mathematics

MDPI

Article

Fuzzy-Based Unified Decision-Making Technique to Evaluate Security Risks: A Healthcare Perspective

Abdulaziz Attaallah [1], Khalil al-Sulbi [2], Areej Alasiry [3], Mehrez Marzougui [3], Syed Anas Ansar [4,*], Alka Agrawal [5], Md Tarique Jamal Ansari [5] and Raees Ahmad Khan [5]

[1] Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[2] Department of Computer Science, Al-Qunfudah Computer College, Umm Al-Qura University, Mecca 24382, Saudi Arabia
[3] College of Computer Science, King Khalid University, Abha 61421, Saudi Arabia
[4] Department of Computer Applications, Babu Banarasi Das University, Lucknow 226028, Uttar Pradesh, India
[5] Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow 226025, Uttar Pradesh, India
* Correspondence: syed000anas@gmail.com

Abstract: Neoteric biomedical, technological, and normative shifts have prompted care firms to establish clinical governance as a contrivance to assure high-quality service in an exceedingly intricate milieu. Web security is an epochal concern in the healthcare sector, although it has garnered scant attention since the inception of web applications. The necessity to provide adequate security for healthcare web applications (HWAs) cannot be exaggerated, as umpteen health agencies are contingent on them to carry out their operations. Every healthcare organization renders a humongous volume of data available online to practitioners, pharmacies, and patients. Researchers are continually endeavoring to ameliorate techniques to increase the security and longevity of HWAs. In this context, experts examined certain imperative security risks in HWAs to quantitatively evaluate them in the design phase and covered numerous facets of HWAs, along with their security attributes and risk factors. The authors have proposed a combined approach of fuzzy-based symmetric techniques, i.e., AHP-TOPSIS (Analytic Hierarchy Process–Technique for Order of Preference by Similarity to Ideal Solution), for the assessment of alternative HWAs, leveraging the multi-criteria decision-making (MCDM) approach. Ten consecutive HWAs from local hospitals in Uttar Pradesh, India, have been taken to estimate the security risk, incorporating this methodology to evaluate the priority of weightage and the impact of security attributes. Henceforth, the findings and methodology employed in this study can assist security practitioners in identifying and prioritizing the most influential risk factors to secure HWAs and encourage them to develop revamped or novel methods.

Keywords: healthcare web application (HWA); security risk factors; CIA (confidentiality, integrity, availability) triad; fuzzy analytic hierarchy process (AHP); fuzzy technique for order of preference by similarity to ideal solution (TOPSIS); multi-criteria decision-making (MCDM)

MSC: 03B42; 03B52; 03B70

Citation: Attaallah, A.; al-Sulbi, K.; Alasiry, A.; Marzougui, M.; Ansar, S.A.; Agrawal, A.; Ansari, M.T.J.; Khan, R.A. Fuzzy-Based Unified Decision-Making Technique to Evaluate Security Risks: A Healthcare Perspective. *Mathematics* **2023**, *11*, 2554. https://doi.org/10.3390/math11112554

Academic Editor: José Antonio Sanz

Received: 6 May 2023
Revised: 28 May 2023
Accepted: 30 May 2023
Published: 2 June 2023

1. Introduction

In this rapidly evolving IT world, scientific communities, local or multinational businesses, and the medical sector rely extensively on computers to store sensitive data. The dispensation of healthcare amenities is being reformed from an archaic hospital-centric model to a more virtual, dispersed service that extensively exploits the most recent technologies such as the 3D printing of tissues and implants, intelligent machines, genomics, data analytics, and robotics. This advancement has transformed the working environment of web applications via myriad innovative techniques to help them carry out their tasks

quickly and efficiently. Medical workers are assigned a copious assemblage of responsibilities, and managing them is more intricate and arduous. Plenty of patients' documentation has to be managed, including tracking inventory, the working schedules of doctors, records for keeping bills, patient reports, etc. [1]. Due to the ubiquitous use of computers, healthcare web applications (HWAs) are becoming inexorably convoluted and require high levels of security [2]. The security assessment process gives HWA practitioners the assurance that the presence of any vulnerability will not have a negative impact on their systems and that they can always use mitigation techniques. Hereby, this process maximizes the success of user satisfaction on HWA systems, but in the present scenario, security issues are constantly evolving due to the heterogeneous nature of HWAs. Digital technology is being researched and implemented in all facets of healthcare. Figure 1 divides the numerous HWAs into several application domains; however, there are thousands of distinct applications [3].

