IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 15 September 2022, accepted 1 October 2022, date of publication 14 October 2022, date of current version 19 October 2022.

*Digital Object Identifier 10.1109/ACCESS.2022.3212735*

RESEARCH ARTICLE

# Features-Based IoT Security Authentication Framework Using Statistical Aggregation, Entropy, and MOORA Approaches

**HABIB ULLAH KHAN [1], MUHAMMAD SOHAIL [1], AND SHAH NAZIR [2]**
[1]Department of Accounting & Information Systems, College of Business & Economics, Qatar University, Doha, Qatar
[2]Department of Computer Science, University of Swabi, Swabi 23430, Pakistan

Corresponding authors: Habib Ullah Khan (habibkhab@qu.edu.qa), Muhammad Sohail (sohail_kpk@yahoo.com), and Shah Nazir (shahnazir@uoswabi.edu.pk)

This work was supported in part by the Qatar National Library, Doha, Qatar; and in part by Qatar University Internal under Grant QUHI-CBE-21/22-1.

**ABSTRACT** The Internet of Thing (IoT) is one of the most imperative technology for all organizations that's play a vital role in many operations, using communication networks, for exchange of data in order to perform a useful task. However, security of IoT devices and data is a major concern. This research work prioritizes the alternatives of security authentication features from studied articles. The multi-objective optimization method based on the ratio analysis (MOORA) is useful in multi-criteria decision making (MCDM) for ranking the alternatives. The statistical aggregation (SA) method has been used to assign weights to security authentication features in comparison to entropy method. In this paper, we identify weights for authentication features using the proposed SA method. Moreover, we evaluate the accuracy rates of the proposed model using entropy method. Finally, we ranked out the alternatives of authentication features using the MOORA approach. In fact, the entropy weight values came against the initial value of the objects in which the accuracy was 15% which is not suitable to this problem while the accuracy of the SA is 85%. Hence, the accuracy improvement is approximately 70 % using the SA method. This method is applicable for finding the weights of the objects based on initial values by MCDM approaches. We study the key security authentication which is the preserving of confidentiality, integrity, and availability that are the prime objectives for security of an IoT device. Furthermore, challenges are preserving the selected attributes through any approach, as discussed in the literature, adds to the complexity of IoT device security. We identify the future challenges to improve the security of IoT devices.

**INDEX TERMS** IoT, security requirements, weightage, MOORA, MCDM, entropy method.

## I. INTRODUCTION

The Internet of Things is the merge technology of the internet and devices linked together connected through the communication in the network to perform a useful task meet the need of an organization requirements. Its work for data

Generation or operate the data or information in order to perform a useful task. The data security is the key term for IoT devices in the network to be secure from unauthorized access. The security of the IoT devices have based on the security authentication features. The present challenge for the researcher is to ensure the security of an IoT devices to confirm the strong security authentication feature that are most important for IoT devices. IoT became popular based on Radio frequency identification for cloud computing and data analysis in the latest embedded universal [1]. There are numerous obstacles associated with enormous and potential IoT based on smart devices that has focused on security concerns, as well as other topics. The control internet security issues is done by the vulnerabilities of the network that make unsecure the IoT devices in the communication network [2].

The primary goals of an IoT device security is to ensure the security of the users privacy, confidentiality to protect an IoT device and stop the leak of information, as well as to

The associate editor coordinating the review of this manuscript and approving it for publication was Giovanni Pau.

ensure the secure availability of the services provided by an IoT environment [3]. This study provided a new developed model based on multi criteria decision making approach that allows for an accurate assessment of the threats to fundamental data infrastructures [4]. Features weight of alternative for many MCDM mostly faced to the problems in which some time used the aggregation process to find its weight. The criteria's and its weightages are playing a vital role for overall preference measuring of alternatives. These 'objective weighting methods' and 'subjective weighting methods are weighting methods [5]. Weights are determined by decision-makers' preferences, whereas objective weighting methods use mathematical calculations to determine the weights, and the decision-makers have no part in deciding the relative significance of criteria [6]. Subjective weighing methods are used to determine the criteria for decision-makers' preferences dictate weights, but objective weighting systems employ mathematically based methods to compute weights. The decision-makers have no say in determining the relative importance of criteria [7].

The clearer explanation of the process acquisition of the objects weighing approaches, by the objectives weighting mechanism is not very well and ignores the decision maker's subjective assessment of the information [8]. Ranking approach used to find out the ranking of authentication features base on weight value of the objects to point out the strong security authentication features for an IoT device. The popular objective weighting methods have also discussed to a little bit complicate one. When there are quite a few of alternative (may be over 100) containing some criteria's (objectives), the objectives weighting methods could gain the great advantage in term of computational efficiency.

The statistical aggregation (SA) method is the calculation of weight distribution among the object according to its initial values based on statistical formulas. This method has used to assign the weight to the objects for MCDM approach.

The security authentication features have retrieved from related study for prioritization. Selected articles have based on IoT security problem to collect the security authentication features out of population that contains some important security authentication features. The main contributions in this paper are:

- Identify the weights for authentication features using the proposed SA method. Also, evaluate the accuracy rates of the proposed model using entropy method.
- Ranked out the alternatives of authentication features using MOORA approach; and
- Using the literature as an evidence, identify the future challenges to improve the security of IoT devices.

This paper is organized as follows. Section II describes the literature review; section III has detailed the methodology and contribution of the proposed research work. Observations are listed in section IV. Section V explains the analysis and finding of this research work performed on the accumulated relevant articles. It also outlined the results and future recommendation of this research work. Finally, the conclusions along with future work are discussed in section VI.

## II. LITERATURE REVIEW

Data protection can be done by the secure addressing and manual authentication (SAMA) protocols which is the key requirement for authentication and access control. It was great research for the better performance of an IoT and network security to protect the devices from unauthentic users. It uses to scan the devices to detect the unauthorized access with the help of addressing and identification methods to provide a secure the communication path between the clients and server. The protection of the system against the unauthorized access that try to hack the system with the help of the different tools and logics. It has based on automatic validation of internet security protocols and applications are (AVISPA) tool and burrows–abadi–needham (BAN) logic respectively [9].

The uses of secure communication media for IoT based devices in the medical field with radio media access control protocols are secure for communication and authentication. Some other protocols for reliable communication in order to authenticate the user for secure communication between the patients and doctors. Furthermore, the lightweight three factor authentication access control and ownership LACO was able to overcome the security flaws in the contemporary situation. The authentication protocols proposed for the e-health system, but it was still vulnerable for tracing, disconnection, denial of service (DOS), and internal attacks [10]. The ZigBee technique is used for IoT devices authentication to make secure the exchange of data among devices in IoT to generate a session key to share with a trusted device the connected devices in the communication network. Two types of analyses were used is formal and informal using BAN logic and application Tool Kit in the protection of IoT devices in the entire network. It has to find the vulnerability and generate an action against the hackers [11]. On the base of distributed ledger technology and artificial intelligence (AI) connected to health care that used to find out the vulnerability in IoT device communication in order to protect the IoT device based on those vulnerabilities in the legacy system. It has used to find the problems in the cloud sever related security of an IoT device to fix it through AI. The security can be strong by the security challenges to make the system more secure [12].

Wireless body area networks (WBAN) are precious networks for attacker detection through fast sensitive sensors in the health care side WBAN has used to protect the system from unauthorized access. Security and its solution are the big challenges from last years. Sensor network is most useful network for an IoT device security authentication and protection schemes in health care also protect it from unauthorized entities in online search [13]. IoT is most essential for our daily life for any information exchange process in the modern era of information technology. The IoT devices connectivity plays a vital role in each and every field of our life in the extension of computing. It tenses to decentralized security which is a difficult task in cloud computing here it discussed the fog computing architecture to find out the authentication problems. This framework of an IoT device authentication is very useful in health care system IoT [14].

A vehicular Ad hoc network (VA NET) is very important for a safe life in the modern-days because of traffic congestion. Due to the large transmission of data in value added network VAN, it becomes difficult to handle the security's issues. The cure technique is cryptography technique which is based on key technique provide a key session, public, and code for the message this scheme also called mac based authentication. It is also uses the technique of lightweight authentication to secures the system by biological also protect the vehicle from the malicious attacks [15]. The security of an IoT device plays a vital role in a communication network. On the basis of multi-factor authentication security a system perform remotely biometric authentication and key generation technique to make secure the IoT service. Formal security can be performed by using the VISPA tool that ensure the security against the multi threats in which the XOR and hash operation is useful because of less expensive [16].

RFID technology enables in IoT components for physical connection to keep a check on security and privacy issues. It is an efficient and reliable scheme of authentication to encrypt the data for the purpose of protection of privacy. Security authentication protocols used to protect the IoT communication against main in the middle (MIM) like resynchronization, relay, and tracing using different methods in which the BAN logic is the most suitable for this kind of protection [17]. It works on robust secure the IoT device operations on the base of cryptographic username and password scheme. The holistic views into the app in the middle of IoT the device architecture for the achievement of security goals needs base on authentication for resistance the un forge ability in the response of attack. The different scenarios indicates the token generation method for security goals and rule explanation [18].

