective IoT devices in several different given devices in the network environment. The proposed algorithm and system are applicable to filter the most effective IoT devices in a number of devices. It is evident that our proposed system is effective for the recommendation, decision making, and selection of IoT devices

in a number of devices to carry information tasks for the IoT network. Similarly, the proposed algorithm is efficient for the IoT device recommendations in network environments, especially when there are several IoT devices, and it is not easy to select which IoT device is effective for efficient communication between two smart nodes in the opportunistic network environment. The idea and implementation of our proposed Softsystemalgo is very simple and easy for the selection and decision making problem related to IoT devices, especially in the opportunistic network environment. Though, the proposed system and algorithm is effective for the identification and selection of IoT devices. However, some effective information that we learned in this research study is given below as:

(i) In this study, it is evident that the proposed system named SoftSystem is able to select effective IoT devices in opportunistic network by using three different parameters IoT Device Security (IDSC), IoT Device Storage (IDST), and IoT Device Communication Speed (IDCS)

(ii) Similarly, it is clear that the proposed algorithm is efficient for the IoT devices selection, especially when there are several IoT devices and difficult to select which IoT device is effective for efficient communication between two smart nodes in the IIoT network environment

(iii) In this paper, only three different IoT devices parameters are conducted for the effective performance results as IoT Device Security (IDSC), IoT Device Storage (IDST), and IoT Device Communication Speed (IDCS). However, it is noted that more useful parameters can be identified and used for the desired problem as this is the future work

6. Conclusions

To overcome the problem of utilizing edge computing devices in the IIoT network environment, in this paper, we proposed a new framework model named SoftSystem based on the soft set technique that can select and recommend effective IoT devices from several IoT devices in the IIoT network. Based on our proposed SoftSystem, then we proposed an algorithm named Softsystemalgo. For the proposed system, three different parameters are selected: IoT Device Security (IDSC), IoT Device Storage (IDST), and IoT Device Communication Speed (IDCS). For better communication and IoT device recommendation, we find out the most effective parameters from the given set of parameters. It is evident that our proposed system is effective for the recommendation, decision making, and selection of IoT devices in a number of devices.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare no conflict of interest regarding this publication.

Acknowledgments

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), 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] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.

[2] 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*, pp. 1653–1657, Beijing, China, 2008.

[3] 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.

[4] M. Cuka, D. Elmazi, K. Bylykbashi, E. Spaho, M. Ikeda, and L. Barolli, "Effect of node centrality for iot device selection in opportunistic networks: a comparison study," *Concurrency and Computation: Practice and Experience*, vol. 30, no. 21, article e4790, 2018.

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

[6] X. Du, M. Guizani, Y. Xiao, and H. Chen, "Transactions papers a routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1223–1229, 2009.

[7] R. Yadav and W. Zhang, "Mereg: managing energy-sla tradeoff for green mobile cloud computing," *Wireless Communications and Mobile Computing*, vol. 2017, 11 pages, 2017.

[8] R. Yadav, W. Zhang, K. Li, C. Liu, M. Shafiq, and N. K. Karn, "An adaptive heuristic for managing energy consumption and overloaded hosts in a cloud data center," *Wireless Networks*, vol. 26, no. 3, pp. 1905–1919, 2020.

[9] R. Yadav, W. Zhang, O. Kaiwartya, P. R. Singh, I. A. Elgendy, and Y.-C. Tian, "Adaptive energy-aware algorithms for minimizing energy consumption and sla violation in cloud computing," *IEEE Access*, vol. 6, pp. 55923–55936, 2018.

[10] R. Yadav, W. Zhang, H. Chen, and T. Guo, "Mums: energy-aware vm selection scheme for cloud data center," in *2017 28th International Workshop on Database and Expert Systems Applications (DEXA)*, pp. 132–136, Lyon, France, 2017.

[11] Z. Qu, Y. Wang, L. Sun, D. Peng, and Z. Li, "Study qos optimization and energy saving techniques in cloud, fog, edge, and iot," *Complexity*, vol. 2020, 16 pages, 2020.