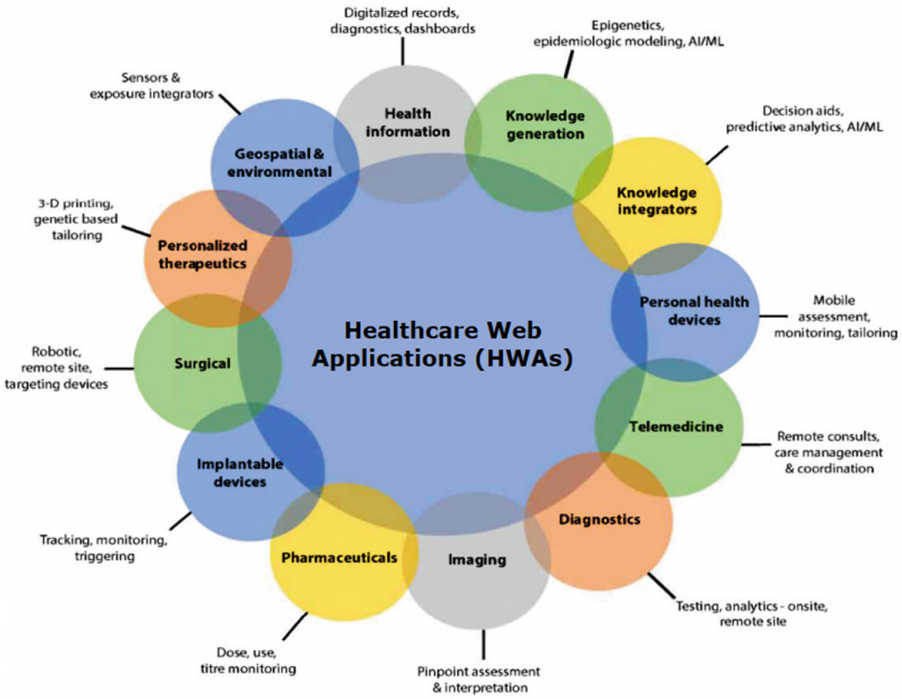

Figure 1. Different categories of healthcare web applications (HWAs).

The security estimation of HWAs focuses on the functional aspects of the application and its ability to endure a malicious attack and recover without data loss or any other abnormality. Security breaches are compromising thousands of health records. Ample statistics have shown data breach instances, and recently, innumerable incidences of the inadvertent loss or theft of sensitive clinical data have been documented [4,5] that have affected patients. Moreover, threats from botnets (a network of surreptitiously infected computer systems due to malware) have increased drastically. Cybercriminals purchase access to botnets and use the network of infected computer systems for various crimes, usually financial data thefts, the dissemination of spam, concealing other crimes, or distributed denial of service (DDoS). According to a recent study, every year, almost 25 million compelled authorizations for the disclosure of healthcare records are issued in the United States [6]. According to the Cyber Crime Website of the Department of Justice, USA [7], a company has reportedly suffered a loss of more than USD 100,000 as a result of cybercrime. As per a white paper published by Cyber Unit CCIPS, US Department of Justice, many public and private organizations are increasingly adopting vulnerability disclosure programs, which increase their ability to detect security issues, protect sensitive data, and prevent the disruption of services [8]. A built-in software security framework that includes all security attributes can be a viable and potent solution to numerous security issues [9,10]. It can prove to be a boon

to the users, organizations, and governments that spend billions of dollars every year on securing their networks.

Consequently, to secure an individual's data, three major security factors and privacy goals are commonly identified as the CIA (confidentiality, integrity, and availability) triad [11,12]. There is a significant necessity to the CIA triad: confidentiality must be included for highly sensitive data; integrity is essential because it may be fatal to provide an inaccurate procedure based on faulty medical data; and availability is also necessary because the data must be available on time for adequate treatment. In the medical field, the security and privacy of individual data are critical, and it is a major challenge to protect healthcare data [13].