In the distributed network the data comes from different places mostly cloud base data storage through networks which is difficult to keep secure due to unlimited boundary and geographical limitation. The centralized database is not secure because of easy-open attack of multi-user access. A Lightweight IoT device can be secure due to limited storage. The present study is between the smart city and IoT devices on the basis of IoT technology environment strength weaknesses, opportunities, and threats (SWOT) has highlighted. Other block chain applications like bitcoin cryptocurrency are used in it that need security challenges. This work is on decentralization to enhance the security based on framework dated by security features as needed for security. The effective combination of IoT device is to provide the secure services which are the basically security requirements [19].

The block chain technology provides distributed and scalable continue solution-based authentication called continuous authentication architecture based block chain (CAB) for IoT devices. It is a machine learning model based on face recognition that is used for authentication of outlier and abnormal users. It is a secure communication between the authenticated nodes for the achievement of security performance using lightweight authentication. The evaluation of IoT device is a good consideration of security from attack [20]. A CPS ensures the security for IoT components in term of its flexibility and possibilities. The integration components may be software or hardware based on the achievement of IoT device security challenges. The security requirements are the collections extend the existing ecosystem framework in the existence of IoT device security [21].

IoT base component are composed of entities in the network connected through communication links in order to exchange the data. Each and every device as IoT has assigned two types of address one is called physical address or MAC address and the other is a called logical or IP address used to resolve the physical address for authentication. CPS is use to coordinate the communication of an IoT device with its services devices that are connected through internet. The cloud network monitor communication to allow only the external users whose are authorize. In the real-time data access from IoT devices.

The components like sensors in the cloud computing request to hide the query from user to control the access of data based by establishing an authentication access link in cloud computing for big data. It discuss the security issues, network threats, and security requirement as future challenge. The authentication scheme and IT component basis on big data security protocols [22]. In this era the 5th and 6th generation internet is for long term faced with great security challenges based on machine learning and artificial intelligent in order to provide high speed secure network in which authentication, encryption, and the access control are the major concerns. In the advance network required high security address the strong security authentication features [23].

The above twenty security authentication features for IoT device that has selected from the above literature as shown in Figure 1.Thease security authentication features can used by the IoT devices for strong security of data according to the requirement the organization. These are the important security authentication features some of these are very essential for a IoT devices security as basic requirement that are most important for an IoT device which are common in many devices that are important and basic security requirement.

The main purpose is to priorities these security feature base on its importance and requirements.

## III. METHODOLOGY

Previous study has highlighted the common security authentication features that has selected from the large numbers of articles out of papulation in which fifteen articles are finalized which are the most relevant to this problem. The selected articles contain some important security authentication feature discussed in the literatures cited articles that are substitute the name as alternative denoted by A in order to best selection of an alternative that contains strong security authentication features. The alternatives required to categorize in ranking

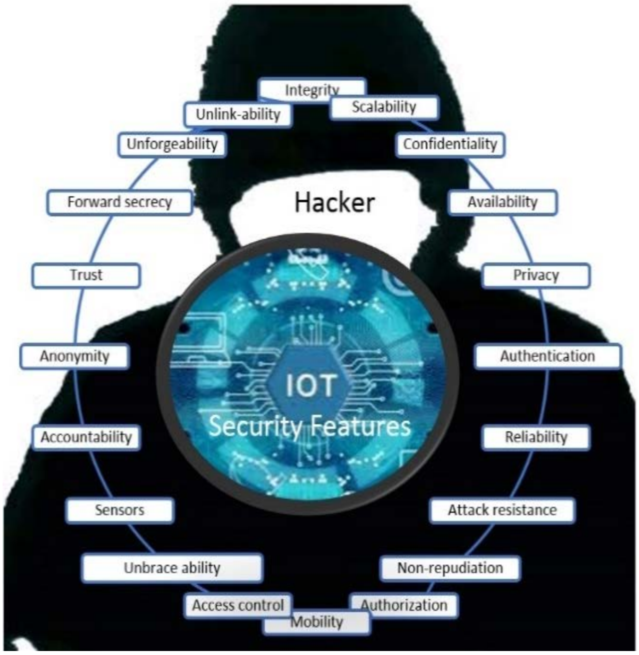

**FIGURE 1.** Features base security assessment.

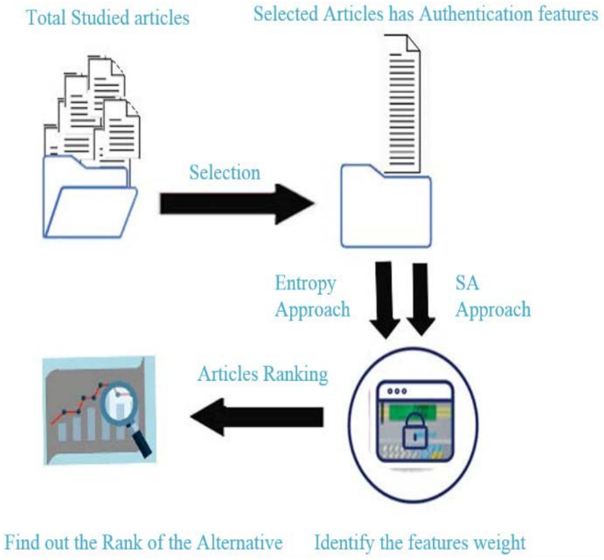
Total Studied articles
Selected Articles has Authentication features
Selection
Entropy Approach
SA Approach
Articles Ranking
Find out the Rank of the Alternative
Identify the features weight

**FIGURE 2.** Security features based ranking.

form using the different approaches such that entropy and SA approach. These approaches are used to assign the weight to the objects (features). The MOORA approach is using to rank out the alternatives.

The following algorithm represents the flow of work:

- Relevant article selection from papulation.
- Alias to the features by F1 to F20 and articles by A1 to A15.
- Count the same features in number of articles.
- SA and entropy method used to the assign weight
- Rank out the alternatives.

The above Figure 2 represents the process of this research work in order to identify the security authentication features for an IoT device. The main contribution is in this work is to prioritize the security authentication features based on its requirements using SA, entropy and MOORA approaches. The first step is consist of previous study in second step is the selection of relevant articles in third step we search for the strong authentication features. The value of a feature is consist of maximum number of usability of that security feature in articles. The initial value is the count number of a same authentication feature in number of multi articles. The entropy approach is one of the old method while the SA is a propose approach used for features weight calculation. The last step is to identify the ranking of the alternative that has most essential security authentication features.

### A. ENTROPY METHOD STEPS FOR SECURITY AUTHENTICATION FEATURES WEIGHT

The entropy method is use to assign the weight to the objects based on initial values. According to information theory, the smaller the information entropy of the alternative is, the greater the amount of information the alternative provides, and the greater importance of the alternatives. This implies that attribute of which the information entropy performs relatively low gets a higher weight [24].

*Step 1:*

$$X = x_{ij} = \begin{bmatrix} x_{ij} & \cdots & x_{in} \\ \vdots & \vdots & \vdots \\ x_{m1} & \cdots & x_{mn} \end{bmatrix} \tag{1}$$

In this step the data can be written in matrix form consists of some rows and columns' X represent the total matrix where 'i' represents the number of rows and 'j' represents the number of columns.

*Step 2:*

$$e_j = -h \sum_{i=1}^{m} r_{ij} \ln r_{ij} \tag{2}$$

where j = 1, 2, 3 . . . n,

$$h = \frac{1}{\ln(m)} \tag{3}$$

where m is the total numbers of alternatives

$$r_{ij} = \frac{x_{ij}}{\sum_{i=1}^{m} x_{ij}} \tag{4}$$

To calculate ej value for equation (5) where h is the height calculate by equation. (3) and $r_{ij}$ calculated by equation (4) to complete the equation (5).

*Step 3:* This step has the equation (5) that is used to calculate the weight value of the security authentication features which is represented by $\mathrm{W_j}$.

$$w_j = \frac{1 - e_j}{\sum_{j=1}^{n} (1 - e_j)} \tag{5}$$

where $\mathrm{j} = 1, 2, 3 \ldots \mathrm{n}$

In the Eq. (5) wj represent the weightage of the objects where ej is the entropy value and (1-ej) is the degree of diversification as described in [25] and [26].

### B. SA METHOD FOR SECURITY AUTHENTICATION FEATURES WEIGHT (AS PROPOSED METHOD)

The use of this method is to find out the weight of an object on the base initial parameter.

The initial value can be write in the matrix form.

*Step 1:*

$$X = x_{ij} = \begin{bmatrix} x_{ij} & \cdots & x_{in} \\ \vdots & \vdots & \vdots \\ x_{m1} & \cdots & x_{mn} \end{bmatrix} \tag{6}$$

In the above equation of the matrix represents the basic values for weight calculation. It represents the data in tabular form in order to find out the weight of an object.

