The Journal of Supercomputing (2024) 80:5870–5899
https://doi.org/10.1007/s11227-023-05685-3

Protecting IoT devices from security attacks using effective decision-making strategy of appropriate features

Inam Ullah[1] · Asra Noor[2] · Shah Nazir[2] · Farhad Ali[2] · Yazeed Yasin Ghadi[3] · Nida Aslam[4]

Accepted: 21 September 2023 / Published online: 7 October 2023

Abstract

The term "Internet of things (IoT)" refers to a network in which data from all connected devices may be gathered, analyzed, and modified as per requirements to offer new services. IoT devices require a constant Internet connection to exchange data. The volume and speed of data continue to grow quickly with the expansion of IoT devices nowadays. IoT systems frequently use messaging protocols to exchange IoT data. IoT security must be established using advanced techniques as it is vulnerable to many threats. The primary objectives of IoT security are to protect customer privacy, data integrity, and confidentiality, as well as the security of assets and IoT devices and the accessibility of services provided by an IoT ecosystem. In this regard, the IoT must meet user demands while consuming the least number of resources, including money, vitality, and time. The proposed research work is organized into numerous categories to make it easier for researchers and readers to solve and understand security problems in IOT devices. The categories "Features" are identified from available literature, and a specific criterion is adopted for choosing alternatives. The entropy approach to determine criterion relevance by calculating features weights is utilized. The second method "EDAS" approach is used and the alternatives are sorted chronologically based on the criterion weights for easy identification and selection of an effective alternative. Finally, all alternatives are precisely analyzed and ranked. Using our research method, various appropriate features are extracted and are evaluated to solve security issue within IoT devices. The most significant features are ranked to help researchers and manufacturers to focus on security-related issues in IoT devices.

Keywords Internet of things · IoT device · IoT security · Security and privacy · Networks

Extended author information available on the last page of the article

1 Introduction

The Internet has been evolving continuously over the past few decades. Social networking services, blogs, and wikis are now playing an essential role for both international trade and social interaction [1]. In addition to the existing technologies such as World Wide Web and ubiquitous mobile accessibility, the Internet of things (IoT) represents the most potentially disruptive technological development in the modern era. The developmental community is currently experiencing a paradigm change as common things are given the capabilities of connectivity and intelligence [2]. The Internet of things (IoT) revolutionizes daily life by connecting everyday items through data exchange and intelligent cooperation. Combining sensors, actuators, and communication interfaces, IoT transforms ordinary things into intelligent machines, improving convenience and effectiveness, and fostering innovation. The Internet of things (IoT) enables autonomous communication through interconnected devices with sensors, actuators, and communication modules. These devices collect data from their surroundings, transmit it to centralized systems, and share information. This enables real-time collaboration, data exchange, and informed decisions, enhancing efficiency and functionality in various applications. Through the development of several communication protocols and the miniaturization of transceivers, it is now feasible to transform a standalone device into a communicative entity. Despite having much smaller physical dimensions, computer or sensor devices presently offer significantly greater computational power, and storage capabilities. Many organizations and multinational corporations throughout the world are working on the design and development of IoT-based technologies. Providing a wide range of reliable services is challenging for designers, especially in complicated organizational structures [3].

According to Gartner, there will be twenty-five billion Internet-connected devices by 2020, and such interconnections will make it possible to use data for flexible analysis of information, organizing, supervising, and decision-making [4]. IoT allows "things and people to be connected anytime, anyplace, with anything and anyone, perfectly by using any path/network and any service." Modern technology is characterized by Internet-enabled IoT systems, which include a variety of technologies including personal computers, cellphones, automated teller machines (ATMs), RFID EDAS (radio frequency identification) and wearable gadgets [5, 6] that assists human beings to carry out their task efficiently and effectively.

IoT is a network of interconnected objects that uses intelligent sensors to make wireless connections. IoT can communicate without human assistance. There are several IoT applications that improve our daily lives due to the rapid growth in digital twin technology. IoT consists of anything from basic devices to common household products that improve the quality of life for people. Several limitations pose various challenges to the development of IoT systems for complex organizations. These include limitations such as real time, memory, processing, and the supply of continuous energy. The IoT is still in its infancy, although there have been numerous significant advancements in the integration of physical things with large number of connected sensors or monitoring devices [7].

IoT solutions are rapidly being utilized in almost every facet of daily life, thereby expanding the range and variety of applications for these technologies. The domains that are currently experiencing the greatest utilization of IoT in order to enhance their efficiency and effectiveness include smart industry, smart home, smart energy applications, smart transportation systems, smart health, and smart parking systems. In order to ensure adherence to regulatory requirements, the DSS actively monitors and reports on various metrics. By considering a multitude of factors, such as the volume of waste, its location, and the level of urgency, the DSS system assists in optimizing the allocation of resources [8]. IoT can also be used to upsurge transparency and promote local government actions toward citizens, raise people's consciousness of the state of their city, encourage active citizen involvement in public administration management, and stimulate the creation of new services [9].

The article provides an overview of IoT devices that are connected to provide smart services to organizations and people. The key contribution of the proposed research is provided in bullets.

- To highlight IoT and its importance in modern era.
- To analyze the features of IoT devices in terms of security and privacy.
- To evaluate the features using entropy method.
- To rank the most significant features using evaluation based on distance from average solution (EDAS) method.

The remaining paper is organized in various sections: Sect. 2 presents the literature review, while Sect. 3 presents the methodology of the proposed work. The feature selection is illustrated in Sect. 4, and finally, the paper is concluded in Sect. 5.

2 Literature review

In the past three decades, the Internet has grown significantly, transitioning from a network of a few hundred hosts to a platform connecting billions of "things" worldwide, including individuals and businesses of all sizes, via computers and devices of any imaginable size and capability, and the applications that run on them. The Internet is still expanding and is gradually causing a new, widespread paradigm in computers and communications. With the help of this new paradigm, the conventional Internet is transformed into a smart IoT built around the intelligent interconnectivity of various physical items, including cars, smartphones, homes, and the people who live in them. It makes use of low-cost information collection and dissemination tools, such RFID tags and sensors, that enable quick interactions between items as well as between objects and people at any time and location (Fig. 1). To address many of the problems that people and organizations encounter on a daily basis, the IoT will bring in a wide range of intelligent applications and services [10]. In Fig. 1, various IoT devices are linked together. The data are gathered using various sensors and are processed to reduce redundancy and complexity, and they are either represented and displayed on various medium to users or stored on cloud.

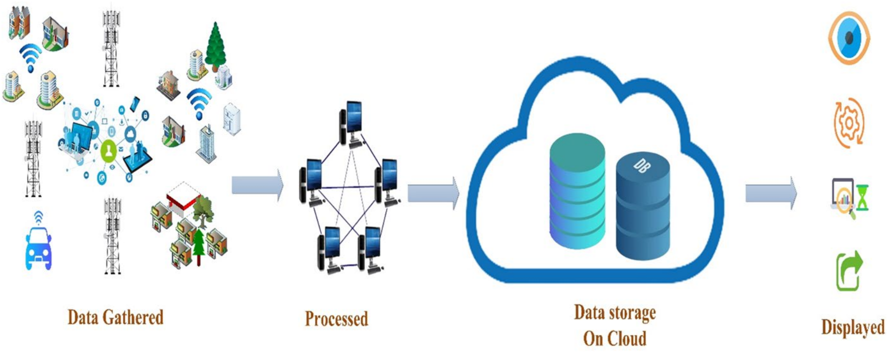

Fig. 1 The working and representation of IoT phenomenon

In the context of the IoT, it is noted that how current Internet protocols and security frameworks may be used and how they can be limited [11–13]. The deployment model and fundamental security requirements are first given a brief outline. Then, the difficulties and needs for IP-based security solutions were discussed and certain technical shortcomings of IP security standards were identified [14]. The use of common Internet protocols for communication between people and things or things and things in embedded networks is one way to directly interpret the phrase "IoT." The necessity for security in this area is generally established, but it is still unclear how to apply the IP security protocols and architectures that are already in place. The proper sharing of the licensed spectrum, which is restricted, is one of the main obstacles predicted in the extensive use of wireless technology in smart system applications. As a result, the performance of next-generation IoT devices may be constrained, and extensive research into new communication protocols can only fix these issues. The IoT seeks to change society such that it is intelligent, practical, and effective with the possibility of having significant positive effects on the economy and environment [15]. For this revolutionary transition to be possible, reliability is one of the key issues that must be solved. This article, which is based on the layered IoT architecture, starts by outlining the dependability issues that certain supporting technologies of each tier are posing a thorough analysis of the literature on IoT dependability. This study classifies and reflects reliability models and solutions at four tiers.

Research on privacy preservation in IoT raises concerns about commercial motivations and potential revenue streams. This article emphasizes the need for new strategies, transparency, and ethical design. A framework with policies is proposed to implement ethical design, allowing users broader control over their personal data and IoT facilities. Key players and measures are identified for deployment in typical IoT Setup [16]. The fast expansion of the IoT has generated a lot of interest in the creation of low-power wireless sensors. Wireless sensors are increasingly included in processing systems in order to collect data in a meaningful and reliable manner to monitor processes and control operations in industries, smart buildings, healthcare, defense, production, and manufacturing sites. Wireless sensor networks (WSNs) are essential for the advancement of Internet of things (IoT) technology. These networks consist of interconnected autonomous sensors that communicate wirelessly, collecting and transmitting data from the physical world to digital platforms. WSNs enable IoT processes to gather real-time information, monitor variables, and relay this data to central systems for analysis and decision-making. Their wireless nature reduces installation complexities and costs, enabling the expansion of IoT networks across vast geographical areas. The IoT devices may be used due to their long-term viability and self-sustaining operation [17].