Often, experts in the IT industry have focused on the deployment phase of HWAs to improve security longevity and minimize maintenance costs and time. However, integrating security and unearthing vulnerabilities early in the design phase of web applications can reduce the time and cost of development by minimizing the development team's work [14–16]. This reveals the impact of vulnerabilities that can affect healthcare web applications' integrity, violate confidentiality and privacy norms, and exploit loopholes in the design phase. Moreover, security flaws in the design may also cause the application to violate its security and result in the unauthorized disclosure, modification, and destruction of data [17]. The vulnerability may impact exhaustive data theft, malware, and spyware injection that may cause failure in the entire HWA security. In light of this, it has become vitally important in today's environment to ensure security from the early stages of the software development life cycle (SDLC). In accordance with a recent study, software organizations are contemplating implementing a software security risk in the early phase of development rather than depending on the later phase of the SDLC. This step could improve the situation and reduce losses to a substantial level. In addition, techniques of security optimization can further help security practitioners and researchers reduce the time and cost required for developing an HWA system. Moreover, in-depth identification, analysis, and mitigation will deliver a quality product.

Despite the increasing prevalence of HWAs in contemporary healthcare systems, there is a notable research gap in comprehending certain security issues and risk factors pertaining to these applications. Prior research has predominantly focused on generic web application security with minimal emphasis on the specific risks and vulnerabilities that are unique to HWAs. This study aims to address this research gap by:

- Conducting an extensive analysis of the inherent security risks of HWAs, considering factors such as patient data confidentiality, secure data transmission, access control, and authentication.
- Examining the impact of these security risks on the availability, confidentiality, and integrity of sensitive healthcare data.
- Identifying and prioritizing the most significant security risk factors requiring immediate attention and effective mitigation strategies.
- Providing healthcare organizations, developers, and security professionals with actionable recommendations and guidelines to improve the security of HWAs and protect patient data.

This study advances the field of HWA security by addressing these research gaps. The findings provide insights and practical implications for healthcare organizations and security practitioners, allowing them to proactively address the unique security challenges posed by HWAs and safeguard sensitive healthcare data. This research paper contributes significantly to the field of HWA security by introducing the AHP-TOPSIS (Analytic Hierarchy Process–Technique for Order of Preference by Similarity to Ideal Solution) system. Multiple HWAs are scrutinized, and their potential security risks are evaluated using the MCDM approach. The authors conducted an empirical study based on MCDM and have acknowledged numerous studies on the methods of risk management strategies. The proposed methodology is based on risk assessment in HWAs, which identi-

fies, maps, prioritizes, and evaluates the impact of risk factors on various alternatives, as discussed below:

- The identification of security risk factors and attributes: It creates a roadmap for security professionals for the development of secure healthcare web applications. The identification aim is to target key risk factors at the design phase to mitigate them at the earlier phase of the development life cycle.
- Mapping security risk factors with security attributes: This may be done through an in-depth literature survey and expert points of view. It gives developers an understanding and overview, i.e., whether the security requirements are fulfilled or not.
- The prioritization of security risk factors: The authors used fuzzy AHP for the prioritization of security risk factors corresponding to their respective weights and ranks.
- The impact of attributes on alternatives: The fuzzy AHP-TOPSIS is used to evaluate the impact of attributes on different alternatives. The identification and prioritization of the risk factors will provide a path to develop a secure healthcare web application.

The paper is organized in the following manner: Section 2 reviews the existing literature in this domain. Section 3 discusses the software security risk factors along with their related attributes in healthcare web applications. In Section 4, the methodology and numerical analysis of the experimental data are described in depth. The paper is concluded in Section 5 with a succinct analysis and discussion.