*Step 2:* The feature average value is $(a_i)$

It used to find out of the average value of a feature as shown in below equation

$$\begin{aligned} &\lambda 11 + \lambda 12 \ldots \lambda 1\mathrm{n})/\mathrm{n} = \mathrm{a}1, \\ &\quad (\lambda 21 + \lambda 22 \ldots \lambda 2\mathrm{n})/\mathrm{n} = \mathrm{a}2\ldots\ldots \\ &\quad \times ((\lambda \mathrm{m}1 + \lambda \mathrm{m}2 \ldots \lambda \mathrm{mn})/\mathrm{n} = \mathrm{a_i} \end{aligned}$$

where n is the last counting number in rows and columns

$$\text{Total (t)} = \sum\nolimits_{i=1}^{i=i} (a_i) \tag{7}$$

where 't' represents the sum of average values of the features

$$Wj = (a_i) * \left(\frac{1}{\mathrm{t}}\right) \tag{8}$$

To verify eq.8 $\sum_{j=1}^{j=n} (W_j) = 1$

Where i and $\mathrm{j} = 1, 2, 3 \ldots, \mathrm{n}$

It is the aggregate base weight distribution among the objects in percent based of initial value. The total combination of features weight is 100% =1 the weight calculation will according to the feature values't' is the sum of average values of a feature.

Hence 1 (100%) is the total weight for distribution among the objects according to $(a_i)$ values.

The $\mathrm{a_i}$ is average number of feature occurring in overall final selected papers based on final selection criteria's.

### C. MOORA METHOD FOR ALTERNATIVES RANKING

This method is used to optimize the multi objectives on the basis of ratio analysis. This method consists of 3 steps to optimize the objectives.

*Step 1:* The value of objective can write in the matrix form

$$\text{i.e. } X = x_{ij} = \begin{bmatrix} x_{ij} & \cdots & x_{in} \\ \vdots & \vdots & \vdots \\ x_{m1} & \cdots & x_{mn} \end{bmatrix} \tag{9}$$

In this equation the data must be in the rows and columns form for calculation. In the Eq. (9) 'i' represents the number of rows and 'j' represents the number of columns.

*Step 2:* Evaluate the equation

$$X_{ij}^{*} = \frac{x}{\sqrt{\sum_{i=1}^{m} x_{ij}^{2}}} \tag{10}$$

*Step 3:* To calculate the final result in ranking form is to obtain the final result.

(Beneficial attributes – Non-beneficial attribute)

$$Y_i^{*} = \sum\nolimits_{j=1}^{g} w_j X_{ij}^{*} - \sum\nolimits_{j=g+1}^{n} w_j X_{ij}^{*} \tag{11}$$

### D. FEATURES USABILITY-BASED INITIAL VALUE IDENTIFICATION

In the following Figure 1 the security authentication features of the alternatives have written taken from the final relevant article highlighted in the literature. The initial vale of a feature is the count number of a security authentication features in overall articles. The availability of same feature in number of articles is to note with it citation. The calculation of weight is depending upon count number of feature availability in multiple articles as discussed before. Final selected numbers of articles is fifteen. Total number feature: TF=Twenty.

$$\mathrm{V\,j} = \frac{NF}{TF} \tag{12}$$

where vj is the values, NF is the number of repeated feature in the total alternatives and tf is the total number of features (object) in multiple articles.

The twenty security authentication features has taken from fifteen alternatives to better identify the strong security authentication features. The features has represented by F and the Alternatives has represented by A. the Alternatives has started from A1 to A15 and the features has started from F1 to F20.The alternatives has been representing the cited article containing some IoT security authentication features. The features are Integrity (F1), Scalability (F2), Confidentiality (F3), Availability (F4), Privacy (F5), Authentication (F6), Reliability (F7), Attack resistance (F8). Non Repudiation (F9), Authorization (F10), Mobility (F1), Access control (F12), Unbrace ability (F13), Sensors (F14), Accountability (F15), Anonymity (F16), Trust (F17), Secrecy (F18), Unforgeability (F19), Unlink-ability (F20).

In the discussion of the Table 1 contain twenty security authentication features from F1 to F20 and taken from the articles from A1 to A15 in which it shows that F1 integrity available in availed in All the articles except A8, A9, A10 that are in 12 articles shown in the No. of F mean feature column and so on.... The values are calculate as to divide no of F by T (total number of articles that is fifteen) so on...

**TABLE 1.** IoT authentication features in the alternatives.

| | A1 | A2 | A3 | A4 | A5 | A6 | A7 | A8 | A9 | A10 | C11 | A12 | A13 | A14 | A15 | $V_j$ | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | [9] | [10] | [11] | [12] | [13] | [14] | [15] | [16] | [17] | [18] | [19] | [20] | [21] | [22] | [23] | No. of F | Value=F/T |
| Integrity(F1) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | | ✓ | ✓ | ✓ | ✓ | ✓ | 12 | 0.8 |
| Scalability (F2) | ✓ | | | ✓ | | | | ✓ | | | ✓ | | | ✓ | | 5 | 0.34 |
| Confidentiality (F3) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | 13 | 0.87 |
| Availability (F4) | | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 13 | 0.87 |
| Privacy (F5) | | ✓ | | ✓ | | | ✓ | | ✓ | ✓ | ✓ | | | | | 6 | 0.4 |
| Authentication (F6) | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | 12 | 0.8 |
| Reliability (F7) | | | | | ✓ | | | | | | | | | | | 1 | 0.07 |
| Attack resistance (F8) | ✓ | | | | | | | ✓ | | ✓ | | | | | | 3 | 0.2 |
| Non-repudiation(F9) | | | | | ✓ | ✓ | ✓ | | ✓ | | ✓ | ✓ | | | | 6 | 0.4 |
| Authorization(F10) | | | | ✓ | ✓ | ✓ | | | | | ✓ | | | ✓ | | 5 | 0.34 |
| Mobility(F11) | | | | | | | | | | | | | ✓ | ✓ | | 2 | 0.14 |
| Access control (f12) | | ✓ | | | | ✓ | | | | | ✓ | | | ✓ | | 4 | 0.27 |
| Untrace ability (F13) | | ✓ | ✓ | | | | | | | | | | | | | 2 | 0.14 |
| Sensors (F14) | | | | ✓ | | | | | | | | | | | | 1 | 0.07 |
| Accountability(F15) | | | | | ✓ | | | | | | | | | | | 1 | 0.07 |
| Anonymity (16) | ✓ | | ✓ | | ✓ | ✓ | | | ✓ | | ✓ | | | | | 6 | 0.4 |
| Trust (F17) | | | | | | | | | | | ✓ | | | | | 1 | 0.07 |
| Forward secrecy(18) | | | | | ✓ | ✓ | | | | | | | | | | 2 | 0.14 |
| Unforgeability (F19) | | | ✓ | | | | | | | ✓ | | | | ✓ | | 3 | 0.2 |
| Unlink ability (F20) | | | ✓ | | ✓ | | ✓ | | | | | | | | | 3 | 0.2 |

On the basis of repetition the most repeated Security authentication feature in many articles are Integrity in 12 articles,confidentiality in 13 articles availability in 13 article for authentication which is in 12 articles others are not above then 6 articles. The Finally selected article has selected from one 3000 article using 4 different databases and publishers in which IEEE Explore,Elsevier,Springer,Wiley,Tayler and Frances are in the top. The above features represents that the first priority of the article must be contains confidentiality, integrity and availability with authentication features for security authentication of an IoT device.

So the value of feature can be considered the value column from the above Table 1 it is the initial value for wait calculation and further calculation for ranking.

### *E. ALTERNATIVE SELECTION AND WEIGHT CALCULATION*

From the above literature has discussed articles consists of important security authentication features as feature set of the alternatives. If all the features of an alternatives 'Ai' are available in the alternative 'Aj' then the selection of an alternative can be done by the union subset of authentication features and super set of authentication features of the alternatives.

$$\text{If } A_i \subseteq A_j,\ \text{then } A_i \text{ U } A_j = A_j \qquad \text{(q)}$$

$$\text{To select Aj, where 'i' and 'j'} = 1,2,3\ldots 15$$

The alternative Aj is the supper set while Ai is the sub set alternative of the authentication features. The subset alternatives are eliminated by superset alternatives to choose the superset instead of subset alternatives. SA and entropy methods have used to find out the weight of features for ranking the alternatives using MOORA approach. From the above Table 1 to eliminate the common or subset alternatives of the features is address the alternatives minimization in order better optimization.

To evaluate the Eq. (q) in order to eliminate the useless alternative of the subset of authentication of the features the main purpose of the elimination of these alternative to make decrease in the number of alternative for better selection of an alternative that contain important security authentication features because in the availability of super set of security authentication features it does not need to compare the subject in the competition of the others alternatives.

superset features of alternatives out of total Alternatives A1, A2, A3, A4, A5, A6, A7, A8, A9, A10, A11, A12, A13, A14, A15.To normalize and eliminate subset alternatives if A15 and A13 $\subseteq$ A14, A12 $\subseteq$ A 11, A9 $\subseteq$ A 11.

