mathematics

IMPACT FACTOR 2.4

CITESCORE 3.5

Article

A Features-Based Privacy Preserving Assessment Model for Authentication of Internet of Medical Things (IoMT) Devices in Healthcare

Habib Ullah Khan, Yasir Ali and Faheem Khan

MDPI

https://doi.org/10.3390/math11051197

mathematics

MDPI

Article

A Features-Based Privacy Preserving Assessment Model for Authentication of Internet of Medical Things (IoMT) Devices in Healthcare

Habib Ullah Khan [1,*], Yasir Ali [2] and Faheem Khan [3,*]

[1] Department of Accounting and Information Systems, College of Business and Economics, Qatar University, Doha 2713, Qatar
[2] Higher Education Department Khyber Pakhtunkhwa, Shahzeb Shaheed Government Degree College, Swabi 23430, Pakistan
[3] Department of Computer Engineering, Gachon University, Seongnam-si 13120, Republic of Korea
* Correspondence: habib.khan@qu.edu.qa (H.U.K.); faheem@gachon.ac.kr (F.K.)

Abstract: Internet of Things (IoT) devices have drawn significant attention over the last few years due to their significant contribution to every domain of life, but the major application of these devices has been witnessed in the healthcare sector. IoT devices have changed the complexion of healthcare set-up, however, the major limitation of such devices is susceptibility to many cyberattacks due to the use of embedded operating systems, the nature of communication, insufficient software updates, and the nature of backend resources. Similarly, they transfer a huge amount of sensitive data via sensors and actuators. Therefore, the security of Internet of Health Things (IoHT) devices remains a prime concern as these devices are prone to various cyberattacks, which can lead to compromising and violating the security of IoT devices. Therefore, IoT devices need to be authenticated before they join the network or communicate within a network, and the applied method of authentication must be robust and reliable. This authentication method has to be evaluated before being implemented for the authentication of IoT devices/equipment in a healthcare environment. In this study, an evaluation framework is introduced to provide a reliable and secure authentication mechanism based on authentication features. The proposed framework evaluates and selects the most appropriate authentication scheme/method based on evaluating authentication features using a hybrid multicriteria decision-making approach. It completes this in two steps: in the first step, the analytic hierarchy process (AHP) method is applied for assigning criteria weights; and in the second step, the technique for order preference by similarity to ideal solution (TOPSIS) approach selects the best authentication solution for IoHT devices based upon identified authentication features. This is the first attempt to present a features-based authentication model for selecting the improved authentication solution employed in IoHT devices.

Keywords: authentication; IoMT; security features; AHP; TOPSIS; MCDM

MSC: 94A62

Citation: Khan, H.U.; Ali, Y.; Khan, F. A Features-Based Privacy Preserving Assessment Model for Authentication of Internet of Medical Things (IoMT) Devices in Healthcare. *Mathematics* **2023**, *11*, 1197. https://doi.org/10.3390/math11051197

Academic Editor: Fuyuan Xiao

Received: 4 February 2023
Revised: 23 February 2023
Accepted: 24 February 2023
Published: 28 February 2023

1. Introduction

The terms IoHT and IoMT are often used interchangeably, these concepts describe a collection of medical devices connected with each other through a network to provide access to healthcare personnel and data related to patients. IoT has provided significant changes not only in the healthcare sector, but the number of IoT sensors, devices, and equipment is exponentially increasing due to their suitability and adaptability in other domains. It is predicted that this number will be between 50 and 100 billion by 2020 [1]. However, IoT devices have brought many challenges related to security in different fields, but these challenges become noteworthy in the healthcare area, where sensitive data is collected and processed by IoT sensors and equipment. Security and privacy concerns may

arise as these devices are attributed to constrained resources and low processing abilities [2]. These features make them susceptible to many cyberattacks, such as spoofing, denial of service (DoS), man-in-middle, replay attacks, eavesdropping, phishing, privacy breaches, etc. [3,4]. There are security challenges that IoT devices need to address since they can operate in an ad-hoc network [5–7], wireless network [8–10], and the Internet of Things in a healthcare setting [11,12], where sensitive data is transmitted and collected by a terminal node [13]. Keeping the privacy and security of IoT devices in mind, strong authentication schemes are indispensable for dealing with emerging security problems. Authentication is a mechanism for verifying the identity of an entity against the stored credential in a database or authentication server [14]. The authentication schemes in the IoT are always the main security concern due to the machine-to-machine interactions and number of devices [15]. Authentication provides preventive measures against certain types of attacks and confirms the validity of messages [16]. The authentication of IoHT devices has to be performed efficiently by considering factors such as power consumption, processing abilities, and storage options [17]. The authentication mechanism employed for the IoT is implemented based on different factors, such as biometrics, mobile devices, smart cards, fingerprints, and passwords [18]. These factors are the most important considerations before deploying an authentication model for IoT devices in a healthcare setting.

In the last decade, many authentication schemes have been presented to overcome the security issues in the healthcare domain. Consequently, it has become a challenging job to compare the existing authentication methods based on their security performance. Similarly, the vast number of vendors, the complexity of authentication methods, and the number and type of features supported by the authentication methods are also a major concern for healthcare professionals and network engineers. Furthermore, in a healthcare environment, technical personnel fail to evaluate and test the existing authentication solutions against a proper benchmark. Therefore, a features-based evaluation framework is introduced to evaluate the authentication schemes against the proposed criteria that consist of the most important features related to authentication. The features related to authentication are selected based on the extensive literature study, and the most essential features are taken into account. A case study is conducted with an expert panel to design a benchmark/criterion that can be applied as an evaluation benchmark for authentication schemes. A full-pledged criterion is built with input from the expert group in the field of network security. After finalizing the criteria, AHP and TOPSIS multi-criteria decision-making (MCDM) methods have been applied to assess and rank the authentication methods/algorithms against the criteria's features.

1.1. Contribution

The following are the points of contribution to this research work.

- According to our literature study, it has been observed that various assessment methodologies have been proposed to address the security aspects of healthcare systems, but we did not find any significant study that focuses on evaluating the authentication aspects of security. Although, existing evaluation models in the healthcare area targeted security evaluation of electronic medical records (EMR) and electronic health records (HER).
- This is the first attempt to solve authentication issues with IoT devices in the healthcare sector by presenting an assessment framework for authentication using a hybrid MCDM approach. The supposed framework leverages the most advanced evaluation techniques, such as AHP and TOPSIS, for decision-making and installing authentication methods in the healthcare area.
- Similarly, it has also been noticed that the existing criteria are designed without significant literature study and feature analysis. The existing evaluation models or frameworks do not focus on sufficient features related to authentication. The authentication features are identified and collected from authentic sources of literature. A detailed and in-depth search has been carried out to select and scrutinize all papers

for the identification of features. Therefore, a research gap exists and is addressed by this proposed work, which provides a robust and efficient solution to the selection problem of the best authentication scheme employed in IoHT devices.

- A survey-based case study is conducted to check the robustness and validity of features with an expert panel. A systematic and well-organized methodology is followed in the overall evaluation of the proposed framework. The proposed model is tested by experts, and it is recommended for the evaluation of authentication in the healthcare area.

1.2. Motivation

The main motivations to pursue this research are mentioned below.

- The security of IoHT devices has been a hot research topic in the last few years. Therefore, a lot of evaluation models have been presented to cope with the security concerns in the healthcare area, however, the authentication of IoT devices is found to be missing in the literature.
- IoHT devices in the healthcare sector are susceptible to more security attacks, so it is more important to check their authenticity before making them part of the healthcare network infrastructure. Access control and identity management are imperatives, as any intruder will compromise the security of the entire network. An assessment framework is required to check the degree of authenticity of IoMT devices.
- A lot of authentication models have been proposed over the last few years with varying features. It is not possible to directly compare these authentication mechanisms with each other. There is a need for an evaluation model where the existing authentication schemes can be assessed and improved in terms of features due to the type of data managed by the healthcare sector.