2. Related Work

Several studies have been undertaken by researchers using multiple methodologies and symmetrical techniques to analyze the security of healthcare web applications. Along with fuzzy AHP, symmetrical TOPSIS techniques have been utilized in various domains of interest to improve security measures and handle MCDM (multi-criteria decision-making)-based problems. Considerable research on the security of healthcare web applications has previously been conducted utilizing various methodologies and techniques. The following research studies have been reviewed by the authors in this domain:

Abdulaziz et al. (2022) examined big data security by identifying and prioritizing security measures using two hybrid approaches. The approaches include fuzzy AHP and classical AHP. The fuzzy AHP approach quantitatively analyzes as well as prioritizes the different factors based on their weight to enhance overall security. The early identification of vulnerability will heighten the security and durability of big data, which will benefit consumers and enterprises. This study's findings showed that MCDM approaches, i.e., fuzzy AHP, demonstrated more efficient results than classical AHP. It is helpful in the procedures of decision-making to alleviate the problem of uncertainty [18]. Alfakeeh et al. (2022) used AHP-TOPSIS with a hesitant fuzzy technique to forecast the risk of different healthcare applications. This approach is used to measure the security and durability that would help in designing secure healthcare applications. The authors selected 10 alternatives to evaluate the efficiency and security of applications. Among the 10, alternative 6 provided the most efficient and long-lasting security. Furthermore, the authors concluded that security breaches could be considerably mitigated if addressed early in their development phase and prioritized security as the topmost concern [19].

Lotfi et al. (2022) asserted that a strategy called Resilience and Sustainable Health Care Supply Chain (RSHCSC) with VMI, which combines fuzzy and data-driven robust optimization, is suitable for enhancing the inventory management system and addressing unpredictability and disruption. The use of hybrid fuzzy and data-driven robust optimization with a stochastic programming technique was suggested for three RSHCSC models. Essential variables such as fuzzy cut, robustness and resilience coefficient, level of confidence, and size models were subjected to sensitivity analysis. According to the results, as the fuzzy cut, robustification coefficient, confidence level, resiliency coefficient, and CVaR confidence level increase, the number of costs also increases [20]. To determine which maturity model best adheres to TQM (Total Quality Management) principles for Industry 4.0 maturity models, Zceylan and Elibal (2022) used the linguistically fuzzy TOPSIS

(Technique for Order Preference by Similarity to Ideal Solution) method for ranking and the DEMATEL (Decision-Making Trial and Evaluation Laboratory) method for weighting criteria. Seven main criteria and 33 supporting factors were used to assess the maturity of four Industry 4.0 models. Researchers and practitioners can use the study's findings to compare, create, and improve Industry 4.0 maturity models [21].

Abushark et al. (2021) defined several taxonomies and created a design hierarchy, incorporating the most prevalent quality evaluation factors, which integrate variables, characteristics, and traits from different Security Requirements Engineering (SRE) methodologies. The fuzzy AHP-TOPSIS model was utilized in this paper as an MCDM (Multiple-Criteria Decision-Making) model. The author defined the STORE technique as a highly consistent and usable approach among all other SRE techniques with a threat-driven approach. In addition, they concluded that STORE elicits security requirements in an efficient and well-organized manner [22]. Kumar et al. (2021) identified and analyzed the characteristics of security and sustainability. In this study, the fuzzy AHP algorithm was utilized for quantitative assessment, which was verified by four other approaches based on AHP. As a result, the evaluation of security in this study can assist developers in formulating standards that will ensure the development of more secure online applications [23].

Attaallah et al. (2020) discussed security as a critical aspect in the process of software development that must be considered during its development cycle. Thus, the researcher evaluates the effect of security risks using the integrated approach of TOPSIS and fuzzy AHP. This hybrid approach is ideal for evaluating malware analysis on the basis of its impact. According to the evaluation report, among the 10 institutions, the 8th institutional web application was determined as the most efficient and durable security system among all competing options [24]. Al-Zahrani (2020) reviewed healthcare applications to ensure software usability and security by using the hybrid technique. The author suggested that security experts must design a healthcare web application with two intents; it ensures usability, given to fulfill the users rather than ensuring the optimum security and efficacy of security as well as usability in the early development phase [25].