The subset alternatives are A1, A2, A3, A4, A5, A6, A7, A8, A10, A11, and A14. It represents all alternatives from the total alternatives that contains the subset of security authentication features. If all the features of the alternative A15 and A13 are available in the alternative A14 and the features of alternative A12 and A9 are available in alternative A11 Then it will better to take super set alternatives A14 and A11 of the features instead of comparison of all the alternatives. The selected alternatives of features are shown in the below table in which some of these alternative has distinct security authentication features in order to calculate the features weightages of these features by SA method with the comparison of entropy method.

To calculate the weightage of feature after then the calculation of the average value ($a_i$) as shown in Table 2. The average calculated values a feature multiply with where $\frac{1}{\sum a_i}$ where $\sum a_i$ is the sum of average values for equal distribution of weigh among total according to its initial values. Using Eq. (7) we calculate the weight of object to the Eq. (7) in

**TABLE 2.** Selected alternatives that contains superset of features.

| | F1 | F2 | F3 | F4 | F5 | F6 | F7 | F8 | F9 | F10 | F11 | F12 | F13 | F14 | F15 | F16 | F17 | F18 | F19 | F20 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A1 | 0.8 | 0.34 | 0.87 | 0 | 0 | 0.8 | 0 | 0.2 | 0 | 0 | 0 | 0.8 | 0.34 | 0.87 | 0 | 0 | 0.8 | 0 | 0.2 | 0 | |
| A2 | 0.8 | 0 | 0.87 | 0.87 | 0.4 | 0.8 | 0 | 0 | 0 | 0 | 0 | 0.8 | 0 | 0.87 | 0.87 | 0.4 | 0.8 | 0 | 0 | 0 | |
| A3 | 0.8 | 0 | 0.87 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.8 | 0 | 0.87 | 0 | 0 | 0 | 0 | 0 | 0 | |
| A4 | 0.8 | 0.34 | 0.87 | 0.87 | 0.4 | 0.8 | 0 | 0 | 0 | 0.34 | 0 | 0.8 | 0.34 | 0.87 | 0.87 | 0.4 | 0.8 | 0 | 0 | 0 | |
| A5 | 0.8 | 0 | 0.87 | 0.87 | 0 | 0.8 | 0.07 | 0 | 0.4 | 0.34 | 0 | 0.8 | 0 | 0.87 | 0.87 | 0 | 0.8 | 0.07 | 0 | 0.4 | |
| A6 | 0.8 | 0 | 0.87 | 0.87 | 0 | 0.8 | 0 | 0 | 0.4 | 0.34 | 0 | 0.8 | 0 | 0.87 | 0.87 | 0 | 0.8 | 0 | 0 | 0.4 | |
| A7 | 0.8 | 0 | 0 | 0.87 | 0.4 | 0.8 | 0 | 0 | 0.4 | 0 | 0 | 0.8 | 0 | 0 | 0.87 | 0.4 | 0.8 | 0 | 0 | 0.4 | |
| A8 | 0 | 0.34 | 0.87 | 0.87 | 0 | 0.8 | 0 | 0.2 | 0 | 0 | 0 | 0 | 0.34 | 0.87 | 0.87 | 0 | 0.8 | 0 | 0.2 | 0 | |
| A10 | 0 | 0 | 0.87 | 0.87 | 0.4 | 0.8 | 0 | 0.2 | 0 | 0 | 0 | 0 | 0 | 0.87 | 0.87 | 0.4 | 0.8 | 0 | 0.2 | 0 | |
| A11 | 0.8 | 0.34 | 0.87 | 0.87 | 0.4 | 0.8 | 0 | 0 | 0.4 | 0.34 | 0 | 0.8 | 0.34 | 0.87 | 0.87 | 0.4 | 0.8 | 0 | 0 | 0.4 | |
| A14 | 0.8 | 0.34 | 0.87 | 0.87 | 0 | 0.8 | 0 | 0 | 0 | 0.34 | 0.14 | 0.8 | 0.34 | 0.87 | 0.87 | 0 | 0.8 | 0 | 0 | 0 | |
| Sum | 7.2 | 1.7 | 8.7 | 7.83 | 2 | 8 | 0.07 | 0.6 | 1.6 | 1.7 | 0.14 | 1.08 | 0.28 | 0.07 | 0.07 | 2 | 0.07 | 0.28 | 0.2 | 0.6 | $\Sigma a_i$ |
| $a_i$ | 0.66 | 0.16 | 0.8 | 0.72 | 0.19 | 0.73 | 0.01 | 0.06 | 0.15 | 0.16 | 0.02 | 0.1 | 0.03 | 0.01 | 0.01 | 0.19 | 0.01 | 0.03 | 0.02 | 0.06 | 1.71 |

**TABLE 3.** Objects weight comparison.

| Features | *Initial values* | weightages ($W_j$) by Entropy | weightages($W_j$) by SA |
|---|---|---|---|
| F1 | 0.8 | 0.0076696 | 0.15387368 |
| F2 | 0.34 | 0.03013471 | 0.037260691 |
| F3 | 0.87 | 0.00364274 | 0.190687064 |
| F4 | 0.87 | 0.0076696 | 0.188741278 |
| F5 | 0.4 | 0.03013471 | 0.043836107 |
| F6 | 0.8 | 0.00364274 | 0.175344427 |
| F7 | 0.07 | 0.09164715 | 0.00187869 |
| F8 | 0.2 | 0.04965838 | 0.01118268 |
| F9 | 0.4 | 0.03866322 | 0.042941492 |
| F10 | 0.34 | 0.03013471 | 0.045625335 |
| F11 | 0.14 | 0.09164715 | 0.003757381 |
| F12 | 0.27 | 0.03866322 | 0.022342995 |
| F13 | 0.14 | 0.06515519 | 0.004070496 |
| F14 | 0.07 | 0.09164715 | 0.00187869 |
| F15 | 0.07 | 0.09164715 | 0.00187869 |
| F16 | 0.4 | 0.03013471 | 0.043836107 |
| F17 | 0.07 | 0.09164715 | 0.00187869 |
| F18 | 0.14 | 0.06515519 | 0.007514761 |
| F19 | 0.2 | 0.09164715 | 0.005367687 |
| F20 | 0.2 | 0.04965838 | 0.01610306 |

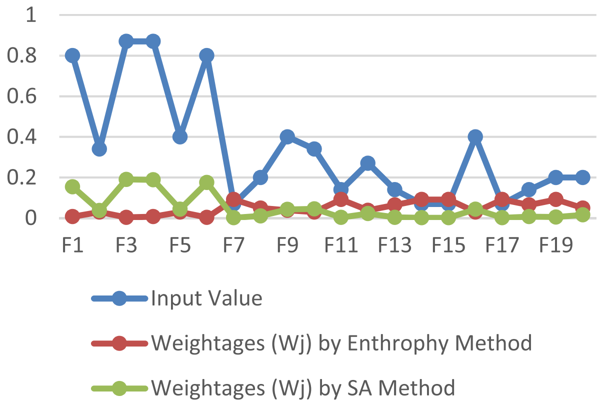

**FIGURE 3.** Features value obtained by both methods.

Eq. (8) for IoT security authentication features weight $W_j$. The Eq. (8) Wj represents the weight of an object where ai is the average value and t is the sum of the average values which is the aggregate value of an object on the basis of initial values of security feature.

The weight of the IoT security authentication features represent their importance. In the consequences of this method the values of the authentication features are not against the initial value of security authentication feature where the maximum value feature performs the main function in the security which is most valuable and high weighted that are mostly used in many systems. SA is one of the good statistical distribution of weight among the authentication features.

### F. ENTROPY AND SA METHOD COMPARISON

The below both Table 3 represent the weightages of the authentication features calculated based on availability in the

The above Table 3 describes the differences between feature's weightages obtained by SA and entropy approaches to evaluate the data have taken from the same Table 1. The ranking is the basis on the initial value of the weightage which should be corresponding to the initial values according to its importance and requirement.

The accuracy of the result is depend upon the weight of the security authentication features that provide the base for calculation of alternatives in order to prioritization. The blue plotted points represents the basic value of s feature, red represented the entropy Wight and green represented the propose method. The weight corresponding to the in input value,SA is from F1 to F17 is 17 and Entropy is from 17 to 20 is 3.Inorder to identify the accuracy of the weigh value against the initial vale to convert it into percentage entropy show 3 out of twenty and SA show 17 out of twenty.

Table 4 represents the initial for ranking using MOORA approach same to Table 2 that has used for weightage calculation using entropy and SA approach.