The control and protection of user data is an important aspect to consider in the design and implementation of the Internet of things (IoT). In this particular context, there are significant challenges arising from the diversity of expertise in the Internet of things, the large number of devices and systems, and the multiple users and their respective roles [18, 19]. Despite the extensive efforts made by the research and calibration communities, there are still certain challenges that need to be addressed, particularly in the areas of interoperability, scalability, trust, and confidentiality. To tackle this, a security toolkit based on modeling is offered, which enables the development and evaluation of security rules for safeguarding user data. This toolkit is integrated into a management framework designed specifically for IoT devices [20].

IoT should not only lay out top-level strategy, advance security, and boost transmission competence, but also support industrial application and boost user stickiness. It would serve to shed light on the industrial structure and technical development trend, aid those in charge of enhancing their technology R&D (research and development) skills, and support them in creating aggressive offensive and defensive strategies [21]. The integrity of data and information has been endangered by hackers acquiring access to a number of entryways through the Internet, which is the major cause of security issues and cyberattacks. However, IoT is entirely dedicated in delivering the most effective methods for securing data and information [22]. With the introduction of the innovative cryptocurrency platform known as Bitcoin, blockchain technology has completely changed the digital currency industry.

IoT devices are becoming more common in many areas of our everyday life, such as smart homes, healthcare infrastructures, and industrial automation, which highlights how important their security is. These technical tools often gather and transmit sensitive information, making them vulnerable to hacking and illegal use. IoT device hacking-related cyberattacks have the potential to affect both people and businesses. IoT uses encryption, authentication, and routine software upgrades to protect data. Additionally, it includes secure boot methods, intrusion detection systems, and access limits. Companies and the makers of these gadgets should abide by the increasingly stringent security requirements and laws. Users' awareness and education are also necessary for IoT device safety. The fundamental ideas behind blockchain technology and the ways in which decentralization, security, and auditability are are achieved using this framework [23]. Blockchain technology is a decentralized, tamper-resistant digital ledger that records transactions or data sequentially. Its unique structure and consensus mechanism prevent unauthorized alterations or fraud. Transactions are verified by nodes, encrypted, and linked to previous ones, creating an immutable record. The decentralized nature eliminates a single point of control vulnerable to attacks. Blockchain's encryption techniques, using complex algorithms, make it difficult for unauthorized parties to access or decipher information, including digital signatures verifying transaction authenticity. The suggested blockchain-based IoT ecosystem is entirely decentralized, trustworthy-free, and secured.

Identification via RFID is a non-contact automated identification technology that uses radio waves to recognize signals and access pertinent target data without the need for user assistance. It can function in a range of challenging environments. More and more cannot meet a realistic and future demand because the logistics in the production control flow with information do not match. The major issue and research around the IoT is how it will overcome the typical flaw in the form coding as well as how it will be impacted by global logistics [24, 25]. It has been proposed that the IoT should be designed in layers, with a semantically enhanced overlay connecting the other levels and making it simpler to give secure access to services. The core of semantic overlay is security analysis, which makes use of ontologies and semantic rules. As last but not least, the interoperability of the security aspect is handled using a machine-to-machine platform [26].

The IoT physical communication layer, logistics, and robotics have all been significantly impacted by radio frequency identification (RFID) devices and sensors during the past several years. The purpose of the current article is to evaluate the key RFID sensors technologies today on the market and to determine the related state of the art when these technologies are applied in real IoT conditions. First, the ideas of radio backscattering and harmonic backscattering are examined, showing the benefits and drawbacks of each strategy [27]. The performance of each cutting-edge solution is then addressed, giving a broad picture of the possibilities of RFID-based sensing in many circumstances. The opportunity to develop a wide range of sharing applications, including peer-to-peer (P2P) automated payment mechanisms, foreign exchange platforms, digital rights management, and cultural assets, to mention a few, exists given the increasing interest in the IoT and blockchain. Even though there are several shared economy scenarios emerging, only a small number of them have used the IoT and blockchain to create distributed apps [28]. The usage of blockchain technology and the IoT to develop secure distributed shared economy applications is discussed in this article. Examples of such distributed applications inside an IoT architecture utilizing blockchain technology.

The term "Future IoT" places great importance on the unpredictable nature of the Internet of things (IoT), specifically highlighting its rapid evolution in terms of technology. It encompasses state-of-the-art advancements, cutting-edge technology, and creative operation of interconnected devices that will transform various industries and integrate the physical nature with the virtual domain. This statement perfectly sums up the interesting process of research and innovation [29]. How to extract "data" and convert them into "knowledge" from the sensing layer to the application layer has become one of the most important issues among them.

In a component-based software architecture for the IoT, "accessors"—proxies for things and services—interact with one another using a time-stamped, synchronized, discrete-event (DE) semantics. These proxies are comparable to web pages that act as intermediaries for cloud-based services like banks, but accessors are made to connect services and things rather than people. Asynchronous atomic callbacks (AACs), a popular technique for managing network interactions, are paired with a deterministic DE semantics. AAC eliminates blocking and the perilous concurrency traps of threads, allowing several synchronized pending requests to be active at once. The actor model in our architecture has been given a temporal semantics, thereby combining AAC and actors. We demonstrate how this architecture may use the previously published Secure Swarm Toolkit (SST) to enable cutting-edge network interaction encryption, authentication, and authorization [30].

Increased decision accuracy and enhanced intrusion detection systems are just two of the many benefits that machine learning has brought to security and CPS/IoT. The machine learning (bad use) vulnerabilities from the perspectives of security and CPS/IoT are more urgently needed, counting the ways in which machine learning schemes can be deceived, weakened, and thereby altered at all stages of the machine learning life cycle (data collection, training, pre-processing, implementation, and validation). The use of machine learning to execute security breaches and incursions is evolving into an alarming phenomenon. Therefore, analyzing current strategies may advance target acquisition and identify threat patterns that may enable creative attacks that are still unidentified [31].

The Internet of things (IoT) opposes numerous operational, technological, and security obstacles that necessitate determination for its advancement. The magnitude and complexity of IoT initiatives demand a significant level of scalability and compatibility, often requiring seamless communication among multiple devices utilizing diverse protocols and standards. The protection of security receives utmost significance, captivating the implementation of continuous measures to prevent potential issues that may arise from the processing of sensitive data by IoT devices and the ever-evolving landscape of risks. Furthermore, the vast amount of data generated by IoT devices pose difficulties for efficient data management and real-time analytics, requiring a robust infrastructure to extract valuable insights. Compatibility issues are frequently encountered by large enterprises when integrating IoT with traditional systems [32].

In the literature, researchers have proposed a variety of methods for improving overall security. However, many of these approaches concentrate on a small number of security concerns. The limitation of using these approaches is that it might lower a system's overall security capabilities. We have examined a wide range of security features in our comprehensive review. Our goal was to find as many functional characteristics as possible that may significantly improve device security. By analyzing all the security-related features, our proposed method will weight and prioritize the most significant features to enhance the security of various IoT devices.

3 Methodology

A precise and thorough methodological effort is required to guide and support analysts and scholars during the assessment and selection process of IoT-based projects by keeping their security and maintenance. A multi-criteria decision-making (MCDM) model, comprising entropy and EDAS methods, has been utilized to assess the fundamental elements of security in the Internet of things (IoT) and to assign ranks to various kinds of alternatives in a sequential manner, aiming to yield an impressive decision. This framework proves to be beneficial in scenarios where the selection and evaluation processes are challenging, and the circumstances are characterized by ambiguity. The comprehensive research methodology has been categorized into distinct sections to facilitate comprehension and resolution for both experts and readers. Initially, we determine the aim, criteria, and alternatives by reviewing the relevant materials available on this topic. Then, we apply the entropy method for the identification of criterion importance by calculating their weights. Based on the criterion weights, we apply the EDAS approach and ranked the alternatives chronologically for the easy identification and selection of an effective alternative. Finally, all the alternatives are evaluated and ranked precisely. The entire set of the following steps in the proposed methodology is shown in Fig. 2.