This paper is split into four (4) sections. Section 2 discusses related work, Section 3 discusses the overall procedure of the proposed methodology and Section 4 discusses the conclusion of this research study.

2. Related Work

Security assessment of IoT devices and sensors deployed in healthcare has been the most intriguing area of research in the last few years. In this respect, different evaluation models have been proposed to deal with security concerns and challenges. These models adopted different evaluation approaches for evaluating the security of IoHT devices, but the authentication aspect is never addressed in the existing literature. The complete list of related works for the proposed work is given below as:

Haghparast et al. [19]'s evaluation model adopted a fuzzy analytic network process (ANP) for security evaluation in the healthcare area. This work addresses the layer-based security of IoHT devices. Al-Zahrani et al. [20] conducted a unified approach by leveraging ANP and TOPSIS with the support of fuzzy logic for the evaluation of healthcare technologies based on four evaluation metrics, such as confidentiality, integrity, availability, and satisfaction. A study put forward by Zarour et al. [21] focused on the assessment of blockchain technology models for preserving the security of electronic health records. They evaluated selected alternatives against six (6) parameters, such as data monitoring, immutability, consensus, value, identity, and data security. Another similar research study was also conducted by Enaizan et al. [22] to design a decision-support system for the security and privacy of electronic medical records (EMR). They adopted AHP-TOPSIS methods along with the K-mean clustering technique to identify the most critical factors, such as authentication, availability, nonrepudiation, integrity, and illegal access. Huang et al. [23] evaluated IoMT-based systems by using the ANP method and considering features from the most popular security standard, such as ISO/IEC 27002 (ISO 27002). The main elements of the evaluation criteria of IoMT systems are: secure key, confidentiality, availability, safety, network monitoring, continuity, authentication, nonrepudiation, trustworthiness, auditing, and secure key management. The study of Hussain Seh1 et al. [24] is aimed at introducing

an effective and efficient assessment framework for evaluating web-based healthcare applications. They utilized AHP and TOPSIS approaches for the evaluation and ranking of alternatives against features, such as authentication, encryption, robustness, revocation of access, data validation, and audit. This study is similar to the computational methodology that is suggested by Ahmad et al. [25] for the empirical analysis of selecting the most ideal security technique for medical care devices. This study applied AHP, hesitant fuzzy, and AHP to evaluate alternatives for criteria features, such as biometric authentication, passwords, backup, access control, software recovery, security tokens, version control, and error detection. Algarni et al. [26] checked the level of security of web-based medical image processing systems by using fuzzy AHP and TOPSIS. The major parameters in their design criteria were authentication, confidentiality, utility, integrity, authorization, resilience, and procession. They evaluated the various aspects of MRI devices, such as X-ray, ultrasound, and CT scan devices. Ansari et al. [27] proposed a quantification framework for the evaluation and selection of the right security requirement engineering (SRE) technology in the medical care system. The major elements of the evaluation criteria are composed of security, threats, risks, assessment, vulnerability, stakeholders, and security requirements. The work suggested by Kumar et al. [28] also utilized AHP-TOPSIS techniques for evaluating factors that affect healthcare information security. Healthcare information security is tested against factors such as human error, malware, social engineering, outdated information technology, med jacking, and low access control management.

3. Proposed Methodology

In wireless sensors or IoT networks, the authentication of nodes or IoT devices brings significant importance from different security perspectives. It is only possible to attain full-fledged security by selecting the most appropriate and full-pledged security scheme or algorithm for authentication. In the last few years, an array of authentication methods has been presented to address the security concerns of IoT devices deployed in the healthcare area. This proliferation has resulted in decision-making issues regarding the installation of the most suitable choice of authentication scheme. Therefore, the major objective of this research approach is to assess and opt for the best algorithm/scheme for IoT devices. Initially, features related to authentication were identified from literature sources and presented at a consultation with experts on a panel. Authentication features were used as metrics for the selection of the best authentication algorithm in the medical care system. This evaluation framework consists of two major phases, as shown in Figure 1. In the first phase, the AHP method was applied to assign criteria scores, and in the second phase, the TOPSIS method was applied to assess and rank the authentication methods with respect to criteria features. The chosen features in this research are the most commonly used and most relevant to the strength of any authentication scheme or algorithm. The complete list of procedures for the proposed research method is given below.

3.1. Collection and Selection of Authentication Features

The feature selection procedure was carried out by completely searching the literature. The criteria were designed based on assessment features. Features were included after consulting with the expert panel, and they provided valuable input in finalizing the list of features. The list of features selected in this study include the criteria for mutual authentication, privacy protection, key agreement, password change, integrity, confidentiality, forward security, scalability, and availability. This research work follows a systematic approach to the collection of features. The following authentication features are collected from literature sources, and the details are given in Table 1.

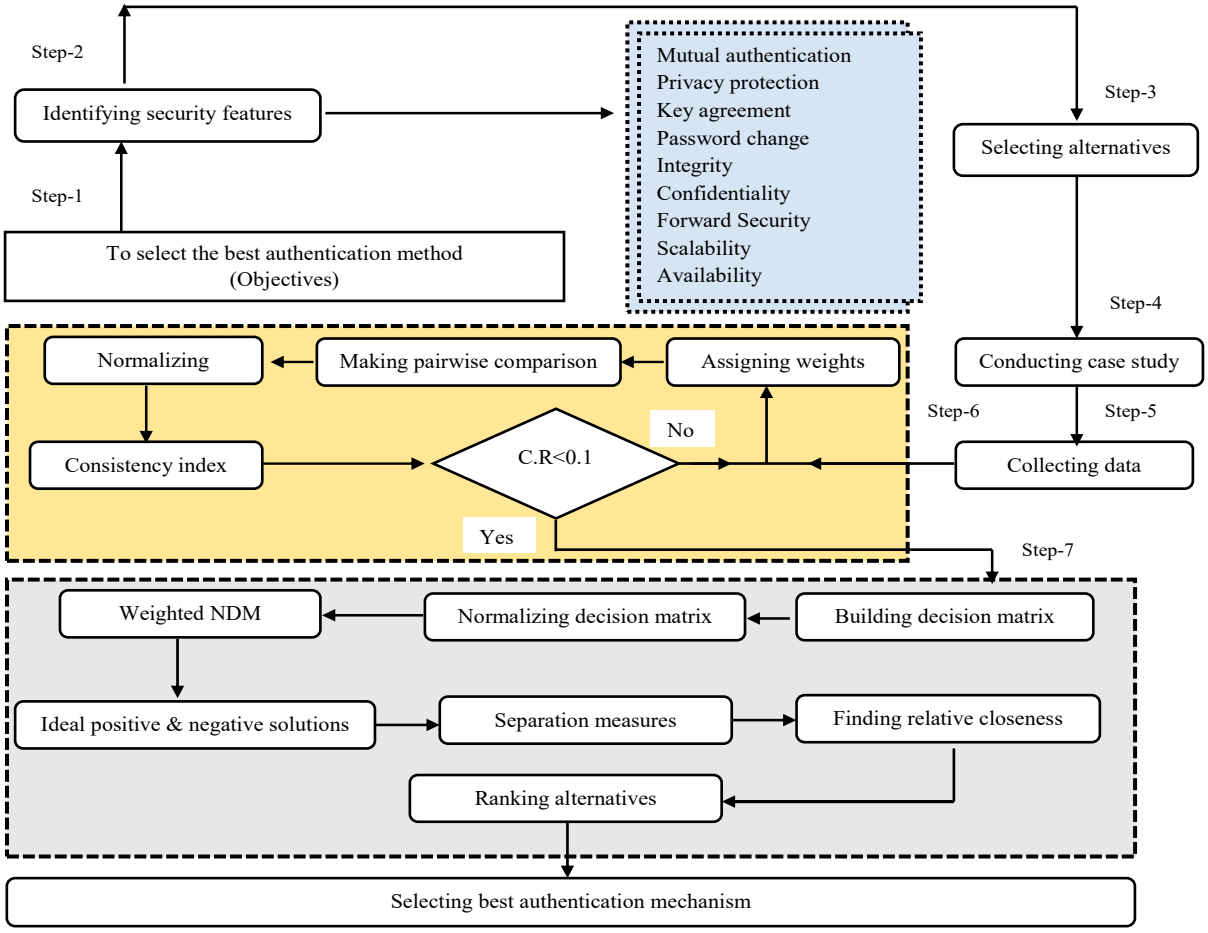

Figure 1. Authentication evaluation framework structure.