### G. MOORA APPROACH FOR ALTERNATIVES RANKING BASED ON SECURITY AUTHENTICATION FEATURES

It represents a newly created model based on coordinated MCDM methodologies for accurately assessing risks to critical data infrastructures. The selection of fifteen articles has

**TABLE 4.** Eq.(a) calculate to get eq. (10).

| | F1 | F2 | F3 | F4 | F5 | F6 | F7 | F8 | F9 | F10 | F11 | F12 | F13 | F14 | F15 | F16 | F17 | F18 | F19 | F20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A1 | 0.8 | 0.34 | 0.87 | 0 | 0 | 0.8 | 0 | 0.2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.4 | 0 | 0 | 0 | 0 |
| A2 | 0.8 | 0 | 0.87 | 0.87 | 0.4 | 0.8 | 0 | 0 | 0 | 0 | 0 | 0.27 | 0.14 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| A3 | 0.8 | 0 | 0.87 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.14 | 0 | 0 | 0.4 | 0 | 0 | 0.2 | 0.2 |
| A4 | 0.8 | 0.34 | 0.87 | 0.87 | 0.4 | 0.8 | 0 | 0 | 0 | 0.34 | 0 | 0 | 0 | 0.07 | 0 | 0 | 0 | 0 | 0 | 0 |
| A5 | 0.8 | 0 | 0.87 | 0.87 | 0 | 0.8 | 0.07 | 0 | 0.4 | 0.34 | 0 | 0 | 0 | 0 | 0.07 | 0.4 | 0 | 0.14 | 0 | 0.2 |
| A6 | 0.8 | 0 | 0.87 | 0.87 | 0 | 0.8 | 0 | 0 | 0.4 | 0.34 | 0 | 0.27 | 0 | 0 | 0 | 0.4 | 0 | 0.14 | 0 | 0 |
| A7 | 0.8 | 0 | 0 | 0.87 | 0.4 | 0.8 | 0 | 0 | 0.4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.2 |
| A8 | 0 | 0.34 | 0.87 | 0.87 | 0 | 0.8 | 0 | 0.2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| A10 | 0 | 0 | 0.87 | 0.87 | 0.4 | 0.8 | 0 | 0.2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| A11 | 0.8 | 0.34 | 0.87 | 0.87 | 0.4 | 0.8 | 0 | 0 | 0.4 | 0.34 | 0 | 0.27 | 0 | 0 | 0 | 0.4 | 0.07 | 0 | 0 | 0 |
| A14 | 0.8 | 0.34 | 0.87 | 0.87 | 0 | 0.8 | 0 | 0 | 0 | 0.34 | 0.14 | 0.27 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

finalized from huge number of publications that are relevant to IoT devices testing and contains the security highlights. The dynamic interaction, it is a vital for the alternatives to pick the best choice based on the benefits of the target collision and the expectations of the leaders. Multi-target development methodologies may be able to meet this potential the defined steps are predefined [27], [28].

*Step 1:* The MOORA technique begins with the building of a problem-solving matrix as shown in Table.4. The criteria (objects) and alternatives are listed in the decision matrix's columns and rows, respectively. The decision matrix shows how several options in terms of certain criteria as Eq. (9)

*Step 2:* Each alternative's performance value on a criterion is calculated by comparing it to the other alternative's performance on that criterion as Eq. (10). In order to solve the formula in to two sections for simplicity

$$\text{zi} = \sqrt{\sum\nolimits_{i=1}^{m} x_{ij}^{2}} \tag{13}$$

It's easy to solve the problem to calculate the denominator to apply Eq. (11).

$Z_i$ obtained from Eq. (11) Shown in Table 5 to find out the value of $z_i$ by the calculated normalized values of security authentication feature of the alternatives.

In the result of $z_i$ value from the above Table 5 to put in the Eq. (10) to get the normalized value of security authentication features in order to its ranking calculation.

To get Eq. (10), divide $x_{ij}$ by $z_i$ have taken from Table 5 to get the normalize value of the feature of alternatives. For non-beneficial criteria are subtracted from the sums for beneficial in this formula, g and (n − g) are the number of criteria to be maximized and minimized, respectively. Sometimes, decision makers want to give more importance to a criterion considering the weights of criteria.

### H. NORMALIZATION OF THE MATRIX VALUES

To normalize the Table 5 for further rank calculation. The Table 6 Contains the initialized values as in the form of matrix as shown in Eq. (9).

$X_{ij}^{*}$ Between [0,1] is a dimensionless number and the normalization activity of ith alternative on jth criteria as As shown in the Table 6. The number of alternatives are fifteen and number of security authentication features are twenty.

We are supposed to factorize the Eq. (10) as Eq. (a) then we can get the calculated value. The beneficial attributes from beneficial attribute. the alternative in descending order of y∗iyi∗ values. High value of $w_j X_{ij}^{*}$ for an alternative gives the higher rank out than the others. In this situation,

*Step 3:* Normalized performance values of beneficial criteria are added and add non-beneficial criteria. Finally, the sums for non-beneficial criteria are subtracted from the sums for beneficial criteria as seen Eq. (11). The result is the overall performance score of each alternative($Y_i^{*}$).

*Step 4:* Finally, ranked all out of the alternatives using Table 7 we multiplied the weight vale of authentication features to vale of $X_{ij}$ from Table 3.

*Step 4:* Finally, ranked all the alternative in descending order of y∗iyi∗ values. High value of y∗iyi∗ for an alternative gives the higher rank out of all the alternative. Obtaining the ranking of the alternatives using MOORA method. Native. Obtaining the ranking of the

$$Y_i^{*} = \sum\nolimits_{j=1}^{g} w_j X_{ij}^{*} - \sum\nolimits_{j=g+1}^{n} w_j X_{ij}^{*} \tag{14}$$

Alternatives using MOORA method. Criteria as seen Eq. (11). The result is the overall performance score of each alternative ($Y_i^{*}$).

In this formula, g and (n − g) are the number of criteria to be maximized and minimized, respectively. Sometimes, decision makers want to give more importance to a criterion

In this formula, g and (n − g) are the number of criteria.

This situation, Eq. (11) is reformulated by the weights of criteria. Here we have non-beneficial attributes are zero such that

$\sum\nolimits_{j=g+1}^{n} w_j X_{ij}^{*} = 0$ Put in Eq. (11) to get the result as below

$$Y_i^{*} = \sum\nolimits_{j=1}^{g} w_j X_{ij}^{*} \tag{15}$$

To apply the Eq. (15) in which all the features are act as beneficial for the IoT devices security where non beneficial attribute has not discussed in the Table 7 after the calculation of Eq. (15) in Table 7 to get Table 8 in which all the feature are in ranking based on its weightage obtained by two different methods in which SA is as proposed method while the entropy

**TABLE 5.** Feature's value of alternative.

| | F1 | F2 | F3 | F4 | F5 | F6 | F7 | F8 | F9 | F10 | F11 | F12 | F13 | F14 | F15 | F16 | F17 | F18 | F19 | F20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A1 | 0.64 | 0.12 | 0.76 | 0 | 0 | 0.64 | 0 | 0.04 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.16 | 0 | 0 | 0 | 0 |
| A2 | 0.64 | 0 | 0.76 | 0.76 | 0.16 | 0.64 | 0 | 0 | 0 | 0 | 0 | 0.08 | 0.02 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| A3 | 0.64 | 0 | 0.76 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.02 | 0 | 0 | 0.16 | 0 | 0 | 0.04 | 0.04 |
| A4 | 0.64 | 0.12 | 0.76 | 0.76 | 0.16 | 0.64 | 0 | 0 | 0 | 0.12 | 0 | 0 | 0 | 0.01 | 0 | 0 | 0 | 0 | 0 | 0 |
| A5 | 0.64 | 0 | 0.76 | 0.76 | 0 | 0.64 | 0.01 | 0 | 0.16 | 0.12 | 0 | 0 | 0 | 0 | 0.01 | 0.16 | 0 | 0.02 | 0 | 0.04 |
| A6 | 0.64 | 0 | 0.76 | 0.76 | 0 | 0.64 | 0 | 0 | 0.16 | 0.12 | 0 | 0.08 | 0 | 0 | 0 | 0.16 | 0 | 0.02 | 0 | 0 |
| A7 | 0.64 | 0 | 0 | 0.76 | 0.16 | 0.64 | 0 | 0 | 0.16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.04 |
| A8 | 0 | 0.12 | 0.76 | 0.76 | 0 | 0.64 | 0 | 0.04 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| A10 | 0 | 0 | 0.76 | 0.76 | 0.16 | 0.64 | 0 | 0.04 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| A11 | 0.64 | 0.12 | 0.76 | 0.76 | 0.16 | 0.64 | 0 | 0 | 0.16 | 0.12 | 0 | 0.08 | 0 | 0 | 0 | 0.16 | 0.01 | 0 | 0 | 0 |
| A14 | 0.64 | 0.12 | 0.76 | 0.76 | 0 | 0.64 | 0 | 0 | 0 | 0.12 | 0.02 | 0.08 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $Z_i$ | 2.4 | 0.78 | 2.76 | 2.62 | 0.9 | 2.53 | 0.1 | 0.35 | 0.8 | 0.78 | 0.15 | 0.57 | 0.2 | 0.1 | 0.1 | 0.9 | 0.1 | 0.2 | 0.2 | 0.35 |