4 Feature selection

Decision support system (DSS) has the capacity to automatically choose relevant information from a subset. By deleting redundant and unnecessary data, this stage improves the precision of the decision-making. This process, also known as feature selection, improves predictive model performance while reducing uncertainties and risk. Feature selection (FS) is a machine learning approach used to simplify computation and dimensionality challenges in complex datasets. It improves efficiency, scalability, and accuracy in fields like data mining, text classification, signal processing, and pattern recognition. Researchers, developers, computer scientist engineers, and various organizations are implementing innovative strategies to tackle security issues related in IoT devices. These approaches, researcher recommendations, and various published studies were examined for enhancing device security. To this end, a comprehensive search of reputable libraries such as ACM, ScienceDirect, IEEE Explore, Springer, Hindawi, Taylor, and Francis has been conducted to

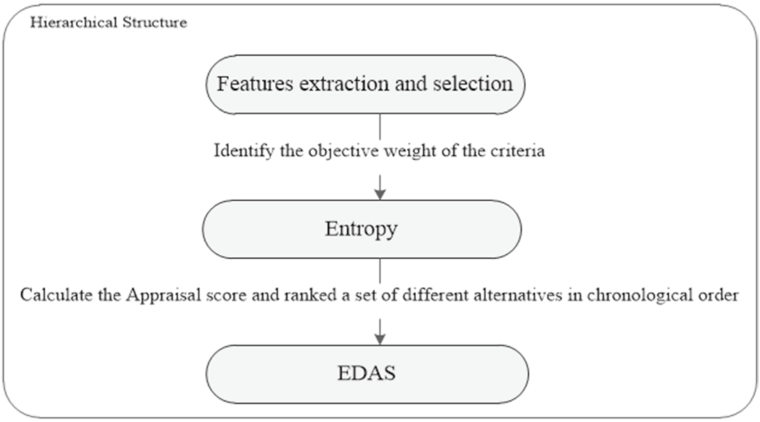
Hierarchical Structure
Features extraction and selection
Identify the objective weight of the criteria
Entropy
Calculate the Appraisal score and ranked a set of different alternatives in chronological order
EDAS

Fig. 2 The proposed research protocol

Table 1 Selected features

Features	Sign	Features	Sign	Features	Sign
Data integrity	$F1$	Reliability	$F7$	Unbrace ability	$F13$
Scalability	$F2$	Resistance	$F8$	Accountability	$F14$
Confidentiality	$F3$	Non-repudiation	$F9$	Anonymity	$F15$
Availability	$F4$	Authorization	$F10$	Trust	$F16$
Privacy	$F5$	Mobility	$F11$	Secrecy	$F17$
Authentication	$F6$	Access control	$F12$	Unforgeability	$F18$

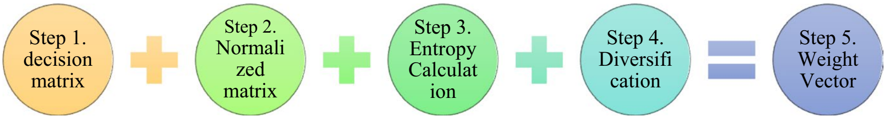

Fig. 3 The overall stages of an entropy method

identify relevant studies in the security domain. Furthermore, the snowballing procedure has been employed to ensure that no pertinent research work is overlooked in the literature. Subsequently, effective features have been extracted from all relevant literature, and their impact on security performance has been evaluated. Some common and comparable characteristics have been extracted and selected from the previous to determine their importance and evaluate the multiple alternatives. All the chosen criteria are listed in Table 1.

4.1 Entropy approach

Entropy is a multi-criteria decision-making method that is mostly utilized for the determination of criterion significance by identifying their weights. The preliminary values have been assigned to each criterion based on their importance to compare them precisely. The entropy approach is an objective weighted method that efficiently measures the importance of the selected criterion and helps us in the solution of multi-criteria-related issues. Their various equations are easy to employ for the measurement of criterion importance and solving multi-criteria problems [33]. It has included several phases that help us in the calculation of criterion weights. The steps involved in this process are shown in Fig. 3.

4.1.1 Numerical work of entropy

In this research, we choose 18 criteria and 12 alternatives to determine the criterion importance and rank the alternatives. The selected criteria have been calculated by applying the entropy method and their weights have been determined. A set of criteria ("$A1$–$A12$" represented in Fig. 4) consists of data integrity ($F1$), scalability ($F2$), confidentiality ($F3$), availability ($F4$), privacy ($F5$), authentication ($F6$), reliability ($F7$),

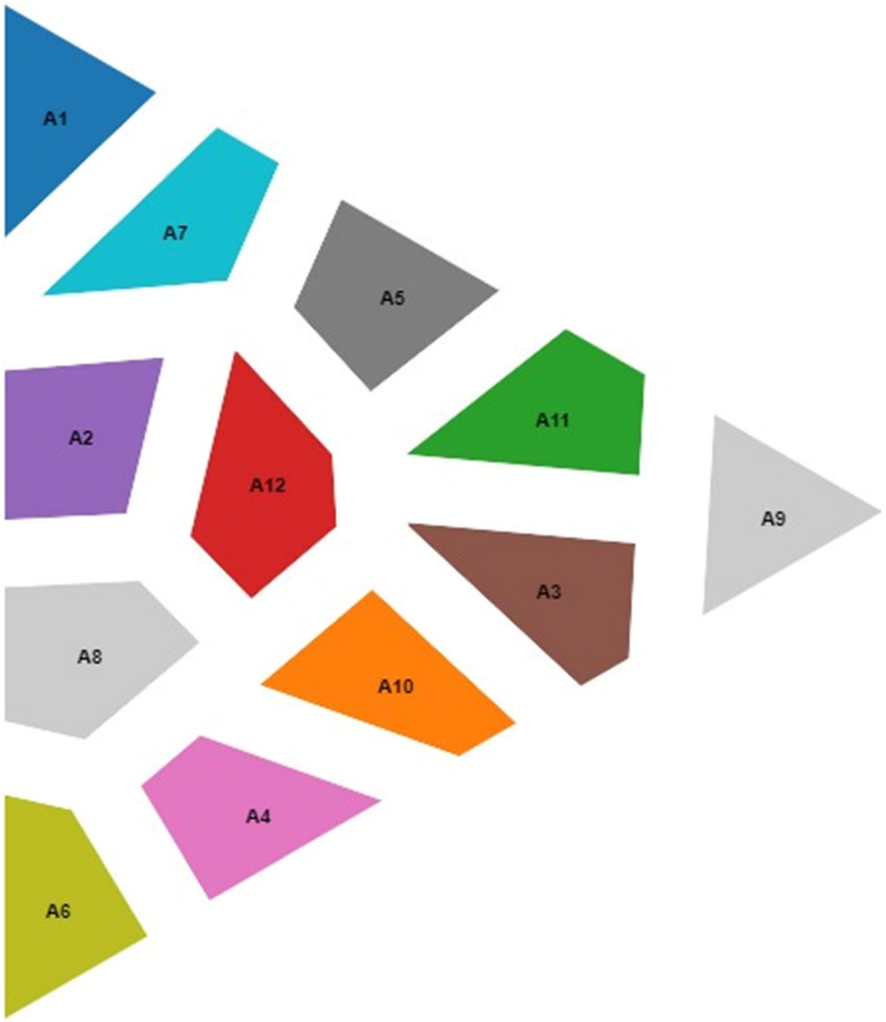

Fig. 4 Representation of overall alternatives

resistance ($F8$), non-repudiation ($F9$), authorization ($F10$), mobility ($F11$), access control ($F12$), unbrace ability ($F13$), accountability ($F14$), anonymity ($F15$), trust ($F16$), secrecy ($F17$), and unforgeability ($F18$). All the chosen criteria in this study are beneficial and thoroughly reviewed. The computational outputs of this process are as follows sequentially.

4.1.2 Comparison matrix

Each of the study's criteria was assigned a specific score between 1 and 10, with 10 being the highest. Equation (1) has been used to create the matrix with 12 possibilities and 18 parameters.

$$E = \begin{array}{c} A_1 \\ \cdot \\ \cdot \\ A_{12} \end{array} \begin{bmatrix} F_1 & \dots & F_n \\ X_{11} & \dots & X_{1n} \\ \vdots & \dots & \vdots \\ X_{m1} & \dots & X_{mn} \end{bmatrix} \tag{1}$$

The decision matrix for the criterion weightage calculation is drawn by using the above equation. Initial scores on a scale from one to ten are assigned. Figure 4 shows the representation. The decision matrix containing the initial score is listed in Table 2.

4.1.3 Normalized matrix

The normalization process is essential for ensuring device reliability and consistency as well as for protecting the Internet of things (IoT). Entropy values are standardized and scaled, which minimizes the risks posed by distortion or suspect sources. Additionally, normalization ensures the reliability of entropy sources, enhances the security and durability of systems against attacks, and increases the strength and variability of encryption keys and information. These steps contribute to enhancing overall security of IoT devices in a connected environment. We put Eq. (2) into practice to obtain the necessary normalized matrix. Table 3 shows the results that were obtained. With regard to the significance of the selected choices and factors, baseline ratings have been given to each. The options were then contrasted according to how crucial they were to the normalization exercise.

$$r_{ij} = \frac{a_{ij}}{\sum_{j=1}^{n} a_{ij}} \tag{2}$$

At first, the values placed in every column are added and their total sum is identified. Then, the initial score of every column is divided by their concerned total sum to get the normalized values. All the calculated outputs are described in Table 3.