Altowaijri (2020) proposed a framework for the healthcare sector to enhance the healthcare security of cloud computing. The author introduced the concept of master nodes and slave nodes in his architecture to store the data. In this architecture, the master node keeps metadata; on the other side, the responsibility of the slave node is to store data. The sensors can access all consumers' data and ensure its efficiency as it is in a quasi-structured form, and these data are easily accessible. This architecture stores data in encrypted form. It is based on the RSA (Rivest Shamir Adleman) and PKI (Public Key Infrastructure) algorithms, which provide accessibility to authorized users at a certain time to access the data of particular patients [26]. Abu-elezz et al. (2020) investigated healthcare blockchain technology's scoping review with strengths and risks. This research was carried out in three phases: the identification phase, the screening phase, and the eligibility phase. These filtering stages were conducted through a flow diagram of Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA). Researchers have suggested that this analysis will help to obtain a more precise understanding, owing to various constraints. The findings of this analysis must be viewed with caution, and this scoping review provides useful insights, particularly in medical care [27].

3. Security Risk Factors and Attributes

Software security is the branch of software engineering that aims to prevent the exploitation of security loopholes in the system and detect possible vulnerabilities that may prove detrimental to the software. The successful implementation of a security plan may converge the developing team's entire focus to select periodic errors/vulnerabilities that may have impacted the healthcare web application system and can prepare a strategy for a timely recovery. In this section, several security attributes and security risk factors are identified on behalf of the literature survey and from the expert's viewpoint. The use of security attributes in the development lifecycle comes under the ambit of security plan

specifications at various stages, without which the security of the software system cannot be insured.

3.1. Security Attributes

Security is a multidimensional and comprehensive process that involves a large gamut of operations divided into several stages to ensure the in-depth analysis of security-related challenges and threats. To mitigate the security issues that could affect the performance of a healthcare web application system, the five set attributes are elucidated: confidentiality, integrity, availability, access control, and authentication. These attributes form the basic fundamentals of security; without them, the security of software cannot be ensured. The main reason for using these attributes is to plug in gaps in the healthcare web application structure so that security breaches cannot be made [28].

3.1.1. Confidentiality

Confidentiality ensures that the data are not disclosed to unauthorized users. This attribute has been described as a pillar of healthcare ethics since Hippocrates [29]. It is a broad security concept implemented at all stages of a healthcare web application system, including the processing, storage, retrieval, and display of information. Hence, it strengthens a trusted binding mechanism of design and all its components, assuring that the sanctity of data is preserved in encrypted form and not violated by intruders.

3.1.2. Integrity

Integrity is the accuracy of the data in storage or during transmission. It assures that the end-user's data are not corrupted or tampered with during transmission. In a more expanded form, integrity can be ensured both at the source and destination, which can prevent the unauthorized use of data [30].

3.1.3. Availability

The availability attribute ensures that a system is ready and available for use by an authorized user whenever needed. The availability of a system may be compromised in case of a denial-of-service attack [31]. The availability of a system confirms that the system is ready to be used for all the needed functionalities. The system should be designed in multiple subsystems so that the availability of the system is not jeopardized in case of the failure of any of the subsystems.

3.1.4. Access Control

Access control limits how the system should be used by its legitimate users. The users are required to present credentials to access the system's specific functionality. Depending on respective access controls, role-based accessibility is allocated to users: some of the users may be given complete control of the system, such as the administrators, while other users may be given only limited access, such as the end-users, based on their specific use of the system [32].

3.1.5. Authentication

Authentication is the process of identifying the legitimate user requesting access to the system. A username and password are the most common method of authenticating any user to provide access. The authentication process involves a mechanism that validates authentic users or multiple users to access information. This authentication can be in the form of a security question, SMS, OTP, biometric, RSA, etc. [33].