**TABLE 6.** Calculation of X∗ij for eq. (10).

| X*ij=xij/zi | F1 | F2 | F3 | F4 | F5 | F6 | F7 | F8 | F9 | F10 | F11 | F12 | F13 | F14 | F15 | F16 | F17 | F18 | F19 | F20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A1 | 0.34 | 0.45 | 0.32 | 0 | 0 | 0.32 | 0 | 0.58 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.45 | 0 | 0 | 0 | 0 |
| A2 | 0.34 | 0 | 0.32 | 0.34 | 0.45 | 0.32 | 0 | 0 | 0 | 0 | 0 | 0.5 | 0.71 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| A3 | 0.34 | 0 | 0.32 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.71 | 0 | 0 | 0.45 | 0 | 0 | 1 | 0.58 |
| A4 | 0.34 | 0.45 | 0.32 | 0.34 | 0.45 | 0.32 | 0 | 0 | 0 | 0.45 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| A5 | 0.34 | 0 | 0.32 | 0.34 | 0 | 0.32 | 1 | 0 | 0.5 | 0.45 | 0 | 0 | 0 | 0 | 1 | 0.45 | 0 | 0.71 | 0 | 0.58 |
| A6 | 0.34 | 0 | 0.32 | 0.34 | 0 | 0.32 | 0 | 0 | 0.5 | 0.45 | 0 | 0.5 | 0 | 0 | 0 | 0.45 | 0 | 0.71 | 0 | 0 |
| A7 | 0.34 | 0 | 0 | 0.34 | 0.45 | 0.32 | 0 | 0 | 0.5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.58 |
| A8 | 0 | 0.45 | 0.32 | 0.34 | 0 | 0.32 | 0 | 0.58 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| A10 | 0 | 0 | 0.32 | 0.34 | 0.45 | 0.32 | 0 | 0.58 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| A11 | 0.34 | 0.45 | 0.32 | 0.34 | 0.45 | 0.32 | 0 | 0 | 0.5 | 0.45 | 0 | 0.5 | 0 | 0 | 0 | 0.45 | 1 | 0 | 0 | 0 |
| A14 | 0.34 | 0.45 | 0.32 | 0.34 | 0 | 0.32 | 0 | 0 | 0 | 0.45 | 1 | 0.5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**TABLE 7.** Weight multiplication with eq. (10) to get eq. (11).

| $w_j X^*_{ij}$ | F1 | F2 | F3 | F4 | F5 | F6 | F7 | F8 | F9 | F10 | F11 | F12 | F13 | F14 | F15 | F16 | F17 | F18 | F19 | F20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A1 | 0.05 | 0.02 | 0.06 | 0 | 0 | 0.06 | 0 | 0.01 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.02 | 0 | 0 | 0 | 0 |
| A2 | 0.05 | 0 | 0.06 | 0.06 | 0.02 | 0.06 | 0 | 0 | 0 | 0 | 0 | 0.01 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| A3 | 0.05 | 0 | 0.06 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.02 | 0 | 0 | 0.01 | 0.01 |
| A4 | 0.05 | 0.02 | 0.06 | 0.06 | 0.02 | 0.06 | 0 | 0 | 0 | 0.02 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| A5 | 0.05 | 0 | 0.06 | 0.06 | 0 | 0.06 | 0 | 0 | 0.02 | 0.02 | 0 | 0 | 0 | 0 | 0 | 0.02 | 0 | 0.01 | 0 | 0.01 |
| A6 | 0.05 | 0 | 0.06 | 0.06 | 0 | 0.06 | 0 | 0 | 0.02 | 0.02 | 0 | 0.01 | 0 | 0 | 0 | 0.02 | 0 | 0.01 | 0 | 0 |
| A7 | 0.05 | 0 | 0 | 0.06 | 0.02 | 0.06 | 0 | 0 | 0.02 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0.01 |
| A8 | 0 | 0.02 | 0.06 | 0.06 | 0 | 0.06 | 0 | 0.01 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| A10 | 0 | 0 | 0.06 | 0.06 | 0.02 | 0.06 | 0 | 0.01 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| A11 | 0.05 | 0.02 | 0.06 | 0.06 | 0.02 | 0.06 | 0 | 0 | 0.02 | 0.02 | 0 | 0.01 | 0 | 0 | 0 | 0.02 | 0 | 0 | 0 | 0 |
| A14 | 0.05 | 0.02 | 0.06 | 0.06 | 0 | 0.06 | 0 | 0 | 0 | 0.02 | 0 | 0.01 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

is an old method has used for objects weights calculation based on initial values. The initial values has been calculate by the both methods using Table 1. In the Table 8 shows the ranking of the alternatives (articles) to compare the both results obtained by Entropy and SA weighting methods.

The article have highlighted in literature section. In order to achieve the satisfactory result under the implementation of both results.

**TABLE 8.** Ranks obtained by both approaches.

| Alternatives | Rank obtained by Entropy | Rank obtained by SA |
|---|---|---|
| A1 | 8 | 10 |
| A2 | 9 | 6 |
| A3 | 1 | 11 |
| A4 | 7 | 4 |
| A5 | 2 | 3 |
| A6 | 4 | 2 |
| A7 | 3 | 7 |
| A8 | 10 | 9 |
| A10 | 11 | 8 |
| A11 | 6 | 1 |
| A14 | 5 | 5 |

In the above Table 9 analyzed the articles approached for strong security with some security authentication features based on strong protection mechanism as mentioned with their ranking obtained by statistical analysis. The collected security authentication features have taken from articles highlighted in the literature review in order to selection of strong security authentication features. The different techniques, mechanism, security authentication protocols, logic and tools have applied for prevention the unauthorized access to mitigate the security risk which was a big challenge for future IoT security. The ranking of the alternatives of authentication

**TABLE 9.** Articles With their security issues protocol,techniques,logic, and scheme with their ranking positions.

| Citations | Years | Security features | Attacks | Security Protocols, Technologies, Logic, and Scheme | Ranks1 | Ranks2 |
|---|---|---|---|---|---|---|
| [9] | 2021 | Confidentiality<br>Integrity<br>Scalability<br>Authentication<br>Attack Resistance<br>Anonymity<br>Access control<br>Untrace ability | DoS attack, Replay attack, MiM attack, Masques attack, Off-line password guessing attack, Message forgery attack, Privileged Insider attack | Secure addressing and Mutual Authentication protocol (SAMA) scheme, using AVISPA tool and widely-accepted BAN logic model, Robustness the proposed scheme, Forward and Backward secrecy | 8 | 10 |
| [10] | 2019 | Integrity<br>Confidentiality<br>Availability<br>Privacy<br>Authentication | Traceability, De-synchronization, denial of service (DoS), | Lightweight Three-Factor Authentication, Access Control and<br>Ownership | 9 | 6 |
| [11] | 2019 | Integrity<br>Confidentiality<br>Untrace-ability<br>Anonymity<br>Unlink-ability | Replay attack, Eavesdropping attack, Impersonation attack, MiM attack, Attack against the temporary secret key, Device stolen database attack, Forward/backward security, Session key guessing attack | BAN logic, AVISPA toolkit, IoT anonymous authentication with the unlink ability and un-traceability, Transactions, Cryptography for security | 1 | 11 |
| [12] | 2021 | Integrity<br>Scalability<br>Confidentiality<br>Availability<br>Privacy<br>Authentication<br>Sensors | End device attacks, Communication Channel attacks, Network protocol attacks, Sensory data attacks, DoS attacks, Software attacks | Distributed Ledger Technology (DLT), Distributed peer-to-peer nature can address the shortcomings of client/server models (Security Block Chain of IoT) | 7 | 4 |
| [13] | 2021 | Integrity<br>Confidentiality<br>Availability<br>Authentication<br>Non-Repudiation<br>Authorization<br>Accountability<br>Anonymity<br>Froward secrecy<br>Unlink-ability | DoS attack, Routing attacks, Masquerade/Impersonation attack, Replay attack, Node Subversion/Node Compromise attack, Intrusion, De-Synchronization, Node Replication/Cloning attack | WBAN, Security and Authentication. | 2 | 3 |
| [14] | 2020 | Integrity<br>Confidentiality<br>Availability<br>Authentication,<br>Non-repudiation<br>Authorization<br>Access Control<br>Anonymity<br>Forward secrecy | Defend MiM attack, Defend against eavesdropping, Defend against node capture attack, Defend against Replay attack, Defend against brute force attack | Distributed fog computing architecture.<br>Subsequently<br>Asymmetric cryptographic algorithm and one-way hash function, Decentralized solution for IoT. | 4 | 2 |
| [15] | 2019 | Integrity<br>Availability<br>Privacy<br>Authentication<br>Non-Repudiation<br>Unlink-ability | Replay attack: , Message modification and generation attack:, Repudiation attack:, Impersonation attack: Location tracking attack: | MAC-based authentication schemes | 3 | 7 |
| [16] | 2017 | Scalability<br>Confidentiality<br>Availability<br>Authentication<br>Attack resistance<br>Anonymity | Eavesdropping attack , Impersonation attack , Man-in-the-middle attack , Denial of Service attack , Stolen smart device attack, Parallel session attack , Password change attack , Gateway node bypassing attack, Anonymity ,Availability, Forward secrecy, Scalability, Attack resistance, Relay attack, Masquerade attacks, Spoofing attacks, Man-in-the-middle attacks | Multi-factor based authentication, lightweight biometric based remote user authentication and key agreement, lightweight hash operations and XOR operation | 10 | 8 |