4.1.4 Entropy and diversification calculation

The entropy and diversity scores were calculated using the corresponding Eqs. (3 and 4). First, we use Eq. (3) to determine the entropy ratios. On the basis of this, the results of diversification are obtained, and Eq. (4) has been used.

$$\text{entropy}(e) = -h\left(\sum_{\mathrm{i}=1}^{m} r_{ij} * \ln\left(r_{ij}\right)\right) \tag{3}$$

Table 2 The pairwise matrix of comparison

Criteria / Alternatives	$F1$	$F2$	$F3$	$F4$	$F5$	$F6$	$F7$	$F8$	$F9$	$F10$	$F11$	$F12$	$F13$	$F14$	$F15$	$F16$	$F17$	$F18$
$A1$	2	5	9	3	6	4	9	7	3	5	8	2	9	6	8	4	7	5
$A2$	5	9	2	7	4	3	6	2	8	2	5	7	3	8	2	6	4	9
$A3$	7	3	5	4	8	6	2	9	4	7	3	6	8	5	7	3	8	6
$A4$	3	6	8	9	5	2	7	4	5	8	6	9	2	7	4	8	2	3
$A5$	9	4	3	2	7	8	5	6	9	3	2	5	7	3	9	2	5	4
$A6$	4	8	2	5	9	7	6	3	2	5	7	4	9	6	3	5	7	2
$A7$	2	7	6	8	3	5	4	9	7	2	4	8	5	9	6	7	3	8
$A8$	5	3	4	2	6	9	8	7	5	4	9	6	3	4	5	9	8	7
$A9$	8	6	9	7	2	3	5	4	8	6	2	9	8	2	7	4	6	3
$A10$	3	9	5	4	7	6	2	8	4	9	3	7	6	5	3	8	4	9
$A11$	7	2	8	6	3	4	9	5	7	2	5	8	4	9	2	5	6	4
$A12$	5	8	3	5	9	2	4	7	6	3	4	2	8	2	5	6	9	8

Table 3 Normalized matrix

	$F1$	$F2$	$F3$	$F4$	$F5$	$F6$	$F7$	$F8$	$F9$	$F10$	$F11$	$F12$	$F13$	$F14$	$F15$	$F16$	$F17$	$F18$
$A1$	0.033	0.071	0.141	0.048	0.087	0.068	0.134	0.099	0.044	0.089	0.138	0.027	0.125	0.091	0.131	0.060	0.101	0.074
$A2$	0.083	0.129	0.031	0.113	0.058	0.051	0.090	0.028	0.118	0.036	0.086	0.096	0.042	0.121	0.033	0.090	0.058	0.132
$A3$	0.117	0.043	0.078	0.065	0.116	0.102	0.030	0.127	0.059	0.125	0.052	0.082	0.111	0.076	0.115	0.045	0.116	0.088
$A4$	0.050	0.086	0.125	0.145	0.072	0.034	0.104	0.056	0.074	0.143	0.103	0.123	0.028	0.106	0.066	0.119	0.029	0.044
$A5$	0.150	0.057	0.047	0.032	0.101	0.136	0.075	0.085	0.132	0.054	0.034	0.068	0.097	0.045	0.148	0.030	0.072	0.059
$A6$	0.067	0.114	0.031	0.081	0.130	0.119	0.090	0.042	0.029	0.089	0.121	0.055	0.125	0.091	0.049	0.075	0.101	0.029
$A7$	0.033	0.100	0.094	0.129	0.043	0.085	0.060	0.127	0.103	0.036	0.069	0.110	0.069	0.136	0.098	0.104	0.043	0.118
$A8$	0.083	0.043	0.063	0.032	0.087	0.153	0.119	0.099	0.074	0.071	0.155	0.082	0.042	0.061	0.082	0.134	0.116	0.103
$A9$	0.133	0.086	0.141	0.113	0.029	0.051	0.075	0.056	0.118	0.107	0.034	0.123	0.111	0.030	0.115	0.060	0.087	0.044
$A10$	0.050	0.129	0.078	0.065	0.101	0.102	0.030	0.113	0.059	0.161	0.052	0.096	0.083	0.076	0.049	0.119	0.058	0.132
$A11$	0.117	0.029	0.125	0.097	0.043	0.068	0.134	0.070	0.103	0.036	0.086	0.110	0.056	0.136	0.033	0.075	0.087	0.059
$A12$	0.083	0.114	0.047	0.081	0.130	0.034	0.060	0.099	0.088	0.054	0.069	0.027	0.111	0.030	0.082	0.090	0.130	0.118

here$j = 1, 2, \dots, n$. And as we know that $h = 1/\ln(m)$, where m indicates a set of alternatives

$$\text{So } h = 1/\ln(12), \text{ hence, } h = 1/2.48491$$

$$h = 0.40243 \text{ and } -h = -0.40243$$

$$\text{Diversification } (d) = 1 - e \tag{4}$$

We divided this step into multiple other steps to easily identify the desired outcomes. At first, we identify the values of a set that is inside the brackets. After the identification of their values, we then sum them column vice and multiply their total sum with the determined value of "*h*" to get the desired outputs of entropy. To continue this procedure, we then apply the next equation in the same step by minus the values of entropy from 1 to get the diversification outcomes. Table 4 shows the entropy and diversification values of security features.

4.1.5 Criterion weights

The comparative importance of the specifications is determined by dividing the diversity score of each column by the entirety of those scores. Utilizing Eq. (5), criteria weights have been calculated.

$$\text{Weight}(W) = \frac{d}{(\sum d)} \tag{5}$$

Based on the above equation, we get the desired weightage of each criterion. According to this, we divide each diversification value by its total sum to get the criterion weightage. Table 5 presents the calculated measures for every factor.

After the determination of the weightage of each criterion, it is necessary to indicate it in graphical form for easy understanding. We organized the derived weightage of each criterion that is evaluated and selected in this research in a graphical form. The derived weights of each criterion are illustrated in Fig. 5.

The percentage-wise criteria weights of each alternatives are shown in Fig. 6.

4.2 EDAS approach

It is a type of MCDM technique that is widely utilized in evaluation and selection scenarios where the situation is complex and making an efficient decision is hard. It is implemented for the efficient determination of the ranking of multiple alternatives. It consists of several easy equations that make it viable to use in complex scenarios easily. It is further solved and used in multi-criteria problems where the evaluation of a set of different alternatives based on their components is difficult and ambiguous [34]. It can decrease the computational burden on evaluators and save their time and cost. The required steps involved in this mechanism are mentioned in Fig. 7.

Table 4 Entropy and diversification values

	$F1$	$F2$	$F3$	$F4$	$F5$	$F6$	$F7$	$F8$	$F9$	$F10$	$F11$	$F12$	$F13$	$F14$	$F15$	$F16$	$F17$	$F18$	$\sum d$
$A1$	−0.113	−0.189	−0.276	−0.147	−0.212	−0.182	−0.270	−0.228	−0.138	−0.216	−0.273	−0.099	−0.260	−0.218	−0.266	−0.168	−0.232	−0.192	
$A2$	−0.207	−0.264	−0.108	−0.246	−0.165	−0.151	−0.216	−0.101	−0.252	−0.119	−0.211	−0.225	−0.132	−0.256	−0.112	−0.216	−0.165	−0.268	
$A3$	−0.251	−0.135	−0.199	−0.177	−0.250	−0.232	−0.105	−0.262	−0.167	−0.260	−0.153	−0.205	−0.244	−0.195	−0.248	−0.139	−0.250	−0.214	
$A4$	−0.150	−0.211	−0.260	−0.280	−0.190	−0.115	−0.236	−0.162	−0.192	−0.278	−0.235	−0.258	−0.100	−0.238	−0.179	−0.254	−0.103	−0.138	
$A5$	−0.285	−0.164	−0.143	−0.111	−0.232	−0.271	−0.194	−0.209	−0.268	−0.157	−0.116	−0.184	−0.227	−0.141	−0.282	−0.105	−0.190	−0.167	
$A6$	−0.181	−0.248	−0.108	−0.203	−0.266	−0.253	−0.216	−0.134	−0.104	−0.216	−0.255	−0.159	−0.260	−0.218	−0.148	−0.194	−0.232	−0.104	
$A7$	−0.113	−0.230	−0.222	−0.264	−0.136	−0.209	−0.168	−0.262	−0.234	−0.119	−0.184	−0.242	−0.185	−0.272	−0.228	−0.236	−0.136	−0.252	
$A8$	−0.207	−0.135	−0.173	−0.111	−0.212	−0.287	−0.254	−0.228	−0.192	−0.189	−0.289	−0.205	−0.132	−0.170	−0.205	−0.270	−0.250	−0.234	
$A9$	−0.269	−0.211	−0.276	−0.246	−0.103	−0.151	−0.194	−0.162	−0.252	−0.239	−0.116	−0.258	−0.244	−0.106	−0.248	−0.168	−0.212	−0.138	
$A10$	−0.150	−0.264	−0.199	−0.177	−0.232	−0.232	−0.105	−0.246	−0.167	−0.294	−0.153	−0.225	−0.207	−0.195	−0.148	−0.254	−0.165	−0.268	
$A11$	−0.251	−0.102	−0.260	−0.226	−0.136	−0.182	−0.270	−0.187	−0.234	−0.119	−0.211	−0.242	−0.161	−0.272	−0.112	−0.194	−0.212	−0.167	
$A12$	−0.207	−0.248	−0.143	−0.203	−0.266	−0.115	−0.168	−0.228	−0.214	−0.157	−0.184	−0.099	−0.244	−0.106	−0.205	−0.216	−0.266	−0.252	
e	0.959	0.965	0.953	0.962	0.966	0.959	0.964	0.969	0.971	0.950	0.959	0.966	0.964	0.960	0.959	0.971	0.971	0.962	
d	0.041	0.035	0.047	0.038	0.034	0.041	0.036	0.031	0.029	0.050	0.041	0.034	0.036	0.040	0.041	0.029	0.029	0.038	0.668