3.2. Security Risk Factors

The demand for security is escalating every day as the IT field expands, resulting in enhanced applications that may require high levels of security. Security typically relies on two integrated viewpoint elements, i.e., effective risk management as well as effective

countermeasures [34]. To estimate security risk and ameliorate it, organizations need to identify and address the different types of security characteristics that affect security directly or indirectly. HWAs' security may be enhanced by identifying and mitigating security risks at earlier phases of the SDLC. In this paper, the risk is defined from the perspective of the software vulnerability, taking into account both the likelihood of HWA vulnerability and exploitation impact in a system. This may cause the potential loss, destruction, or damage of assets, while a vulnerability is a weakness that could expose threats within user systems, networks, and applications [35]. A system's security is jeopardized when a vulnerability is discovered but not patched, and new vulnerabilities are identified over the course of a software system's lifespan. As per the studies of existing research and experts' opinions, some of the common security risks are listed below with a concise elucidation (see Table 1).

Table 1. An overview of security risk factors in the design phase.

S. No.	CWE ID	Security Risk Factors	Scope Factor
1.	ACPVPM	This weakness might allow an attacker to modify the variable that contains an unintended value. It is a public method that reads, alters, or modifies a private variable; it may violate other code parts' definitions or values. In addition, if an attacker can read the private variable, it is easy for the attacker to launch more attacks as well as expose sensitive information, and it affects the integrity scope of variables [36].	Integrity, Access Control
2.	PCF	The software keeps passwords within configuration files that could be accessed by unknown actors. Having access to this file would allow an attacker to either steal the password, modify it to their own preference, or create unfavorable conditions [37].	Access Control, Authentication
3.	MESD	This vulnerability is introduced due to the absence of proper data encryption, which allows the transmission of the assurance of confidentiality, transparency, and integrity by properly enforced encryption. Before the storage or transmission of data, the application does not encrypt critical and confidential information. This vulnerability is triggered during the phase of architecture and design due to lacking security tactics [38].	Confidentiality, Integrity
4.	UPC	An attacker might use this flaw to alter the victim's password and allow him to gain access to the user's data. On the other hand, the application does not require any kind of authentication or knowledge about the user's original password when creating a new password [39].	Access Control, Authentication
5.	RCT	In a multi-threaded environment that uses the locking functionality around code that enforces the system to block, alter, and read persistent data. If a resource is used concurrently by two execution threads, there is a risk that invalid resources can be used. It is mainly introduced in programming when the critical resource is changed by two or more execution threads [40].	Integrity
6.	USP	This weakness might allow attackers to access data files in an unauthorized way or unexpectedly change configuration settings to execute their programs. Such programs will enable the application to find critical resources using a search path, which an attacker may alter through malicious code [41].	Confidentiality, Integrity, Availability, Access Control
7.	DCIC	The main drawback of this weakness is that the program's executable code or source code is downloaded without verifying its data integrity and origin. The absence of authentication makes it possible for attackers to fool the machine by executing malicious code or altering the source code [42].	Confidentiality, Integrity
8.	RC	In this flaw, concurrent operations are executed on a single resource without proper synchronization. The code requires that certain states should not be modified between two operations, but a timing window exists in which the state can be modified by an unexpected actor or process. Such conditions allow a remote user to take advantage of the race by executing a series of commands and conducting a DoS (denial of service) attack [43].	Integrity
9.	EITV	The critical internal variables are initialized by software or stored data by using input fields that can be manipulated by unauthorized users. If any variables have been externally initialized, they should be distrusted, specifically in the case of users, because there is the possibility of incorrect initialization. The improper initialization of variables may interrupt the software response and create vulnerabilities in software security [44].	Integrity
10	ICMD	This vulnerability occurs when software uses an upstream component (client to server) to receive input data that defines several variables, fields, or properties in an object that should be updated or initialized. However, it is unable to appropriately control which attributes may be modified. If any attributes of an object are only solely meant for internal use, then their unintentional modification may result in a security flaw [45].	Integrity

4. Methodology

Web application security is one of the chief concerns that define the application's reliability, lifespan, and efficiency for both end-users and developers. In order to raise the caliber of a web application, security estimation is essential in the design phase that extends the security lifespan. Apart from technological progress in the development sector, numerous statistics have shown data breach instances that have affected the privacy of patients and the eminence of HMS. This section delineates the MCDM-based fuzzy methodology to evaluate security attributes and their risk factors.