Table 1. Features Literature.

Criteria Features	References
Mutual Authentication	[29–41]
Privacy Protection	[29,37,38,42–44]
Key agreement	[31,39–41,44,45]
Password Change	[36,39,40,46]
Integrity	[37,39,40,44,47–50]
Confidentiality	[30,32,37,42,44,45,47–51]
Forward Security	[41,45,46,49]
Scalability	[39,45,50,52]
Availability	[38,41,42,45,47]

We selected the most vital features that have an overall impact on authentication from the literature. The importance of selected features can be estimated from the number of citations, i.e., references used by different authors for evaluation. The frequency of individual authentication features cited in the literature is given in Figure 2.

The hierarchical structure of features and authentication devices is given in Figure 3.

3.2. Case Study

A case study is conducted with ten (10) experts who are working as expert network security analysts. The major purpose of consultation with experts is to understand the level of importance of each feature in the evaluation approach. In this method, a questionnaire was given to experts in the field of network/IoT security. A few questions were asked about the authentication features of IoT devices. They rated the importance of features

for any authentication mechanism by using their expert opinions. Criteria are built by considering the most vital feature. The experts responded by using the well-known Saaty's scale. The answers were provided on a different sheet of paper. After collecting data, the average of the values assigned by each expert is calculated for individual features. The complete procedure of steps of this case study is depicted in Figure 4. In the first step, the authentication issues were investigated based on the literature study, and then a survey was conducted with security experts who know about the significance of features in the authentication method.

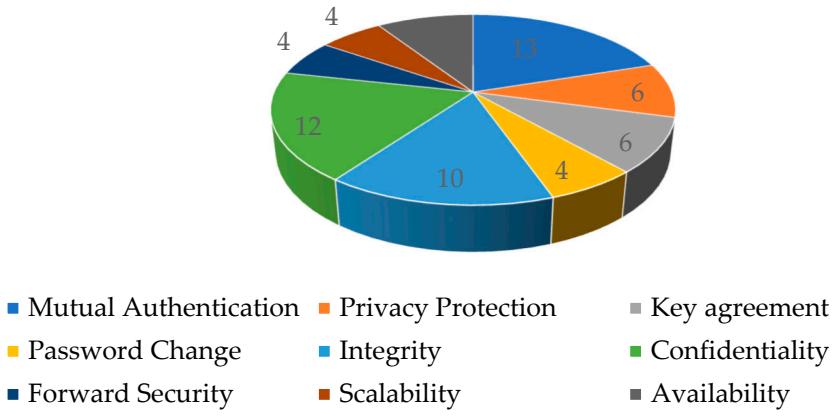

Figure 2. Authentication features frequency of occurrence.

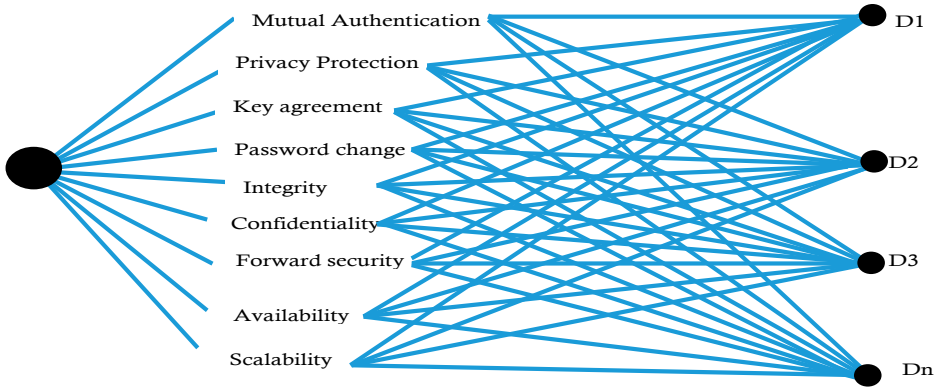

Figure 3. Hierarchical structure of authentication mechanisms and features.

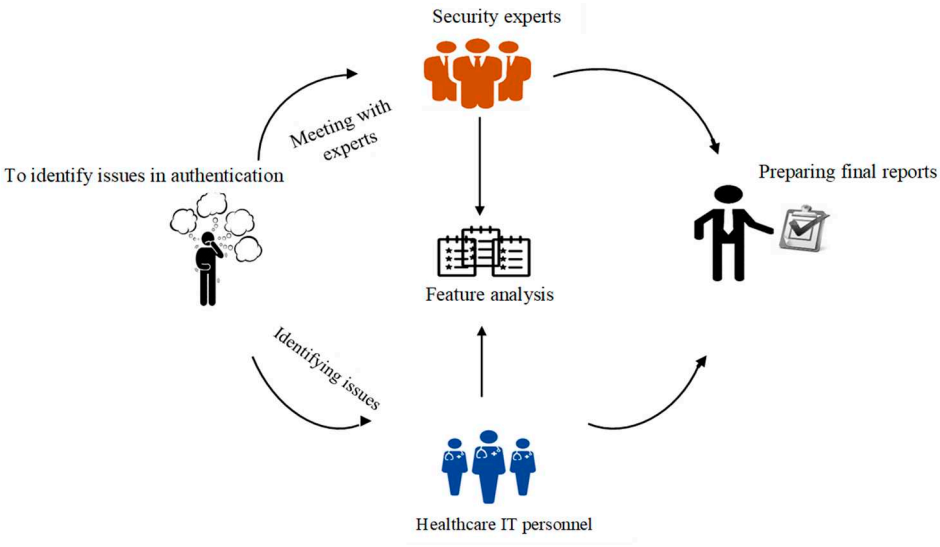

Figure 4. Case study scenario.

3.3. Assigning Criteria Weights

It is important to assign weights to the criteria's features. In this regard, a well-known MCDM approach such as AHP was adopted to assign criteria weights. This method is the most suitable choice for assigning weights to the criteria in MCDM problem scenarios. There are several reasons behind the application of this method. First, it focuses on eliminating the cognitive errors through the simplification procedure, multi-attribute comparison, and partitioning. This approach has the potential to compare both qualitative and quantitative attributes, simultaneously. Hence, it covers different decision-making situations, such as evaluation, prioritization selection, conflict resolution, resource allocation, and optimization. Furthermore, this method is subjective, which means it can be used to assign criteria weights based on opinions provided by the expert panel or decision makers [53]. The AHP approach prioritized the selected alternatives by using the concept of goal identification and the significance of hierarchy [54]. The AHP method applies the following steps [55–57].

Step-1. Assigning weights

The AHP method starts its step-wise procedure while assigning weightage scores to criteria by using the concept of relative importance. In this process, the relative importance of each criterion over another criterion is defined according to a predefined scale. Then, the qualitative values are shifted into a quantitative form.