Table 5 Criterion weights

Criteria	*W*	*W* in %
*F*1	0.062	6.159
*F*2	0.052	5.214
*F*3	0.070	7.000
*F*4	0.057	5.670
*F*5	0.051	5.065
*F*6	0.062	6.193
*F*7	0.054	5.427
*F*8	0.046	4.577
*F*9	0.044	4.385
*F*10	0.074	7.426
*F*11	0.062	6.176
*F*12	0.051	5.051
*F*13	0.053	5.345
*F*14	0.059	5.932
*F*15	0.061	6.142
*F*16	0.043	4.322
*F*17	0.043	4.288
*F*18	0.056	5.627

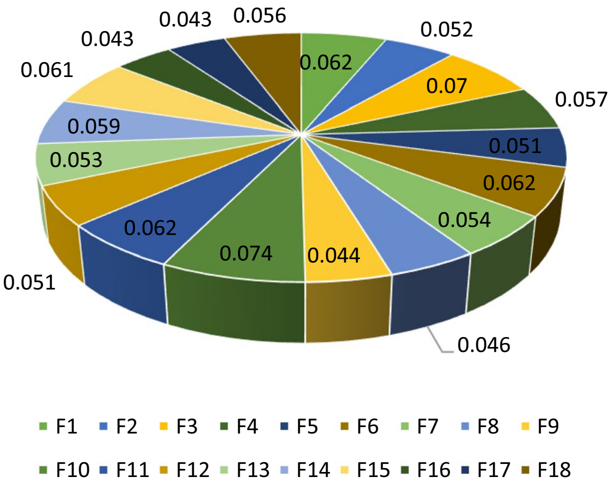

Fig. 5 Criterion weights of overall security features (*F*1–*F*18)

4.2.1 Numerical work of EDAS

The EDAS method is adopted to measure IoT security and ranked the chosen alternatives. This approach involved multiple equations that help us in the precision evaluation and determination of the ranking of a set of different kinds of alternatives.

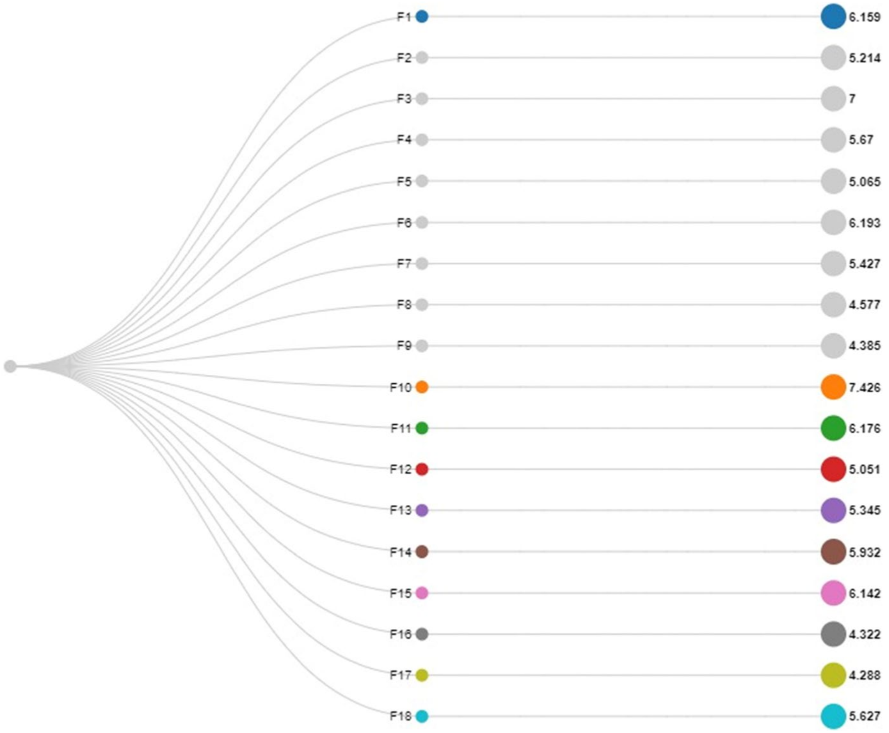

Fig. 6 Representation of criteria weights in percentages

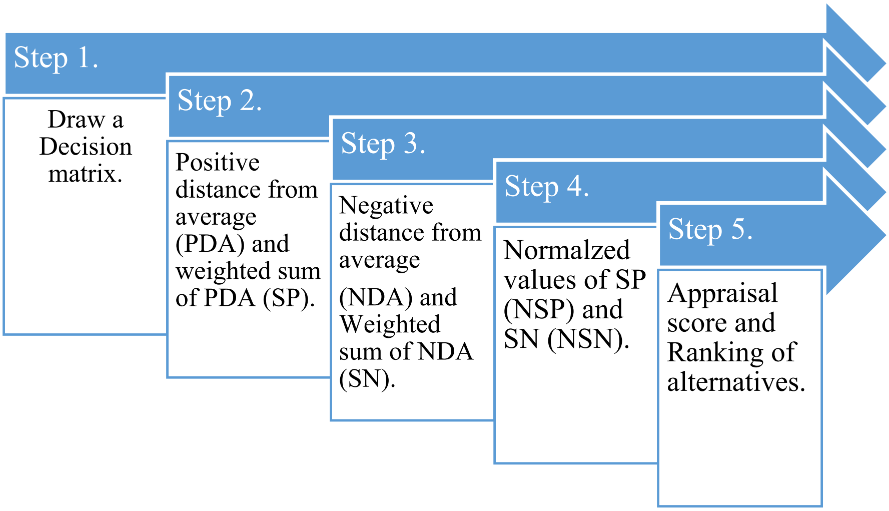
Step 1.
Draw a Decision matrix.
Step 2.
Positive distance from average (PDA) and weighted sum of PDA (SP).
Step 3.
Negative distance from average (NDA) and Weighted sum of NDA (SN).
Step 4.
Normalzed values of SP (NSP) and SN (NSN).
Step 5.
Appraisal score and Ranking of alternatives.

Fig. 7 The various steps of EDAS approach

Twelve alternatives are selected in this study that is evaluated and ranked based on their essential 18 components. All the criteria that are chosen for the evaluation are beneficial. In the end, the selected alternatives from $A1$ to $A12$ have been ranked chronologically. The computational outcomes of this process are as follows.

4.2.2 Comparison matrix and average calculation

The comparison matrix for the EDAS is the same as mentioned in Table 2 for entropy. The average for further processing has been determined by using Eq. (6) given as follows:

$$\boldsymbol{AV_j} = \frac{\sum_{i=1}^{\boldsymbol{n}} \boldsymbol{A_{ij}}}{\boldsymbol{n}} \tag{6}$$

The above equation is initially used to measure the average values of each column. According to this, the total sum of values is divided by the total number of alternatives to obtain the average outcomes. All the generated average outcomes along with the initial score are mentioned in Table 6.

4.2.3 Positive distance from average (PDA)

The PDA results are produced using Eqs. (7 and 8), respectively. Algorithm (7) serves to determine the scores for beneficial criteria, although algorithm (8) is performed to determine the values for non-beneficial criteria. The obtained PDA readings and criteria grades are outlined in Table 7.

If *j*th criteria are beneficial:

$$\mathbf{PDA}_{ij} = \frac{\mathbf{max}(0, \left(\boldsymbol{A_{ij}} - \boldsymbol{AV_j}\right))}{\boldsymbol{AV_j}} \tag{7f}$$

If *j*th criteria are non-beneficial:

$$\mathbf{PDA}_{ij} = \frac{\mathbf{max}(0, \left(\boldsymbol{AV_j} - \boldsymbol{A_{ij}}\right))}{\boldsymbol{AV_j}} \tag{8}$$

Based on the above equations, we obtained the desired outputs of PDA. Here, we apply Eq. (10) in detail to calculate the required PDA scores of every alternative based on their chosen criteria. All the calculated outputs along with criteria weights are listed in Table 7.

4.2.4 Weighted sum of PDA (SP)

The equation listed in the following is used to determine SP outcomes. According to Eq. (9), the criterion weights have been multiplied by their concern column values in the PDA matrix and then sum their resultant values to obtain the SP outputs.