[12] M. R. Anawar, S. Wang, M. Azam Zia, A. K. Jadoon, U. Akram, and S. Raza, "Fog computing: an overview of big iot data analytics," *Wireless Communications and Mobile Computing*, vol. 2018, 22 pages, 2018.

[13] D. Molodtsov, "Soft set theory—First results," *Computers & Mathematics with Applications*, vol. 37, no. 4-5, pp. 19–31, 1999.

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

[15] 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.

[16] 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, 17 pages, 2017.

[17] 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.

[18] 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.

[19] 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*, vol. 107, pp. 433–442, 2020.

[20] F. Hao, Z. Pei, D.-S. Park, V. Phonexay, and H.-S. Seo, "Mobile cloud services recommendation: a soft set-based approach," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 4, pp. 1235–1243, 2018.

[21] L. Chaddad, A. Chehab, I. H. Elhajj, and A. Kayssi, "Mobile traffic anonymization through probabilistic distribution," in *2019 22nd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, pp. 242–248, Paris, France, France, 2019.

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

[23] 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*, vol. 7, no. 6, pp. 4682–4696, 2020.

[24] 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.

[25] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "Corrauc: a malicious bot-iot traffic detection method in iot network using machine learning techniques," *IEEE Internet of Things Journal*, 2020.

[26] 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.

[27] Y. Meidan, M. Bohadana, Y. Mathov et al., "N-BaIoT—network-based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12–22, 2018.

[28] 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.

[29] X. Jin, S. Chun, J. Jung, and K.-H. Lee, "A fast and scalable approach for iot service selection based on a physical service model," *Information Systems Frontiers*, vol. 19, no. 6, pp. 1357–1372, 2017.

[30] M. Wu, Z. Song, and Y. B. Moon, "Detecting cyber-physical attacks in cybermanufacturing systems with machine learning methods," *Journal of Intelligent Manufacturing*, vol. 30, no. 3, pp. 1111–1123, 2019.

[31] F. L. Rodríguez, U. S. Dias, D. Campelo, R. O. Albuquerque, S.-J. Lim, and L. G. Villalba, "Qos management and flexible traffic detection architecture for 5g mobile networks," *Sensors*, vol. 19, no. 6, p. 1335, 2019.

[32] 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)*, pp. 453–466, Seattle, WA, USA, USA, 2001.

[33] G. Chen, J. Huang, B. Cheng, and J. Chen, "A social network based approach for iot device management and service composition," in *2015 IEEE World Congress on Services*, pp. 1–8, New York, NY, USA, 2015.

[34] S. Nazir, Y. Ali, N. Ullah, and I. García-Magariño, "Internet of things for healthcare using effects of mobile computing: a systematic literature review," *Wireless Communications and Mobile Computing*, vol. 2019, 20 pages, 2019.

[35] I. Van der Elzen and J. van Heugten, *Techniques for Detecting Compromised Iot Devices*, University of Amsterdam, 2017.

[36] Z. Tian, X. Gao, S. Su, and J. Qiu, "Vcash: a novel reputation framework for identifying denial of traffic service in internet of connected vehicles," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3901–3909, 2019.

[37] 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*, vol. 16, no. 3, pp. 1963–1971, 2019.

[38] T. T. Nguyen, G. Armitage, P. Branch, and S. Zander, "Timely and continuous machine-learning-based classification for interactive ip traffic," *IEEE/ACM Transactions on Networking*, vol. 20, no. 6, pp. 1880–1894, 2012.

[39] 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.

[40] 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.

[41] M. Li, Y. Meng, J. Liu et al., "When csi meets public wifi: Inferring your mobile phone password via wifi signals," *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1068–1079, 2016.

[42] M. F. Khan, G. Wang, and M. Z. A. Bhuiyan, "Wi-fi frequency selection concept for effective coverage in collapsed structures," *Future Generation Computer Systems*, vol. 97, pp. 409–424, 2019.

[43] 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.

[44] F. Feng, Y. Li, and N. Çagman, "Generalized uni–int decision making schemes based on choice value soft sets," *European Journal of Operational Research*, vol. 220, no. 1, pp. 162–170, 2012.