Step-2. Comparison matrix

A pairwise comparison table/matrix is similar to an input to the AHP method. In this step, a scale normally ranges from 1 to 9. It assigns values to the criteria features based on a comparison matrix, such as $a_{ij,}$ and denotes the relative importance of the ith criteria over the jth criteria. In this step, if a_{ij} is assigned a value greater than one, then the ith criterion is more important than the jth criterion. Additionally, in the case that the a_{ij} value is less than one, then the ith criterion is considered comparatively less important. In situations where $a_{ij} = 1$, then both criteria elements are considered to have equal significance. The results of this procedure can be obtained by using the following matrix (P_m), as given by Equation (1).

$$P_m = \begin{bmatrix} 1 & a_{12} \ldots\ldots & a_{1n} \\ \frac{1}{a_{12}} & 1 \ldots\ldots & a_{2n} \\ \vdots & \vdots & \vdots \\ \frac{1}{a_{1n}} & \frac{1}{a_{2n}} & 1 \end{bmatrix} \quad (1)$$

Step-3. Normalizing pairwise comparison matrix

During the normalization procedure, the total of columns in the matrix is obtained then every element of the matrix is divided by the total, and then the average of the rows is obtained. This normalization process led to the production of the criteria weights. This process can be accomplished by two methods, such as the geometric mean and Lambda max. λmax actually denotes the eigenvalues. It is obtained by using the following equation:

$$\lambda_{max} = \frac{1}{n} \sum_{i=1}^{n} \frac{(Aw)_i}{w_i} \quad (2)$$

Step-4. Creating consistency matrix

The major purpose of the consistency matrix is to check the results comparison for consistency. In this procedure, initially the consistency index was equated with the help of Equation (3). Then, the consistency ratio was obtained using Equation (4).

$$C.I = \frac{\lambda_{max} - n}{n - 1} \quad (3)$$

$$C.R = \frac{C.I}{R.I} \tag{4}$$

The score value of the consistency ratio (C.R) is very important, for example, when C.R = 0.1 OR C.R < 0.1, then it is within the acceptable range, otherwise, the process will be restarted.

In context of this research, AHP is applied to assign weights to the criteria features. The procedure of assigning the weights criteria begins right after the identification of the alternatives, criteria, and sub-criteria. The criteria have been already defined by collecting the authentication features from different sources of literature. In the proposed methodology, we have identified nine (9) authentication features. According to our literature study, these are the most frequently used and recognized features for authentication for IoT devices in healthcare networks. After defining the criteria, the experts in the field of IoT security assigned weights to the criteria. Weights to criteria were assigned by the expert panel using Saaty's scale. For simplicity, the calculation of different codes was assigned to criteria, such as mutual authentication, privacy protection, key agreement, password change, integrity, confidentiality, forward security, scalability, and availability, such as C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8, and C_9, respectively. A pairwise comparison matrix was built by using Equation (1), and the details are given in the pairwise matrix.

$$P_m = \begin{bmatrix} & C_1 & C_2 & C_3 & C_4 & C_5 & C_6 & C_7 & C_8 & C_9 \\ C_1 & 1 & 2 & 1 & 1 & 1 & 5 & 2 & 5 & 3 \\ C_2 & \frac{1}{2} & 1 & 1 & 1 & 2 & 3 & 4 & 7 & 4 \\ C_3 & 1 & 1 & 1 & 2 & 3 & 3 & 3 & 7 & 2 \\ C_4 & 1 & 1 & \frac{1}{2} & 1 & 3 & 2 & 3 & 5 & 4 \\ C_5 & 1 & \frac{1}{2} & \frac{1}{3} & \frac{1}{3} & 1 & 3 & 5 & 4 & 3 \\ C_6 & \frac{1}{5} & \frac{1}{3} & \frac{1}{3} & \frac{1}{2} & \frac{1}{3} & 1 & 2 & 3 & 2 \\ C_7 & \frac{1}{2} & \frac{1}{4} & \frac{1}{3} & \frac{1}{3} & \frac{1}{5} & \frac{1}{2} & 1 & 2 & 3 \\ C_8 & \frac{1}{5} & \frac{1}{7} & \frac{1}{7} & \frac{1}{5} & \frac{1}{4} & \frac{1}{3} & \frac{1}{2} & 1 & 2 \\ C_9 & \frac{1}{3} & \frac{1}{4} & \frac{1}{2} & \frac{1}{4} & \frac{1}{3} & \frac{1}{2} & \frac{1}{3} & \frac{1}{2} & 1 \end{bmatrix}$$

The sum of the columns is calculated, and individual elements in the table are divided by the sum of the columns. This process is repeated for all individual elements. The details of the normalized pairwise matrix are shown in Table 2.

Table 2. Normalized pairwise matrix.

Features	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9
C_1	0.14	0.31	0.19	0.15	0.09	0.27	0.05	0.14	0.13
C_2	0.07	0.15	0.19	0.15	0.18	0.16	0.20	0.20	0.17
C_3	0.14	0.15	0.19	0.30	0.27	0.16	0.15	0.20	0.08
C_4	0.14	0.15	0.10	0.15	0.27	0.11	0.15	0.14	0.17
C_5	0.14	0.08	0.06	0.05	0.09	0.16	0.25	0.12	0.13
C_6	0.14	0.05	0.06	0.08	0.03	0.05	0.10	0.09	0.08
C_7	0.14	0.04	0.06	0.05	0.02	0.03	0.05	0.06	0.13
C_8	0.03	0.02	0.03	0.03	0.02	0.02	0.03	0.03	0.08
C_9	0.05	0.04	0.10	0.04	0.03	0.03	0.02	0.01	0.04

The weights of the criteria elements are calculated from Table 2 by using Equation (2). The results obtained for each criterion are displayed in Table 3.

Table 3. Weights of features.

Codes	Features	Criteria Weights
C_1	Mutual Authentication	0.16
C_2	Privacy Protection	0.17
C_3	Key agreement	0.18
C_4	Password Change	0.15
C_5	Integrity	0.12
C_6	Confidentiality	0.08
C_7	Forward Security	0.06
C_8	Scalability	0.03
C_9	Availability	0.04

Consistency matrix is formed by applying Equation (3). The results of the consistency matrix are shown in Table 4.

Table 4. Consistency matrix.

C.F	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9
C_1	0.16	0.33	0.18	0.15	0.12	0.38	0.06	0.16	0.12
C_2	0.08	0.17	0.18	0.15	0.24	0.23	0.26	0.22	0.16
C_3	0.16	0.17	0.18	0.31	0.36	0.23	0.19	0.22	0.08
C_4	0.16	0.17	0.09	0.15	0.36	0.15	0.19	0.16	0.16
C_5	0.16	0.08	0.06	0.05	0.12	0.19	0.32	0.13	0.12
C_6	0.16	0.06	0.06	0.08	0.04	0.03	0.13	0.10	0.08
C_7	0.16	0.04	0.06	0.05	0.02	0.02	0.06	0.06	0.12
C_8	0.03	0.02	0.03	0.03	0.03	0.01	0.03	0.03	0.08
C_9	0.05	0.04	0.09	0.04	0.04	0.02	0.02	0.02	0.04

After calculating the criteria weights of individual elements, it is necessary to check the procedure of finding the weights of the criteria. For this purpose, the procedure was extended to find the consistency index and was calculated to check how consistent the results were. The random index (R.I) for the "N" number of criteria is given in Table 5 [58]. In this study, as we have selected nine (9) security features, the value of R.I is 1.45, as shown in Table 5.

Table 5. R.I values.

No. of Criteria	1	2	3	4	5	6	7	8	9	10	11	12	13
R.I value	0	0	0.52	0.89	1.11	1.25	1.35	1.4	1.45	1.49	1.52	1.54	1.56

Lambda max (λmax) finds the eigenvalue. First lambda max is calculated and then C.I is found with the help of Equation (3). Both are given below.

$$\lambda_{\max} = 9.9$$

Consistency index is computed as given below.

$$\text{C.I} = \frac{9.9 - 9}{9 - 1} = 0.11$$

Equation (4) has been used to obtain the C.R value.

$$\text{C.R} = \frac{0.11}{1.45} = 0.077 < 0.1 \text{ or } (7.7\% < 10\%)$$

Here, C.R. is less than 0.077 or 7.7%. This means that the results of this procedure are accurate and good enough to carry on with further security evaluation steps.

3.4. Ranking Alternatives

Initially, the TOPSIS method was presented by Hwang and Yoon [59]. It works on the principle of using ideal solutions. It is a simple working mechanism, reliable and well-established [51]. In this approach, whenever the chosen alternative is required to be at the shortest distance from the positive ideal solution and it should be located at the farthest distance from the negative ideal solution. The TOPSIS method is intended to be applied for the assessment and ranking of authentication mechanisms based upon an identified set of features. It involves following steps for the ranking of alternatives [59,60].