Table 6 The pairwise comparison matrix

Criteria / Alternatives	$F1$	$F2$	$F3$	$F4$	$F5$	$F6$	$F7$	$F8$	$F9$	$F10$	$F11$	$F12$	$F13$	$F14$	$F15$	$F16$	$F17$	$F18$
$A1$	2	5	9	3	6	4	9	7	3	5	8	2	9	6	8	4	7	5
$A2$	5	9	2	7	4	3	6	2	8	2	5	7	3	8	2	6	4	9
$A3$	7	3	5	4	8	6	2	9	4	7	3	6	8	5	7	3	8	6
$A4$	3	6	8	9	5	2	7	4	5	8	6	9	2	7	4	8	2	3
$A5$	9	4	3	2	7	8	5	6	9	3	2	5	7	3	9	2	5	4
$A6$	4	8	2	5	9	7	6	3	2	5	7	4	9	6	3	5	7	2
$A7$	2	7	6	8	3	5	4	9	7	2	4	8	5	9	6	7	3	8
$A8$	5	3	4	2	6	9	8	7	5	4	9	6	3	4	5	9	8	7
$A9$	8	6	9	7	2	3	5	4	8	6	2	9	8	2	7	4	6	3
$A10$	3	9	5	4	7	6	2	8	4	9	3	7	6	5	3	8	4	9
$A11$	7	2	8	6	3	4	9	5	7	2	5	8	4	9	2	5	6	4
$A12$	5	8	3	5	9	2	4	7	6	3	4	2	8	2	5	6	9	8
AVj	5	5.83	5.33	5.17	5.75	4.92	5.58	5.92	5.67	4.67	4.83	6.08	6	5.5	5.08	5.58	5.75	5.67

Table 7 Positive distance average (PDA)

	*F*1	*F*2	*F*3	*F*4	*F*5	*F*6	*F*7	*F*8	*F*9	*F*10	*F*11	*F*12	*F*13	*F*14	*F*15	*F*16	*F*17	*F*18
C. Weights	0.062	0.052	0.070	0.057	0.051	0.062	0.054	0.0458	0.044	0.074	0.062	0.051	0.053	0.059	0.061	0.043	0.043	0.056
*A*1	0.000	0.000	0.688	0.000	0.043	0.000	0.612	0.183	0.000	0.071	0.655	0.000	0.500	0.091	0.574	0.000	0.217	0.000
*A*2	0.000	0.543	0.000	0.355	0.000	0.000	0.075	0.000	0.412	0.000	0.034	0.151	0.000	0.455	0.000	0.075	0.000	0.588
*A*3	0.400	0.000	0.000	0.000	0.391	0.220	0.000	0.521	0.000	0.500	0.000	0.000	0.333	0.000	0.377	0.000	0.391	0.059
*A*4	0.000	0.029	0.500	0.742	0.000	0.000	0.254	0.000	0.000	0.714	0.241	0.479	0.000	0.273	0.000	0.433	0.000	0.000
*A*5	0.800	0.000	0.000	0.000	0.217	0.627	0.000	0.014	0.588	0.000	0.000	0.000	0.167	0.000	0.770	0.000	0.000	0.000
*A*6	0.000	0.371	0.000	0.000	0.565	0.424	0.075	0.000	0.000	0.071	0.448	0.000	0.500	0.091	0.000	0.000	0.217	0.000
*A*7	0.000	0.200	0.125	0.548	0.000	0.017	0.000	0.521	0.235	0.000	0.000	0.315	0.000	0.636	0.180	0.254	0.000	0.412
*A*8	0.000	0.000	0.000	0.000	0.043	0.831	0.433	0.183	0.000	0.000	0.862	0.000	0.000	0.000	0.000	0.612	0.391	0.235
*A*9	0.600	0.029	0.688	0.355	0.000	0.000	0.000	0.000	0.412	0.286	0.000	0.479	0.333	0.000	0.377	0.000	0.043	0.000
*A*10	0.000	0.543	0.000	0.000	0.217	0.220	0.000	0.352	0.000	0.929	0.000	0.151	0.000	0.000	0.000	0.433	0.000	0.588
*A*11	0.400	0.000	0.500	0.161	0.000	0.000	0.612	0.000	0.235	0.000	0.034	0.315	0.000	0.636	0.000	0.000	0.043	0.000
*A*12	0.000	0.371	0.000	0.000	0.565	0.000	0.000	0.183	0.059	0.000	0.000	0.000	0.333	0.000	0.000	0.075	0.565	0.412

$$\mathrm{SP}_i = \sum_{j=0}^{m} w_j * \mathrm{PDA}_{ij} \tag{9}$$

The above equation is implemented for the identification of desired SP values. On the basis of this, the SP output is achieved by multiplying each criterion weight with their similar column containing PDA scores. Table 8 presents an outline of the derived SP findings.

4.2.5 Negative distance from average (NDA)

To determine the NDA accurately, we utilize algorithms (10 and 11). Here, Eq. (10) is applied to measure the score of beneficial criteria, although Eq. (11) is adopted to compute the scores of non-beneficial criteria.

If *j*th criteria are beneficial:

$$\mathbf{NDA}_{ij} = \frac{\mathbf{max}(0, \left(\mathbf{AV}_j - A_{ij}\right))}{\mathbf{AV}_j} \tag{10}$$

If *j*th criteria are non-beneficial:

$$\mathbf{NDA}_{ij} = \frac{\mathbf{max}(0, \left(A_{ij} - \mathbf{AV}_j\right))}{\mathbf{AV}_j} \tag{11}$$

After the utilization of the above equations, we derived the desired outcomes of NDA. Here, we implement Eq. (10) in detail to measure the NDA values of each and every alternative based on their chosen criteria. All the determined outputs along with criteria weights are listed in Table 9.

4.2.6 Weighted sum of NDA (SN)

For the measurement of SN outputs, we apply Eq. (12). As mentioned in the following equation, the criterion weights have multiplied by their concern column values in the NDA matrix and then sum their scores to obtain the SN outcomes. All the derived outcomes are depicted in Table 10.

$$\mathrm{SN}_i = \sum_{j=1}^{m} w_j * \mathrm{NDA}_{ij} \tag{12}$$

The above equation is implemented for the identification of desired SN values. On the basis of this, the SN output is achieved by multiplying each criterion weight with their similar column containing NDA values. Table 10 presents an outline of the derived SN findings.

Table 8 The SP calculation

	*F*1	*F*2	*F*3	*F*4	*F*5	*F*6	*F*7	*F*8	*F*9	*F*10	*F*11	*F*12	*F*13	*F*14	*F*15	*F*16	*F*17	*F*18	SP
*A*1	0.000	0.000	0.048	0.000	0.002	0.000	0.033	0.008	0.000	0.005	0.040	0.000	0.027	0.005	0.035	0.000	0.009	0.000	0.214
*A*2	0.000	0.028	0.000	0.020	0.000	0.000	0.004	0.000	0.018	0.000	0.002	0.008	0.000	0.027	0.000	0.003	0.000	0.033	0.144
*A*3	0.025	0.000	0.000	0.000	0.020	0.014	0.000	0.024	0.000	0.037	0.000	0.000	0.018	0.000	0.023	0.000	0.017	0.003	0.180
*A*4	0.000	0.001	0.035	0.042	0.000	0.000	0.014	0.000	0.000	0.053	0.015	0.024	0.000	0.016	0.000	0.019	0.000	0.000	0.219
*A*5	0.049	0.000	0.000	0.000	0.011	0.039	0.000	0.001	0.026	0.000	0.000	0.000	0.009	0.000	0.047	0.000	0.000	0.000	0.182
*A*6	0.000	0.019	0.000	0.000	0.029	0.026	0.004	0.000	0.000	0.005	0.028	0.000	0.027	0.005	0.000	0.000	0.009	0.000	0.153
*A*7	0.000	0.010	0.009	0.031	0.000	0.001	0.000	0.024	0.010	0.000	0.000	0.016	0.000	0.038	0.011	0.011	0.000	0.023	0.184
*A*8	0.000	0.000	0.000	0.000	0.002	0.051	0.023	0.008	0.000	0.000	0.053	0.000	0.000	0.000	0.000	0.026	0.017	0.013	0.195
*A*9	0.037	0.001	0.048	0.020	0.000	0.000	0.000	0.000	0.018	0.021	0.000	0.024	0.018	0.000	0.023	0.000	0.002	0.000	0.213
*A*10	0.000	0.028	0.000	0.000	0.011	0.014	0.000	0.016	0.000	0.069	0.000	0.008	0.000	0.000	0.000	0.019	0.000	0.033	0.197
*A*11	0.025	0.000	0.035	0.009	0.000	0.000	0.033	0.000	0.010	0.000	0.002	0.016	0.000	0.038	0.000	0.000	0.002	0.000	0.170
*A*12	0.000	0.019	0.000	0.000	0.029	0.000	0.000	0.008	0.003	0.000	0.000	0.000	0.018	0.000	0.000	0.003	0.024	0.023	0.127

Table 9 The negative distance average (NDA)