The integrated approach of fuzzy AHP and fuzzy TOPSIS is extremely proficient to scrutinize healthcare web application security from the design tactics viewpoint for gauging HWAs' rankings and fix their security risks. The current study involves various aspects for designing a security risk estimation framework, such as the identification of factors, the mapping of security risk factors with their corresponding security attributes, the assessment of risk factors, and statistical analysis. The mapping matrix is based on synchronizing the top 10 security risk factors, i.e., ACPVPM, PCF, MESD, UPC, RCT, USP, DCIC, RC, EITV, and ICMD, which are mapped with their security attributes such as CIA, Access Control, and Authentication (see Figure 2).

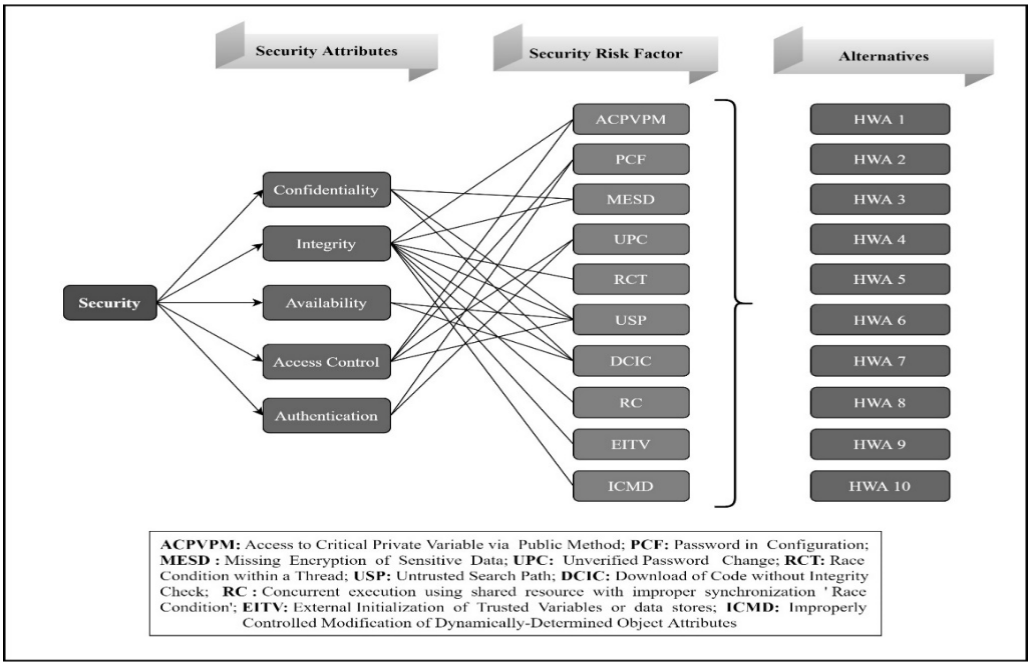

Figure 2. A hierarchy of security attributes and risk factors.

For evaluating the risk factors of healthcare web applications, the hierarchical structure is represented graphically. All the classifying factors and sub-factors for the data processing algorithm, in order to generate the research finding were identified using a literature review and a consultation with experts. The researcher of this review discovered that specialists had used fuzzy theory along with AHP to examine the imprecise real-world challenges because they are exceedingly ambiguous [46]. The precise details of these approaches are discussed in the subsequent section.

4.1. Fuzzy AHP

Fuzzy AHP is a powerful prescript for addressing arduous conclusive problems, and all the complicated problems may be evaluated through various classed levels of objectives. To solve the arduousness of a complex problem, fuzzy AHP divides it into a tree-like structure. In addition, for the estimation of the priority of various alternatives with multiple criteria in a hierarchical structure, it is also utilized as a decision-making

technique [47]. The fuzzy AHP is based on fuzzy interval arithmetic, which uses the TFN to compute the weights of elements. Saaty was the first who proposed the AHP technique [48]. To deal with imprecision in multi-criteria decision problems, it merely uses the pair-wise comparison matrix [49]. The triangular fuzzy numbers are used in this model to represent linguistic variables and to conduct fuzzy operations using AHP. To deal with the uncertainty caused by imprecision and vagueness, Zadeh developed the fuzzy set theory [50].