Step-1 Constructing decision matrix

A decision matrix, denoted (D_m), is constructed with the help of alternatives and criteria. For "n" numbers of alternatives denoted by A_1, A_2 … An and criteria denoted by C_1, C_2 … C_n, the decision matrix is given as:

$$D_m = \begin{array}{c} \\ A_1 \\ \vdots \\ A^n \end{array} \begin{bmatrix} C_1 & \ldots\ldots\ldots\ldots & C_n \\ X_{11} & \ldots\ldots\ldots & X_{1n} \\ & & \\ \vdots & \ddots & \vdots \\ X_{m1} & \ldots\ldots\ldots\ldots & X_{mn} \end{bmatrix} \quad (5)$$

Step-2 Normalizing decision matrix

As a decision matrix collects data from heterogeneous/different sources, it is mandatory to convert data into a dimensionless form. Therefore, a normalized decision matrix denoted by R_{IJ} can be given as:

$$R_{ij} = \frac{X_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}} \quad (6)$$

In Equation (6), the value of i = 1 … … .m, and while, j = 1 … n

Step-3. Weighted normalized decision matrix (WNDM)

The attributes may vary with respect to their importance; therefore, every value of the normalized decision matrix is multiplied with a random score value by using the following equation to obtain a weighted normalized decision matrix (V) as given below:

$$V = W_j \times R_{ij} \ (7) \quad (7)$$

$$V = \begin{bmatrix} V_{11} & V_{12} & V_{1j} & V_{1n} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ V_{i1} & V_{i2} & V_{ij} & V_{in} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ V_{m1} & V_{m2} & V_{mj} & V_{mn} \end{bmatrix} = \begin{bmatrix} w_1r_{11} & w_1r_{11} & w_1r_{11} & w_1r_{11} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ w_1r_{11} & w_1r_{11} & w_1r_{11} & w_1r_{11} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ w_1r_{11} & w_1r_{11} & w_1r_{11} & w_1r_{11} \end{bmatrix}$$

Step-4. Ideal points Calculation

Positive ideal solution denoted by A^+ and negative ideal solution expressed by A^- are computed by using the following equations:

$$A^+ = \{V_1^+, V_2^+, V_3^+ \ldots V_n\}, \text{ Where } V_j^+ = \{((\text{maxi}(V_{ij}) \text{if } j \in J); (\text{mini } V_{ij} \text{ if } j \in J')\} \quad (8)$$

$$A^- = \{V_1^-, V_2^-, V_3^- .. V_n^-\}, \text{ Where } V_j^- = \{(\text{mini}(V_{ij}) \text{if } j \in J); (\text{maxi } V_{ij} \text{ if } j \in J')\} \quad (9)$$

where, J represents beneficial features whereas, J′ is showing nonbeneficial criteria features. Beneficial criteria and nonbeneficial criteria identification is the most important part of the MCDM method. Beneficial criteria are normally those attributes for which high values are desirable, while, on other hand, nonbeneficial criteria are those for which less value is desirable.

Step-5. Finding separation measures

Separation measures, i.e., ideal separation and no-ideal separation measures, are computed by using the following two equations:

$$S^{+} = \sqrt{\sum_{J=1}^{n} \left(V_{ij} - V^{+}\right)^{2}} \text{ where } i = 1 \ldots ... \, m \tag{10}$$

$$S^{-} = \sqrt{\sum_{J=1}^{n} \left(V_{ij} - V^{-}\right)^{2}} \text{ where } i = 1 \ldots ... \, m \tag{11}$$

Step-6. Measuring relative closeness

The relative closeness denoted by C_i is measured for each alternative with respect to the ideal solutions by using the following equation:

$$C_i = \frac{S_i^{-}}{\left(S_i^{+} + S_i^{-}\right)} \text{ When } 0 \leq C_i \leq 1 \tag{12}$$

Step-7. Ranking of alternatives

The ranking of alternatives is based on their C_i values, such that the higher values possessed by the alternative are considered the best preference, while a low value of C_i comparatively shows less performance value.

- The TOPSIS method uses the concept of an ideal solution. It means that if a specific alternative is located at the shortest distance from the positive ideal solution, and if it is located at the maximum distance from the negative ideal solution, then it is considered the best option among the alternatives. The TOPSIS method is more reliable and well-established in its working procedure.
- It has the characteristic of presenting efficiency in the computation process, and results are presented in a simple mathematical form. It is more flexible, and it has various applications in theoretical and real-world MCDM problems.

The purpose of the TOPSIS method is to prioritize alternatives with respect to the identified security features of authentication. The security experts were consulted to know the importance of each feature of the criteria for the authentication solution as discussed in the previous case study. They provided their response according to a ten (10)-point scale. The responses collected from the ten (10)-point scale by the expert panel were divided among ten (10) different authentication alternative solutions. They were assigned values based on a scale starting from 1 to 10. The complete input provided by the expert panel against the authentication criteria is given in the following matrix:

$$D_m = \begin{bmatrix} & C_1 & C_2 & C_3 & C_4 & C_5 & C_6 & C_7 & C_8 & C_9 \\ A_1 & 7 & 9 & 9 & 8 & 6 & 7 & 4 & 6 & 8 \\ A_2 & 8 & 7 & 8 & 7 & 7 & 5 & 4 & 5 & 8 \\ A_3 & 9 & 6 & 9 & 8 & 8 & 6 & 3 & 6 & 7 \\ A_4 & 8 & 7 & 8 & 6 & 9 & 6 & 5 & 3 & 9 \\ A_5 & 6 & 7 & 6 & 7 & 8 & 5 & 6 & 5 & 7 \\ A_6 & 7 & 5 & 6 & 8 & 6 & 7 & 4 & 8 & 9 \\ A_7 & 6 & 7 & 4 & 8 & 7 & 8 & 5 & 5 & 8 \\ A_8 & 5 & 8 & 7 & 4 & 8 & 5 & 7 & 7 & 5 \\ A_9 & 6 & 6 & 5 & 8 & 9 & 8 & 5 & 4 & 7 \\ A_{10} & 6 & 5 & 7 & 4 & 6 & 7 & 4 & 4 & 8 \end{bmatrix}$$

The decision matrix is computed with the help of Equation (6), and the results are listed and given in Table 6. In the last row, the criteria weights that were previously obtained by using AHP are also listed.

Table 6. Normalized decision matrix.

Alternatives	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9
A_1	0.32	0.42	0.40	0.36	0.25	0.34	0.26	0.35	0.33
A_2	0.37	0.48	0.47	0.48	0.46	0.41	0.49	0.49	0.50
A_3	0.41	0.28	0.40	0.36	0.34	0.29	0.20	0.35	0.29
A_4	0.37	0.33	0.36	0.27	0.38	0.29	0.33	0.17	0.37
A_5	0.28	0.33	0.27	0.32	0.34	0.24	0.39	0.29	0.29
A_6	0.32	0.23	0.27	0.36	0.25	0.34	0.26	0.46	0.37
A_7	0.28	0.23	0.27	0.36	0.25	0.34	0.26	0.46	0.37
A_8	0.23	0.33	0.18	0.36	0.30	0.39	0.33	0.29	0.33
A_9	0.28	0.37	0.31	0.18	0.34	0.24	0.46	0.40	0.21
A_{10}	0.28	0.28	0.22	0.36	0.38	0.39	0.33	0.23	0.29
C.W	**0.16**	**0.17**	**0.18**	**0.15**	**0.12**	**0.08**	**0.06**	**0.03**	**0.04**

It is not always the case that every criteria element will be of equal importance, therefore, WNDM is created. To obtain a weighted normalized matrix, we used Equation (7). Normalized data is given in Table 7.

Table 7. Weighted normalized data.