	*F*1	*F*2	*F*3	*F*4	*F*5	*F*6	*F*7	*F*8	*F*9	*F*10	*F*11	*F*12	*F*13	*F*14	*F*15	*F*16	*F*17	*F*18
C. Weights	0.062	0.052	0.070	0.057	0.051	0.062	0.054	0.0458	0.044	0.074	0.062	0.051	0.053	0.059	0.061	0.043	0.043	0.056
*A*1	0.600	0.143	0.000	0.419	0.000	0.186	0.000	0.000	0.471	0.000	0.000	0.671	0.000	0.000	0.000	0.284	0.000	0.118
*A*2	0.000	0.000	0.625	0.000	0.304	0.390	0.000	0.662	0.000	0.571	0.000	0.000	0.500	0.000	0.607	0.000	0.304	0.000
*A*3	0.000	0.486	0.062	0.226	0.000	0.000	0.642	0.000	0.294	0.000	0.379	0.014	0.000	0.091	0.000	0.463	0.000	0.000
*A*4	0.400	0.000	0.000	0.000	0.130	0.593	0.000	0.324	0.118	0.000	0.000	0.000	0.667	0.000	0.213	0.000	0.652	0.471
*A*5	0.000	0.314	0.438	0.613	0.000	0.000	0.104	0.000	0.000	0.357	0.586	0.178	0.000	0.455	0.000	0.642	0.130	0.294
*A*6	0.200	0.000	0.625	0.032	0.000	0.000	0.000	0.493	0.647	0.000	0.000	0.342	0.000	0.000	0.410	0.104	0.000	0.647
*A*7	0.600	0.000	0.000	0.000	0.478	0.000	0.284	0.000	0.000	0.571	0.172	0.000	0.167	0.000	0.000	0.000	0.478	0.000
*A*8	0.000	0.486	0.250	0.613	0.000	0.000	0.000	0.000	0.118	0.143	0.000	0.014	0.500	0.273	0.016	0.000	0.000	0.000
*A*9	0.000	0.000	0.000	0.000	0.652	0.390	0.104	0.324	0.000	0.000	0.586	0.000	0.000	0.636	0.000	0.284	0.000	0.471
*A*10	0.400	0.000	0.062	0.226	0.000	0.000	0.642	0.000	0.294	0.000	0.379	0.000	0.000	0.091	0.410	0.000	0.304	0.000
*A*11	0.000	0.657	0.000	0.000	0.478	0.186	0.000	0.155	0.000	0.571	0.000	0.000	0.333	0.000	0.607	0.104	0.000	0.294
*A*12	0.000	0.000	0.438	0.032	0.000	0.593	0.284	0.000	0.000	0.357	0.172	0.671	0.000	0.636	0.016	0.000	0.000	0.000

Table 10 The SN calculation

	$F1$	$F2$	$F3$	$F4$	$F5$	$F6$	$F7$	$F8$	$F9$	$F10$	$F11$	$F12$	$F13$	$F14$	$F15$	$F16$	$F17$	$F18$	SN
$A1$	0.037	0.007	0.000	0.024	0.000	0.012	0.000	0.000	0.021	0.000	0.000	0.034	0.000	0.000	0.000	0.012	0.000	0.007	0.153
$A2$	0.000	0.000	0.044	0.000	0.015	0.024	0.000	0.030	0.000	0.042	0.000	0.000	0.027	0.000	0.037	0.000	0.013	0.000	0.233
$A3$	0.000	0.025	0.004	0.013	0.000	0.000	0.035	0.000	0.013	0.000	0.023	0.001	0.000	0.005	0.000	0.020	0.000	0.000	0.140
$A4$	0.025	0.000	0.000	0.000	0.007	0.037	0.000	0.015	0.005	0.000	0.000	0.000	0.036	0.000	0.013	0.000	0.028	0.026	0.191
$A5$	0.000	0.016	0.031	0.035	0.000	0.000	0.006	0.000	0.000	0.027	0.036	0.009	0.000	0.027	0.000	0.028	0.006	0.017	0.236
$A6$	0.012	0.000	0.044	0.002	0.000	0.000	0.000	0.023	0.028	0.000	0.000	0.017	0.000	0.000	0.025	0.005	0.000	0.036	0.192
$A7$	0.037	0.000	0.000	0.000	0.024	0.000	0.015	0.000	0.000	0.042	0.011	0.000	0.009	0.000	0.000	0.000	0.021	0.000	0.159
$A8$	0.000	0.025	0.017	0.035	0.000	0.000	0.000	0.000	0.005	0.011	0.000	0.001	0.027	0.016	0.001	0.000	0.000	0.000	0.138
$A9$	0.000	0.000	0.000	0.000	0.033	0.024	0.006	0.015	0.000	0.000	0.036	0.000	0.000	0.038	0.000	0.012	0.000	0.026	0.190
$A10$	0.025	0.000	0.004	0.013	0.000	0.000	0.035	0.000	0.013	0.000	0.023	0.000	0.000	0.005	0.025	0.000	0.013	0.000	0.157
$A11$	0.000	0.034	0.000	0.000	0.024	0.012	0.000	0.007	0.000	0.042	0.000	0.000	0.018	0.000	0.037	0.005	0.000	0.017	0.196
$A12$	0.000	0.000	0.031	0.002	0.000	0.037	0.015	0.000	0.000	0.027	0.011	0.034	0.000	0.038	0.001	0.000	0.000	0.000	0.194

4.2.7 Normalizing the values of SP and SN

The following algorithms (13 and 14) have been adopted to identify the normalized values of SP (NSP) and normalized values of SN (NSN). Algorithm (13) has been applied for the calculation of NSP scores, although algorithm (14) has been adopted for the measurement of NSN values. Figure 8 shows the representation of these values.

For the normalization of SP values:

$$\mathrm{NSP}_i = \frac{\mathrm{SP}_i}{\max(\mathrm{SP}_i)} \tag{13}$$

For the normalization of SN values:

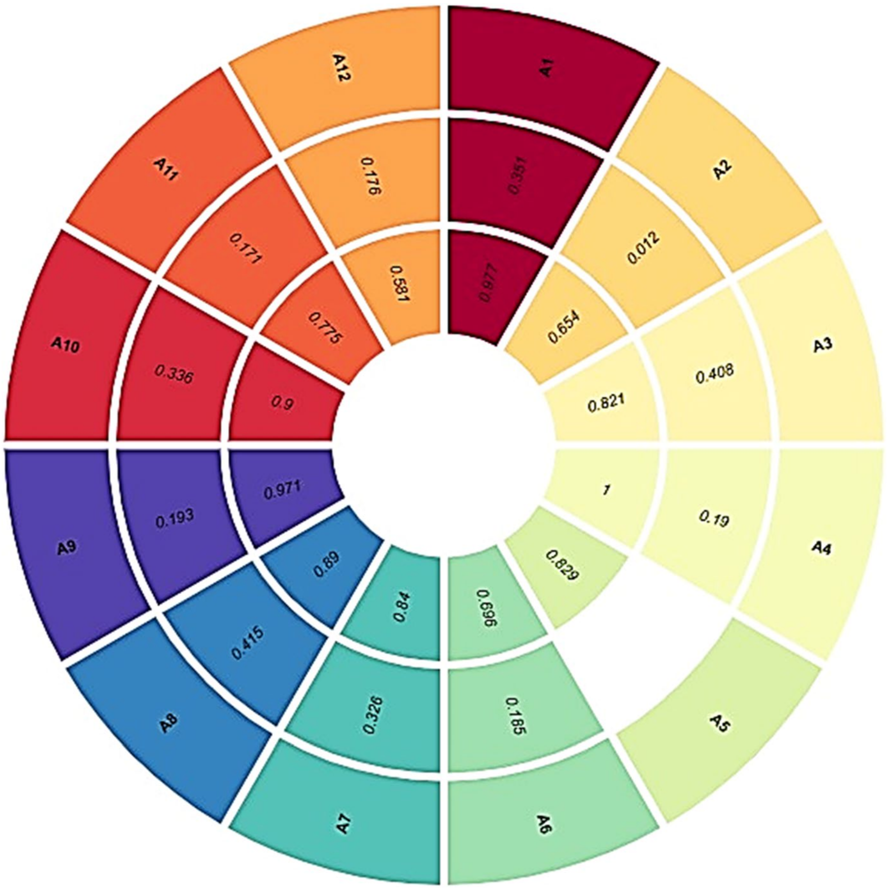

Fig. 8 Representation of normalizing values

Table 11 Normalized values of SP and SN along with AS

Alternatives	NSP_i	NSN_i	AS
*A*1	0.977	0.351	0.664
*A*2	0.654	0.012	0.333
*A*3	0.821	0.408	0.615
*A*4	1.000	0.190	0.595
*A*5	0.829	0.000	0.414
*A*6	0.696	0.185	0.441
*A*7	0.840	0.326	0.583
*A*8	0.890	0.415	0.653
*A*9	0.971	0.193	0.582
*A*10	0.900	0.336	0.618
*A*11	0.775	0.171	0.473
*A*12	0.581	0.176	0.378

Table 12 AS and ranking of alternatives

Alternatives	*A*1	*A*2	*A*3	*A*4	*A*5	*A*6	*A*7	*A*8	*A*9	*A*10	*A*11	*A*12
Final score	0.664	0.333	0.615	0.595	0.414	0.441	0.583	0.653	0.582	0.618	0.473	0.378
Ranking	1	12	4	5	10	9	6	2	7	3	8	11

$$\mathrm{NSN}_i = 1 - \frac{\mathrm{SN}_i}{\max(\mathrm{SN}_i)} \tag{14}$$

The normalized scores of SP and SN are identified in this step by using the above equations. At first, we determine the maximum value from SP and SN. After this, each SP and SN value is divided by the maximum value identified from a set of SP and SN to get the desired NSP and NSN outcomes. All the derived outputs are shown in Table 11.