**TABLE 9.** *(Continued.)* **Articles With their security issues protocol,techniques,logic, and scheme with their ranking positions.**

| | | | | | | |
|---|---|---|---|---|---|---|
| [18] | 2020 | Confidentiality<br>Availability<br>Privacy<br>Authentication<br>Attack resistance<br>Unforgeability<br>Confidentiality<br>Availability<br>Privacy<br>Authentication<br>Attack resistance<br>Unforgeability | Replay attacks | App-in-the-middle | 11 | 9 |
| [19] | 2019 | Integrity<br>Scalability<br>Confidentiality<br>Availability<br>Privacy<br>Authentication<br>Non-repudiation<br>Authorization<br>Access control<br>Anonymity<br>Trust | DoS attacks. | (SWOT) of block chain technology | 6 | 1 |
| [22] | 2019 | Integrity<br>Scalability<br>Confidentiality<br>Availability<br>Authentication<br>Authorization<br>Mobility<br>Access control<br>Unforgeability | Insider attack, Off-line password guessing attack, Stolen smart Card attack, DoS attack, Known session<br>key attack, User impersonation attack, MiM attack, replay attack; | CPS | 5 | 5 |

features has found by the MOORA approach and the entropy and SA methods has been used to assign the weight to the features. The last ranking position obtained by the SA is in the first position of ranking obtained by entropy weight approach. The limitation was of entropy method that the less parameter value weight is high than the high value of feature. In the first position in ranking selected alternative has most essential security authentication features for an IoT devices security. The above analysis has great idea for the future direction on the basis of some gaps as a future challenge for a researcher.

Most security authentication features are common in the above table that shows it important in IoT devices and another column has used some common protocols address the IoT security.

## IV. OBSERVATIONS

This section analyzes the selected citations with important security features, attacks, applied security risk mitigation protocols, technologies, logic, and schemes with its ranking.

The collected security authentication features have taken from articles highlighted in the literature review in order to select of strong security authentication features. Different techniques, mechanism, security authentication protocols, logic and tools have applied to prevent the unauthorized access to mitigate the security risk which was a big challenge for current IoT security. The ranking of the alternatives of authentication features has found by MOORA approach where the entropy and SA methods has used to assign the weight to the features. The first ranking position obtained by entropy is in the last position in the SA wastage approaches. In this case the entropy method is unsuccessful because the maximum value thing must be maximum in weight where over here the value weight was high by the low initial value of feature. In the first position in ranking selected alternative has most essential security authentication features for an IoT devices security.

## V. RESULTS AND DISCUSSION

In the entropy method the weight of an object came against the object initial value in which the minimum initial values of features give us maximum values of a feature. In this case the weight value of features affects the resulted values for ranking of the alternatives. In the entropy method the value of unimportant features combination exceeded then the value of important features combination where the proposed method is applicable for weigh determination of an objects for MCDM approach for prioritization of alternatives on the basis of initial values. The initial value can be obtained by prescribed way based on requirement in previous study.

From Figure 3. We observed the values in the perception of accuracy in which the initial value shows the accuracy line the value obtained by statistical aggregation method and the Statistical aggregation method relation in the term of accuracy.

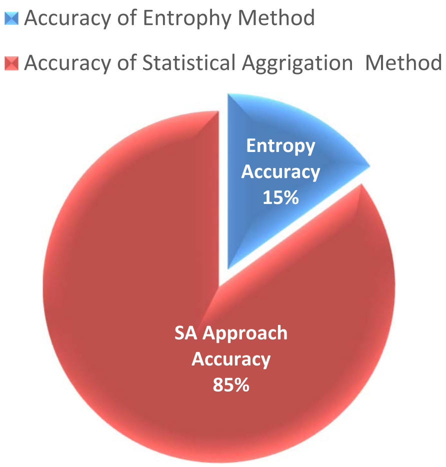

**FIGURE 4.** Show the obtained values accuracy.

SA method =1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17.

From 1 to 17 point are in the matching with the accuracy line hence we have in the relation 'r' =17 numbers out of 20

Symbolic representation of the Statistical aggregation method Accuracy is 'SAC'.

$$\text{SAC} = 17 \times \frac{100}{20} = 85\% \tag{16}$$

Based on entropy method reaction in the term of accuracy

Entropy method = 18, 19, 20.

From 17 to 20 point are in the matching with the accuracy line hence we have in the relation 'r' =3 numbers out of 20

Symbolic representation of the entropy Method SA Accuracy is 'EAC'.

$$\text{Accuracy} = 3 \times \frac{100}{20} = 15\% \tag{17}$$

The propose method shows the height accuracy in the security authentication perfective to parities the authentication features based on its requirements and availability highlighted in Figure 4.

On the basis of the Eq. (15) and Eq. (15) in the consequence the imprudent in the accuracy is

SAC – EAC = 85% -15%

SAC – EAC = 70%

The weight must be corresponding to the initial values of objects with respect their importance such that their use ability in multi article as basic requirement of security for IoT devices authentication. The MCDM approach is most helpful for the selection of alternative from large number of alternatives. The consequences of both methods can examine from the above final ranking Tables 8 in which the positions of alternatives obtained by both methods are distinct while some are same due to the reason of confliction in weight values that has obtained by both methods. The below Figure .4 represents the ranking value differences.

The selected alternative (A11) is in the first position that contains some important security authentication feature that are most crucial for most IoT devices security.

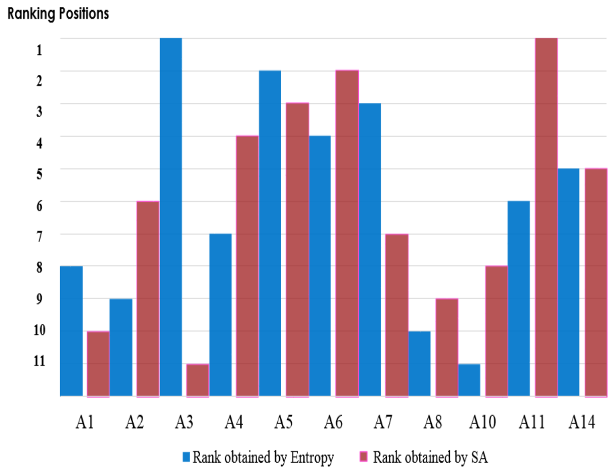

**FIGURE 5.** Value based comparison of results obtained by both object weighting methods.

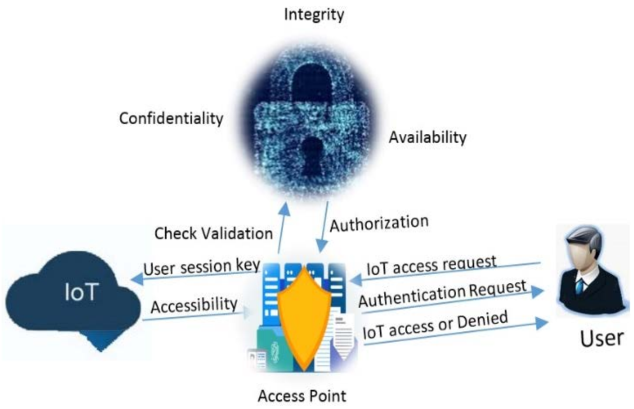

**FIGURE 6.** IoT device authentication.

Most common authentication features from selected articles The selected article was based on security authentication features by MOORA approach. In the top-ranking alternative contains confidentiality integrity authentication availability, non-repudiation authorization scalability. The access control, mobility in which confidentiality, integrity, and availability are most essential authentication features for IoT device security. Confidentiality grants an object authorization to access information. The data can only access by authorized users.

This is allow the authentication to confirm the validity of an item in which it does not refuse to reveal personally identifiable information for the purposes of verification. Integrity is the consistency of data in which it is ensure that the given data and information are accurate or not. The changing information in middle between to objects the middle entity read and alter the information or change the destination are security threads concerns to the security loss. Availability is the allocation of services to the

User in need of any time and everywhere accordingly. It is the availability of service in IoT objects. Strengths, weaknesses, opportunities, and threats (SWOT) of block chain technology used to decentralize the storage database which is multi point security that is close to attack instead of centralize database which was open to attack because of multi point security control. The first three feature in the above study are confidentiality, integrity, and availability (CIA) that are most important features for IoT device security as three sides of a perfect triangle of CIA.