Alternatives	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9
A_1	0.051	0.071	0.072	0.054	0.030	0.027	0.016	0.010	0.013
A_2	0.059	0.081	0.085	0.072	0.055	0.033	0.030	0.015	0.020
A_3	0.066	0.047	0.072	0.054	0.041	0.023	0.012	0.010	0.012
A_4	0.059	0.055	0.064	0.041	0.046	0.023	0.020	0.005	0.015
A_5	0.044	0.055	0.048	0.048	0.041	0.019	0.024	0.009	0.012
A_6	0.051	0.040	0.048	0.054	0.030	0.027	0.016	0.014	0.015
A_7	0.044	0.040	0.048	0.054	0.030	0.027	0.016	0.014	0.015
A_8	0.037	0.055	0.032	0.054	0.035	0.031	0.020	0.009	0.013
A_9	0.044	0.063	0.056	0.027	0.041	0.019	0.028	0.012	0.008
A_{10}	0.044	0.047	0.040	0.054	0.046	0.031	0.020	0.007	0.012

The next step is to find A^+ and A^- for every criteria feature. Equations (8) and (9) have been applied and the results are given in Table 8.

Table 8. Values of A^+ and A^- of criteria elements.

	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_1
A^+	0.081	0.071	0.072	0.063	0.068	0.040	0.041	0.033	0.038	0.022
A^-	0.063	0.047	0.064	0.047	0.045	0.029	0.025	0.017	0.029	0.015

Both ideal separation measures and relative closeness are measured with the help of Equations (10), (11), and (12), respectively and their values are given in Table 9.

Table 9. Relative Closeness.

Alternative	S^+	$S^=$	S^++S^-	Relative Closeness
A_1	0.041	0.061	0.102	0.597
A_2	0.007	0.091	0.099	0.926
A_3	0.048	0.059	0.107	0.549
A_4	0.048	0.048	0.096	0.500
A_5	0.060	0.035	0.095	0.370
A_6	0.067	0.038	0.104	0.360
A_7	0.069	0.035	0.104	0.340
A_8	0.072	0.035	0.107	0.330
A_9	0.064	0.040	0.104	0.382
A_{10}	0.065	0.037	0.102	0.362

Ranking is performed according to the values of relative closeness as given in Table 10. As we can see, among all the alternatives, "A_2" has the highest value. This alternative is the best with respect to the criteria.

Table 10. Ranking preferences.

Alternatives	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
Final score	0.597	0.926	0.549	0.500	0.370	0.360	0.340	0.330	0.382	0.362
Ranking	2	1	3	4	5	8	9	10	6	7

From the empirical assessment of this study, it is concluded that the A_2 alternative has higher values among the other selected alternatives. It means that by taking features into account based on our assessment model of authentication, it is more reliable in terms of the authentication features. Thus, any algorithm having such a feature should be adopted for secure authentication in the healthcare sector. The complete details of the ranking scores of all authentication alternatives are given in Figure 5.

The complete input data provided to the D2 alternative against the criteria features is given in Figure 6. It shows that it can be a better choice of authentication method based on the degree of importance of features. The authentication scheme can be judged based on features, such as mutual authentication, privacy protection, key agreement, password change, integrity, confidentiality, forward security, scalability, and availability.

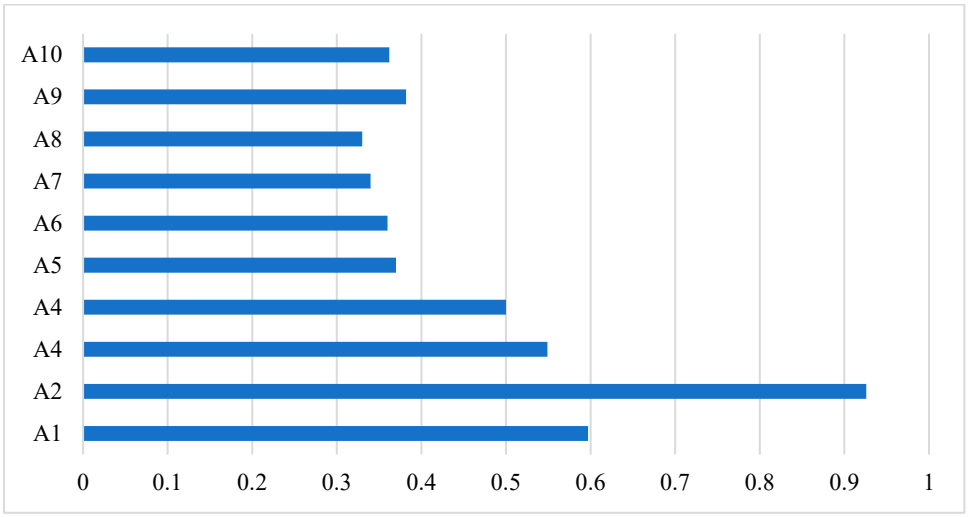

Figure 5. Performance evaluation of authentication alternatives.

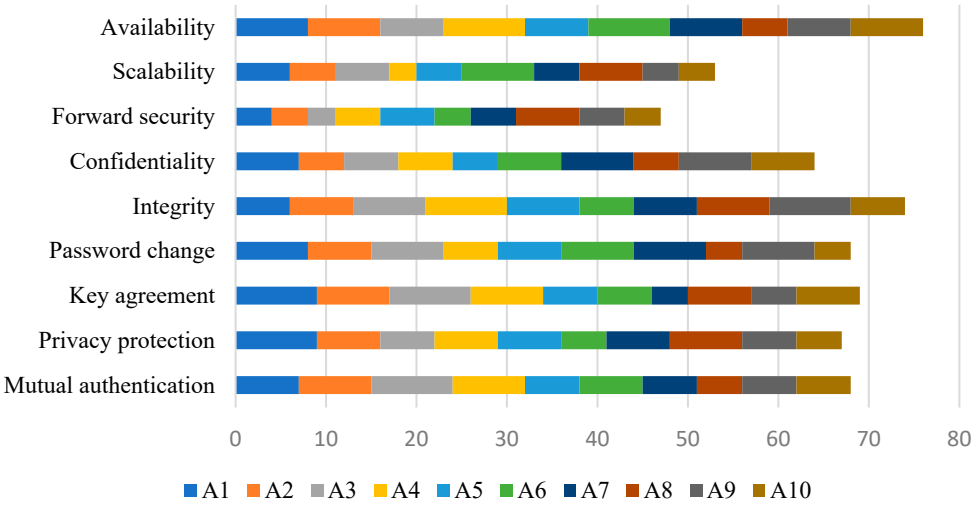

Figure 6. Input given to criteria features for alternatives.

4. Conclusions

The secure protection of IoMT devices in the healthcare domain remains a major concern due to the nature of the devices and data managed by the network. Therefore, it has become an important topic over the last couple of years for researchers and practitioners to provide reasonable security solutions in this area. A plethora of IoT authentication solutions have been introduced to the market for secure authentication of IoMT devices in the healthcare field. This significant intensification of IoT devices has led to decision-making and selection problems for healthcare personnel trying to install the right security solution. In this research study, we present an assessment framework to provide reasonable solutions for the selection and deployment of the right authentication solution. This framework adopts a mathematical approach for decision-making and implements the best authentication solution based on considering the most important features. A case study was conducted with an expert panel to collect data about the authentication features and set criteria for the evaluation of authentication schemes. This framework is composed of two multicriteria decision-making approaches, i.e., AHP and TOPSIS. The AHP technique assigns quantification scores to criteria features; and TOPSIS performs the performance evaluation of the authentication alternatives against the proposed criteria.

The findings of the proposed study suggest that this framework can be used as the best choice for the assessment and ranking of IoT authentication algorithms/schemes in a

real-world scenario in the healthcare area. This framework can be applied as a guideline for practitioners and researchers to evaluate the existing authentication methods based on the selected feature. The research will assist security developers and policymakers in reviewing the existing authentication schemes with respect to security features by applying the proposed model to the evaluation.