4.2.8 Appraisal score (AS) and ranking of alternatives

The AS values have been determined by using Eq. (15). Based on the AS values, all the chosen alternatives are ranked chronologically.

$$\mathrm{AS}_i = \frac{1}{2}(\mathrm{NSP}_i + \mathrm{NSN}_i) \tag{15}$$

According to the above equation, the values of NSP and NSN are summed individually, and then multiply each output with 0.5 to get the desired AS scores. After the identification of these values, a set of different alternatives is organized in a chronological manner to make an efficient decision easily. The entire outputs of AS and the ranking of alternatives are listed in Table 12.

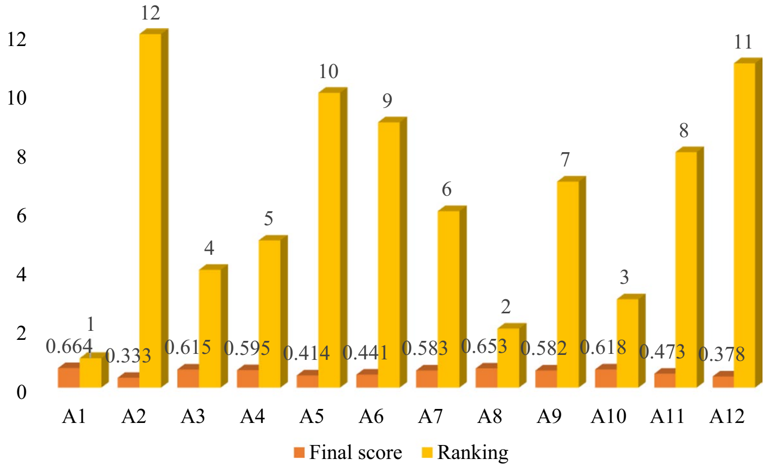

Fig. 9 Final outputs and ranking of alternatives

After the identification of the relative closeness and ranking of each alternative, it is necessary to show the derived values and position of these alternatives in a graphical form that is easily understandable by researchers and experts. Here, we show all the derived outcomes along with the ranking of each alternative in graphical format. The final score and ranking of each alternative are described in Fig. 9.

5 Conclusion

The rapid growth of the IoT is due to developments in communication technology, device mobility, and computer system accessibility. However, these characteristics give rise to certain issues, such as security of confidential information. To protect the IoT system's hardware and network components, IoT security is essential. Due to the peculiarities of IoT devices, security design in the IoT is more difficult due to high degree of scalability, cheap design, resource limitations, and device variability. Implementing security measures is more challenging because of the wide range of devices and protocols, as well as the size or number of network nodes in an IoT system. The majority of security techniques and approaches have been built on approved Internet security norms. In this research study, security features are evaluated using multi-optimization method such as entropy and EDAS to highlight the significant most features to protect IoT devices from security-related issues. The study will assist organization to ensure that their system is using robust authentication protocols, data encryption techniques, routine firmware upgrades, malware detection, and prevention tools for securing their operations.

Author contributions I.U. was involved in conceptualization, data curation, methodology, and hardware. I.U., A.N., and F.A. were involved in formal analysis. I.U. and A.N. contributed to software; S.N. was involved in supervision; F.A. and Y.Y.G. were involved in visualization; I.U. and F.A. were involved in

writing—original draft; and A.N., F.A., S.N., Y.Y.G., and N.A. were involved in writing—review and editing. All authors have read and agreed to the published version of the manuscript.

Funding This research received no external funding.

Data availability The dataset used for this study is available on reasonable request from the corresponding author.

Declarations

Conflict of interest The authors declare no conflict of interests.

Ethical approval Not applicable.

Consent for publication Not applicable.

References

1. Whitmore A, Agarwal A, Da Xu L (2015) The Internet of Things—a survey of topics and trends. Inf Syst Front 17:261–274
2. Feki MA et al (2013) The internet of things: the next technological revolution. Computer 46(2):24–25
3. Mosenia A, Jha NK (2016) A comprehensive study of security of internet-of-things. IEEE Trans Emerg Top Comput 5(4):586–602
4. Ray PP (2018) A survey on Internet of Things architectures. J King Saud Univ-Comput Inf Sci 30(3):291–319
5. Perera C et al (2014) A survey on internet of things from industrial market perspective. IEEE Access 2:1660–1679
6. Bandyopadhyay D, Sen J (2011) Internet of things: applications and challenges in technology and standardization. Wirel Pers Commun 58:49–69
7. Li S, Xu LD, Zhao S (2015) The internet of things: a survey. Inf Syst Front 17:243–259
8. Wortmann F, Flüchter K (2015) Internet of things: technology and value added. Bus Inf Syst Eng 57:221–224
9. Zanella A et al (2014) Internet of things for smart cities. IEEE Internet Things J 1(1):22–32
10. Zheng J et al (2011) The internet of things [Guest Editorial]. IEEE Commun Mag 49(11):30–31
11. Cao J, Zhu T, Ma R, Guo Z, Zhang Y, Li H (2022) A software-based remote attestation scheme for internet of things devices. IEEE Trans Dependable Secure Comput 20:1422–1434
12. Guo Y, Xie H, Wang C, Jia X (2021) Enabling privacy-preserving geographic range query in fog-enhanced iot services. IEEE Trans Dependable Secure Comput 19(5):3401–3416
13. Hayat RF, Aurangzeb S, Aleem M, Srivastava G, Lin JC (2022) ML-DDoS: a blockchain-based multilevel DDoS mitigation mechanism for IoT environments. IEEE Trans Eng Manag. https://doi.org/10.1109/TEM.2022.3170519
14. Heer T et al (2011) Security challenges in the IP-based internet of things. Wirel Pers Commun 61:527–542
15. Xing L (2020) Reliability in Internet of Things: current status and future perspectives. IEEE Internet Things J 7(8):6704–6721
16. Baldini G et al (2018) Ethical design in the internet of things. Sci Eng Ethics 24:905–925
17. Sanislav T et al (2021) Energy harvesting techniques for internet of things (IoT). IEEE Access 9:39530–39549
18. Neisse R et al (2015) SecKit: a model-based security toolkit for the internet of things. Comput Secur 54:60–76
19. Lv Z (2020) Virtual reality in the context of Internet of Things. Neural Comput Appl 32(13):9593–9602
20. Kumar S, Tiwari P, Zymbler M (2019) Internet of Things is a revolutionary approach for future technology enhancement: a review. J Big Data 6(1):1–21

21. Khan HU, Sohail M, Ali F, Nazir S, Ghadi YY, Ullah I (2023) Prioritizing the multi-criterial features based on comparative approaches for enhancing security of IoT devices. Phys Commun 1(59):102084
22. Golmaryami M, Taheri R, Pooranian Z, Shojafar M, Xiao P (2022) SETTI: a self-supervised adversarial malware detection architecture in an IoT environment. ACM Trans Multimed Comput Commun Appl 18(2):1–21
23. Ali MS et al (2018) Applications of blockchains in the Internet of Things: a comprehensive survey. IEEE Commun Surv Tutor 21(2):1676–1717
24. Sun C (2012) Application of RFID technology for logistics on internet of things. AASRI Proc 1:106–111
25. George G, Thampi SM (2020) Combinatorial analysis for securing IoT-assisted Industry 4.0 applications from vulnerability-based attacks. IEEE Trans Ind Inform 18(1):3–15
26. Alam S, Chowdhury MM, Noll J (2011) Interoperability of security-enabled internet of things. Wirel Pers Commun 61:567–586
27. Mezzanotte P et al (2021) Innovative RFID sensors for Internet of Things applications. IEEE J Microw 1(1):55–65
28. Huckle S et al (2016) Internet of things, blockchain and shared economy applications. Proc Comput Sci 98:461–466
29. Tsai C-W, Lai C-F, Vasilakos AV (2014) Future internet of things: open issues and challenges. Wirel Netw 20:2201–2217
30. Brooks C et al (2018) A component architecture for the internet of things. Proc IEEE 106(9):1527–1542
31. Liang F et al (2019) Machine learning for security and the internet of things: the good, the bad, and the ugly. IEEE Access 7:158126–158147
32. Al-Qaseemi SA, Almulhim HA, Almulhim MF, and Chaudhry SR (2016) IoT Architecture Challenges and Issues: Lack of Standardization. In: 2016 Future Technologies Conference (FTC), pp. 731–738. IEEE
33. Khan HU, Sohail M, Nazir S (2022) Features-based IoT security authentication framework using statistical aggregation, entropy, and MOORA approaches. IEEE Access 10:109326–109339
34. Abellana DPM, Roxas RR, Lao DM, Mayol PE, Lee S (2022) Ensemble feature selection in binary machine learning classification: A novel application of the evaluation based on distance from average solution (EDAS) method. Math Probl Eng 2022:1–13

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

Inam Ullah[1] · Asra Noor[2] · Shah Nazir[2] · Farhad Ali[2] · Yazeed Yasin Ghadi[3] · Nida Aslam[4]

✉ Asra Noor
asranoor997@gmail.com

[1] Department of Computer Engineering, Gachon University, Seongnam 13120, Republic of Korea

[2] Department of Computer Science, University of Swabi, Swabi, Pakistan

[3] Department of Computer Science, Al Ain University, P.O. Box 112612, Abu Dhabi, United Arab Emirates

[4] SAUDI ARAMCO Cybersecurity Chair, Department of Computer Science, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, 31441 Dammam, Saudi Arabia