The above figure represents the strong IoT security system in which user can not directly access the IoT devices the third party in the middle is responsible for secure communication to ensure the user authenticity. The service availability is depending upon the type of the user for that he/she are authorized.

## VI. CONCLUSION AND FUTURE WORK

In the emergence of IoT-based applications and devices the security vulnerability is considered as a key concern nowadays. The researchers around the world has suggested the diverse approaches to fix these issues and trying to protect it from unauthorized access based on strong authentication features. This work has addressed to key concern by presenting a statistical aggregation as proposed method which is a simple, easy and short method as compared to others. In the result the accuracy of the proposed method is 85 % where in the perspective of my problem the accuracy of entropy method was 15% which was mostly in another direction the assigned weight to the were against to the initial values. The accuracy improvement rate is 70%. This method is suitable for MCDM for the selection of the best alternative of objects. The alternatives have ranked out on the basis of MOORA method.

The high ranked alternatives contain crucial security authentication features are Integrity, confidentiality, availability, authentication, scalability, authorization, non-repudiation, mobility, access control, and privacy concern to the security authentication problems. The identified challenges for an IoT based device security to protect the device against the DoS attack based on SWOT of block chain technology has concerned to selected article. Some other protocols like SAMA, scheme, ZigBee technology, and Ban logic are also valuable for strong security authentication features in the terms of important IoT device-based security authentication challenges.

Furthermore, challenges are in the improvement of authentication protocols for IoT devices security against any kind of threats. The protection of an IoT devices is address to current challenges such as DoS Attacks handling using intrusion detection system to preserve the confidentiality, integrity, and availability. Our evaluation suggests that the proposed scheme is approximately 70% more secure by the identification of security authentication features than the existing Entropy method.

## REFERENCES

[1] K. K. Patel and S. M. Patel, "Internet of Things-IoT: Definition, characteristics, architecture, enabling technologies, application & future challenges," *Int. J. Eng. Sci. Comput.*, vol. 6, p. 5, May 2016.

[2] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2481–2501, Nov. 2014.

[3] M. B. M. Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Netw.*, vol. 148, pp. 283–294, Jan. 2019.

[4] Z. Turskis, N. Goranin, A. Nurusheva, and S. Boranbayev, "Information security risk assessment in critical infrastructure: A hybrid MCDM approach," *Informatica*, vol. 30, no. 1, pp. 187–211, Mar. 2019.

[5] N. H. Zardari, K. Ahmed, S. M. Shirazi, and Z. B. Yusop, *Weighting Methods and Their Effects on Multi-Criteria Decision Making Model Outcomes in Water Resources Management*. New York, NY, USA: Springer, 2015.

[6] J.-J. Wang, Y.-Y. Jing, C.-F. Zhang, and J.-H. Zhao, "Review on multi-criteria decision analysis aid in sustainable energy decision-making," *Renew. Sustain. Energy Rev.*, vol. 13, no. 9, pp. 2263–2278, Dec. 2009.

[7] G. O. Odu, "Weighting methods for multi-criteria decision making technique," *J. Appl. Sci. Environ. Manag.*, vol. 23, no. 8, pp. 1449–1457, 2019.

[8] A. Aalianvari, H. Katibeh, and M. Sharifzadeh, "Application of fuzzy delphi AHP method for the estimation and classification of ghomrud tunnel from groundwater flow hazard," *Arabian J. Geosci.*, vol. 5, no. 2, pp. 275–284, Mar. 2012.

[9] P. Kumar and L. Chouhan, "A privacy and session key based authentication scheme for medical IoT networks," *Comput. Commun.*, vol. 166, pp. 154–164, Jan. 2021.

[10] S. F. Aghili, H. Mala, M. Shojafar, and P. Peris-Lopez, "LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT," *Future Gener. Comput. Syst.*, vol. 96, pp. 410–424, Jul. 2019.

[11] M. Alshahrani, I. Traore, and I. Woungang, "Anonymous mutual IoT interdevice authentication and key agreement scheme based on the ZigBee technique," *Internet Things*, vol. 7, Sep. 2019, Art. no. 100061.

[12] B. Farahani, F. Firouzi, and M. Luecking, "The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions," *J. Netw. Comput. Appl.*, vol. 177, Mar. 2021, Art. no. 102936.

[13] B. Narwal and A. K. Mohapatra, "A survey on security and authentication in wireless body area networks," *J. Syst. Archit.*, vol. 113, Feb. 2021, Art. no. 101883.

[14] U. Verma and D. Bhardwaj, "Design of lightweight authentication protocol for fog enabled Internet of Things—A centralized authentication framework," *Int. J. Commun. Netw. Inf. Secur.*, vol. 12, no. 2, pp. 162–167, Apr. 2022.

[15] Z. Benyamina, K. Benahmed, and F. Bounaama, "ANEL: A novel efficient and lightweight authentication scheme for vehicular ad hoc networks," *Comput. Netw.*, vol. 164, Dec. 2019, Art. no. 106899.

[16] P. K. Dhillon and S. Kalra, "A lightweight biometrics based remote user authentication scheme for IoT services," *J. Inf. Secur. Appl.*, vol. 34, pp. 255–270, Jun. 2017.

[17] K. Fan, Q. Luo, K. Zhang, and Y. Yang, "Cloud-based lightweight secure RFID mutual authentication protocol in IoT," *Inf. Sci.*, vol. 527, pp. 329–340, Jul. 2020.

[18] H. Liu, J. Li, and D. Gu, "Understanding the security of app-in-the-middle IoT," *Comput. Secur.*, vol. 97, Oct. 2020, Art. no. 102000.

[19] S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed, and M. Imran, "Securing IoTs in distributed blockchain: Analysis, requirements and open issues," *Future Gener. Comput. Syst.*, vol. 100, pp. 325–343, Nov. 2019.

[20] F. Hussain Al-Naji and R. Zagrouba, "CAB-IoT: Continuous authentication architecture based on blockchain for Internet of Things," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 6, pp. 2497–2514, Jun. 2022.

[21] F. Quint, M. Orfgen, M. Schmitt, and S. Weyer, "Secure authentication in CPS-based production environments," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 5907–5913, Jul. 2017.

[22] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. P. C. Rodrigues, "Authentication in cloud-driven IoT-based big data environment: Survey and outlook," *J. Syst. Archit.*, vol. 97, pp. 185–196, Aug. 2019.

[23] S. A. A. Hakeem, H. H. Hussein, and H. Kim, "Security requirements and challenges of 6G technologies and applications," *Sensors*, vol. 22, no. 5, p. 1969, Mar. 2022.

[24] F. Chen, J. Wang, and Y. Deng, "Road safety risk evaluation by means of improved entropy TOPSIS–RSR," *Saf. Sci.*, vol. 79, pp. 39–54, Nov. 2015.

[25] X. Li, K. Wang, J. Xin, H. Yang, C. Gao, and L. Liu, "Application of the entropy weight and TOPSIS method in safety evaluation of coal mines," *Proc. Eng.*, vol. 26, no. 4, pp. 2085–2091, 2011.

[26] S. Guo, "Application of entropy weight method in the evaluation of the road capacity of open area," in *Proc. AIP Conf.*, May 2017, Art. no. 020120.

[27] P. K. Patnaik, P. T. R. Swain, S. K. Mishra, A. Purohit, and S. Biswas, "Composite material selection for structural applications based on AHP-MOORA approach," *Mater. Today, Proc.*, vol. 33, pp. 5659–5663, Jan. 2020.

[28] V. S. Gadakh, "Application of MOORA method for parametric optimization of milling process," *Int. J. Appl. Eng. Res.*, vol. 1, p. 743, Oct. 2010.

**HABIB ULLAH KHAN** received the Ph.D. degree in management information systems from Leeds Beckett University, U.K., in 2008. He has nearly 20 years of industry, teaching, and research experience. He is currently working as a Professor in MIS with the Department of Accounting and Information Systems, College of Business and Economics, Qatar University, Qatar. His research interests include the areas of IT adoption, social media, internet addiction, mobile commerce, computer mediated communication, IT outsourcing, big data, and IT security.

**MUHAMMAD SOHAIL** was born in Swabi, Pakistan, in February 1989. He received the master's degree in science systems from Abdul Wali Khan University Mardan, Pakistan, in 2013. He has nearly ten years of industry, teaching, and one year research experience. He is currently working as a Research Assistant at Qatar University, Qatar. His research interests include the areas of the IoT security, computer networks, AI, IT adoption, and IT security.

**SHAH NAZIR** received the Ph.D. degree in computer science with a specialization in software engineering from the University of Peshawar, in 2015. He has several research publications in well-reputed international journals and conference proceedings. He is currently working as an Assistant Professor and the Head of the Department with the University of Swabi. Prior to this, he worked at the University of Peshawar. His research interests include component-based software engineering, software birthmarks, systematic literature review, and decision making. He is a reviewer of several journals and conferences.