There are some limitations to this study, such as the fact that the features used in this criterion are not absolute metrics for the evaluation of authentication algorithms. Other studies might consider other features for the criteria. The decision-making process can be further improved by using fuzzy concepts. Therefore, we are looking forward to applying the fuzzy approach for the purpose of evaluating authentication algorithms and bringing more accuracy and efficiency to the results.

Author Contributions: Conceptualization, H.U.K., Y.A. and F.K.; methodology, H.U.K., Y.A. and F.K.; software, H.U.K., Y.A. and F.K.; validation, H.U.K., Y.A. and F.K.; formal analysis, H.U.K., Y.A. and F.K.; investigation, H.U.K., Y.A. and F.K.; resources, H.U.K., Y.A. and F.K.; data curation, H.U.K., Y.A. and F.K.; writing—original draft preparation, H.U.K., Y.A. and F.K.; writing—review and editing, H.U.K., Y.A., and F.K.; visualization, H.U.K., Y.A. and F.K.; supervision, H.U.K., Y.A. and F.K.; project administration, H.U.K., Y.A. and F.K.; funding acquisition H.U.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Qatar National Library, Doha, Qatar and Qatar University internal grant IRCC-2021-010.

Data Availability Statement: All the collected data in this study are displayed in figures and tables.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Sundmaeker, H.; Guillemin, P.; Friess, P.; Woelfflé, S. Vision and challenges for realising the Internet of Things. *Clust. Eur. Res. Proj. Internet Things Eur. Commision* **2010**, *3*, 34–36.
2. Almadhoun, R.; Kadadha, M.; Alhemeiri, M.; Alshehhi, M.; Salah, K. A user authentication scheme of IoT devices using blockchain-enabled fog nodes. In Proceedings of the 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), Aqaba, Jordan, 28 October–1 November 2018; pp. 1–8.
3. Atamli, A.W.; Martin, A. Threat-based security analysis for the internet of things. In Proceedings of the 2014 International Workshop on Secure Internet of Things, Wroclaw, Poland, 10 September 2014; pp. 35–43.
4. Kasinathan, P.; Pastrone, C.; Spirito, M.A.; Vinkovits, M. Denial-of-Service detection in 6LoWPAN based Internet of Things. In Proceedings of the 2013 IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob), Lyon, France, 7–9 October 2013; pp. 600–607.
5. Khan, F.; Khan, A.W.; Shah, K.; Qasim, I.; Habib, A. An algorithmic approach for core election in mobile ad-hoc network. *J. Internet Technol.* **2019**, *20*, 1099–1111.
6. Malik, A.; Khan, M.Z.; Faisal, M.; Khan, F.; Seo, J.T. An efficient dynamic solution for the detection and prevention of black hole attack in vanets. *Sensors* **2022**, *22*, 1897. [CrossRef] [PubMed]
7. Abbas, S.; Talib, M.A.; Ahmed, A.; Khan, F.; Ahmad, S.; Kim, D.H. Blockchain-based authentication in internet of vehicles: A survey. *Sensors* **2021**, *21*, 7927. [CrossRef] [PubMed]
8. Khan, F.; Ahmad, S.; Gürüler, H.; Cetin, G.; Whangbo, T.; Kim, C.G. An Efficient and Reliable Algorithm for Wireless Sensor Network. *Sensors* **2021**, *21*, 8355. [CrossRef]
9. Khan, F.; Zahid, M.; Gürüler, H.; Tarımer, İ.; Whangbo, T. An Efficient and Reliable Multicasting for Smart Cities. *CMC-Comput. Mater. Contin.* **2022**, *72*, 663–678. [CrossRef]
10. Khan, F.; Gul, T.; Ali, S.; Rashid, A.; Shah, D.; Khan, S. Energy aware cluster-head selection for improving network life time in wireless sensor network. In *Intelligent Computing, Proceedings of the 2018 Computing Conference, Tokyo, Japan, 21–23 December 2018*; Springer International Publishing: London, UK, 2018; Volume 2, pp. 581–593.
11. Al-Atawi, A.A.; Khan, F.; Kim, C.G. Application and Challenges of IoT Healthcare System in COVID-19. *Sensors* **2022**, *22*, 7304. [CrossRef]
12. Farooqi, M.M.; Shah, M.A.; Wahid, A.; Akhunzada, A.; Khan, F.; ul Amin, N.; Ali, I. Big data in healthcare: A survey. In *Applications of Intelligent Technologies in Healthcare*; Springer: Cham, Switzerland, 2019; pp. 143–152.
13. Zhao, G.; Si, X.; Wang, J.; Long, X.; Hu, T. A novel mutual authentication scheme for Internet of Things. In Proceedings of the 2011 International Conference on Modelling, Identification and Control, Shanghai, China, 26–29 June 2011; pp. 563–566.
14. Idrus, S.Z.S.; Cherrier, E.; Rosenberger, C.; Schwartzmann, J.-J. A review on authentication methods. *Aust. J. Basic Appl. Sci.* **2013**, *7*, 95–107.

15. Ali, I.; Sabir, S.; Ullah, Z. Internet of things security, device authentication and access control: A review. *arXiv* **2019**, arXiv:1901.07309.
16. Airehrour, D.; Gutierrez, J.; Ray, S.K. Secure routing for internet of things: A survey. *J. Netw. Comput. Appl.* **2016**, *66*, 198–213. [CrossRef]
17. Miorandi, D.; Sicari, S.; De Pellegrini, F.; Chlamtac, I. Internet of things: Vision, applications and research challenges. *Ad Hoc Netw.* **2012**, *10*, 1497–1516. [CrossRef]
18. Kavianpour, S.; Shanmugam, B.; Azam, S.; Zamani, M.; Samy, G.N.; De Boer, F. A Systematic Literature Review of Authentication in Internet of Things for Heterogeneous Devices. *J. Comput. Netw. Commun.* **2019**, *2019*, 5747136. [CrossRef]
19. Haghparast, M.B.; Berehlia, S.; Akbari, M.; Sayadi, A. Developing and evaluating a proposed health security framework in IoT using fuzzy analytic network process method. *J. Ambient Intell. Humaniz. Comput.* **2021**, *12*, 3121–3138. [CrossRef]
20. Al-Zahrani, F.A. Evaluating the Usable-Security of Healthcare Software Through Unified Technique of Fuzzy Logic, ANP and TOPSIS. *IEEE Access* **2020**, *8*, 109905–109916. [CrossRef]
21. Zarour, M.; Ansari, T.J.; Alenezi, M.; Sarkar, A.K.; Faizan, M.; Agrawal, A.; Kumar, R.; Khan, R.A. Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records. *IEEE Access* **2020**, *8*, 157959–157973. [CrossRef]
22. Enaizan, O.; Zaidan, A.; Alwi, N.H.M.; Zaidan, B.B.; AlSalem, M.A.; Albahri, O.S. Electronic medical record systems: Decision support examination framework for individual, security and privacy concerns using multi-perspective analysis. *Health Technol.* **2020**, *10*, 795–822. [CrossRef]
23. Huang, X.; Nazir, S. Evaluating security of internet of medical things using the analytic network process method. *Secur. Commun. Netw.* **2020**, *2020*, 8829595. [CrossRef]
24. Seh, A.H.; Al-Amri, J.F.; Subahi, A.F.; Ansari, T.J.; Kumar, R.; Bokhari, M.U.; Khan, R.A. Hybrid computational modeling for web application security assessment. *CMC-Comput. Mater. Contin.* **2022**, *70*, 469–489.
25. Ahmad, M.; Al-Amri, J.F.; Subahi, A.F.; Khatri, S.; Seh, A.H.; Nadeem, M.; Agrawal, A. Healthcare Device Security Assessment through Computational Methodology. *Comput. Syst. Sci. Eng.* **2022**, *41*, 811–828. [CrossRef]
26. Algarni, A.; Ahmad, M.; Attaallah, A.; Agrawal, A.; Kumar, R.; Khan, R.A. A fuzzy multi-objective covering-based security quantification model for mitigating risk of web based medical image processing system. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 481–489. [CrossRef]
27. Ansari, M.T.J.; Al-Zahrani, F.A.; Pandey, D.; Agrawal, A. A fuzzy TOPSIS based analysis toward selection of effective security requirements engineering approach for trustworthy healthcare software development. *BMC Med. Inform. Decis. Mak.* **2020**, *20*, 236. [CrossRef] [PubMed]
28. Kumar, R.; Pandey, A.K.; Baz, A.; Alhakami, H.; Alhakami, W.; Agrawal, A.; Khan, R.A. Fuzzy-based symmetrical multi-criteria decision-making procedure for evaluating the impact of harmful factors of healthcare information security. *Symmetry* **2020**, *12*, 664. [CrossRef]
29. Tahir, M.; Sardaraz, M.; Muhammad, S.; Khan, M.S. A Lightweight Authentication and Authorization Framework for Blockchain-Enabled IoT Network in Health-Informatics. *Sustainability* **2020**, *12*, 6960. [CrossRef]
30. Verma, U.; Bhardwaj, D. Design of Lightweight Authentication Protocol for Fog enabled Internet of Things-A Centralized Authentication Framework. *Int. J. Commun. Netw. Inf. Secur.* **2020**, *12*, 162–167. [CrossRef]
31. Li, X.; Niu, J.; Kumari, S.; Liao, J.; Liang, W.; Khan, M.K. A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity. *Secur. Commun. Netw.* **2016**, *9*, 2643–2655. [CrossRef]
32. Kumar, P.; Lee, S.-G.; Lee, H.-J. E-SAP: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. *Sensors* **2012**, *12*, 1625–1647. [CrossRef]
33. Le, X.H.; Khalid, M.; Sankar, R.; Lee, S. An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare. *J. Netw.* **2011**, *6*, 355–364. [CrossRef]
34. Deebak, B.; Al-Turjman, F. Smart Mutual Authentication Protocol for Cloud Based Medical Healthcare Systems Using Internet of Medical Things. *IEEE J. Sel. Areas Commun.* **2020**, *39*, 346–360. [CrossRef]
35. Mehmood, A.; Natgunanathan, I.; Xiang, Y.; Poston, H.; Zhang, Y. Anonymous authentication scheme for smart cloud based healthcare applications. *IEEE Access* **2018**, *6*, 33552–33567. [CrossRef]
36. Yeh, H.-L.; Chen, T.-H.; Liu, P.-C.; Kim, T.-H.; Wei, H.-W. A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. *Sensors* **2011**, *11*, 4767–4779. [CrossRef]
37. Chen, H.; Ge, L.; Xie, L. A user authentication scheme based on elliptic curves cryptography for wireless ad hoc networks. *Sensors* **2015**, *15*, 17057–17075. [CrossRef]
38. Yoon, E.-J.; Yoo, K.-Y. A new biometric-based user authentication scheme without using password for wireless sensor networks. In Proceedings of the 2011 IEEE 20th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, Paris, France, 27–29 June 2011; pp. 279–284.
39. Althobaiti, O.; Al-Rodhaan, M.; Al-Dhelaan, A. An efficient biometric authentication protocol for wireless sensor networks. *Int. J. Distrib. Sens. Netw.* **2013**, *9*, 407971. [CrossRef]
40. Shi, W.; Gong, P. A new user authentication protocol for wireless sensor networks using elliptic curves cryptography. *Int. J. Distrib. Sens. Netw.* **2013**, *9*, 730831. [CrossRef]
41. Quan, Z.; Chunming, T.; Xianghan, Z.; Chunming, R. A secure user authentication protocol for sensor network in data capturing. *J. Cloud Comput.* **2015**, *4*, 6. [CrossRef]

42. Kumar, P.M.; Gandhi, U.D. Enhanced DTLS with CoAP-based authentication scheme for the internet of things in healthcare application. *J. Supercomput.* **2020**, *76*, 3963–3983. [CrossRef]
43. Yang, T.; Zhang, G.; Liu, L.; Yang, Y.; Zhao, S.; Sun, H.; Wang, W. New Features of Authentication Scheme for the IoT: A Survey. In Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things, London, UK, 15 November 2019; pp. 44–49.
44. Watro, R.; Kong, D.; Cuti, S.-F.; Gardiner, C.; Lynn, C.; Kruus, P. TinyPK: Securing sensor networks with public key technology. In Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, Washington, DC, USA, 25 October 2004; pp. 59–64.
45. Dhillon, P.K.; Kalra, S. Multi-factor user authentication scheme for IoT-based healthcare services. *J. Reliab. Intell. Environ.* **2018**, *4*, 141–160. [CrossRef]
46. Siddiqui, Z.; Abdullah, A.H.; Khan, M.K.; Alghamdi, A.S. Smart environment as a service: Three factor cloud based user authentication for telecare medical information system. *J. Med. Syst.* **2014**, *38*, 9997. [CrossRef]
47. Kanjee, M.R.; Divi, K.; Liu, H. A physiological authentication scheme in secure healthcare sensor networks. In Proceedings of the 2010 7th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), Boston, MA, USA, 21–25 June 2010; pp. 1–3.
48. Shakil, K.A.; Zareen, F.J.; Alam, M.; Jabin, S. BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud. *J. King Saud Univ.-Comput. Inf. Sci.* **2020**, *32*, 57–64. [CrossRef]
49. Wong, K.H.; Zheng, Y.; Cao, J.; Wang, S. A dynamic user authentication scheme for wireless sensor networks. In Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), Taichung, Taiwan, 5–7 June 2006; p. 8.
50. Das, M.L. Two-factor user authentication in wireless sensor networks. *IEEE Trans. Wirel. Commun.* **2009**, *8*, 1086–1090. [CrossRef]
51. Kumari, A.; Kumar, V.; Abbasi, M.Y.; Kumari, S.; Chaudhary, P.; Chen, C.-M. Csef: Cloud-based secure and efficient framework for smart medical system using ecc. *IEEE Access* **2020**, *8*, 107838–107852. [CrossRef]
52. Bhattasali, T.; Saeed, K. Two factor remote authentication in healthcare. In Proceedings of the 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Delhi, India, 24–27 September 2014; pp. 380–386.
53. Pamučar, D.; Stević, Ž.; Sremac, S. A new model for determining weight coefficients of criteria in mcdm models: Full consistency method (fucom). *Symmetry* **2018**, *10*, 393. [CrossRef]
54. Putra, D.; Sobandi, M.; Andryana, S.; Gunaryati, A. Fuzzy analytical hierarchy process method to determine the quality of gemstones. *Adv. Fuzzy Syst.* **2018**, *2018*, 9094380.
55. Al-Azab, F.G.M.; Ayu, M.A. Web based multi criteria decision making using AHP method. In Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M) 2010, Jakarta, Indonesia, 13–14 December 2010; pp. A6–A12.
56. Sehra, S.K.; Brar, D.; Singh, Y.; Kaur, D. Multi criteria decision making approach for selecting effort estimation model. *arXiv* **2013**, arXiv:1310.5220.
57. Nazir, S.S.S.; Abid, S.B.S. Selecting software design based on birthmark. *Life Sci. J.* **2014**, *11*, 89–93.
58. Saaty, T.L.; Tran, L.T. On the invalidity of fuzzifying numerical judgments in the Analytic Hierarchy Process. *Math. Comput. Model.* **2007**, *46*, 962–975. [CrossRef]
59. Krohling, R.A.; Pacheco, A.G. A-TOPSIS–an approach based on TOPSIS for ranking evolutionary algorithms. *Procedia Comput. Sci.* **2015**, *55*, 308–317. [CrossRef]
60. Wang, P.; Li, B.; Shi, H.; Shen, Y.; Wang, D. Revisiting Anonymous Two-Factor Authentication Schemes for IoT-Enabled Devices in Cloud Computing Environments. *Secur. Commun. Netw.* **2019**, *2019*, 2516963. [CrossRef]