On the basis of experts' viewpoints as well as responses via questionnaire or by using brainstorming, the tree structure is prepared, and after that, a triangular fuzzy number (TFN) is fabricated from the hierarchy. In addition, a pair-wise comparison of every cluster of grouped objectives performs a significant contribution to determining the impact of one criterion on the other. The researcher transfigures the linguistic values into the TFN as well as crisp numbers, and in this study, the values of the TFN are between 0 and 1 [51]. The computational simplicity of triangular fuzzy membership functions, as well as their ability to deal with fuzzy data, is the reason for their widespread acceptance [52]. Additionally, the classification of linguistic values is equally important, fairly important, strongly important, weakly important, absolutely important, etc., and apart from these, the crisp values are grouped as from {1, 2, ...9}. Furthermore, a fuzzy number TFN $\mu_a(t)$ is defined by the triangular membership function l_o, m_i, and u_p are given as limits (i.e., lower limit, middle limit, and upper limit, respectively), as shown in Figure 3, and the membership functions are depicted in Equations (1) and (2):

$$\mu_a(t) = \mathrm{a} = (l_o, m_i, u_p) \tag{1}$$

$$\mu_a(t) = \begin{cases} 1, \; if \; t = m_i, \\ \frac{t - l_0}{m_i - l_0}, \; if \; l_o < t < m_i, \\ \frac{u_p - t}{u_p - m_i}, \; if \; m_i < t < u_p, \\ 0, \; otherwise. \end{cases} \tag{2}$$

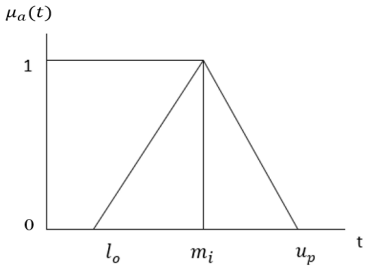

Figure 3. Triangular fuzzy numbers.

(l_o, m_i, u_p) is depicted as a TFN in a quantitative manner, and experts have assigned ratings to the factors affecting the values using the scale shown in Table 2.

In the conversion of numeric values into TFNs, Equations (3)–(6) are used [51–53], which are designated as $(l_{o_{jk}}, m_{i_{jk}}, u_{p_{jk}})$ where, $l_{o_{jk}}$ is lower, $m_{i_{jk}}$ is middle and $u_{p_{jk}}$ is a higher value. In Equations (3)–(6), R_{jkz} indicates the relative importance of the values between two factors, which is given by security expert z, where j and k signify a pair of factors being decided by security experts. n_{jk} is evaluated for a specific comparison on the basis of geometric mean, which is given by experts using TFN $\left[n_{jk}\right]$, where lower, middle, and upper values are as $l_{o_{jk}} \leq m_{i_{jk}} \leq u_{p_{jk}}$. Additionally, TFN$[n_{jk}]$ is recognized by Equation (3).

$$n_{jk} = (l_{o_{jk}}, m_{i_{jk}}, u_{p_{jk}}) \tag{3}$$

$$l_{o_{jk}} = \min(R_{jkz}) \tag{4}$$

$$m_{i_{jk}} = (R_{jk1}, R_{jk2}, R_{jk3})^{\frac{1}{t}} \tag{5}$$

$$and\ u_{p_{jk}} = \max(R_{jkz}) \tag{6}$$

Table 2. TFN scale.

Saaty Scale Definition	Fuzzy Triangle Scale	
1	Equally important	(1, 1, 1)
3	Weakly important	(2, 3, 4)
5	Fairly important	(4, 5, 6)
7	Strongly important	(6, 7, 8)
9	Absolutely important	(9, 9, 9)
2	Intermittent values between two adjacent scales	(1, 2, 3)
4		(3, 4, 5)
6		(5, 6, 7)
8		(7, 8, 9)

Furthermore, with the help of Equation (7), a fuzzy pair-wise comparison matrix in the form of an $m \times m$ matrix is generated after obtaining the TFN values for each pair of comparisons.

$$\widetilde{P^z} = \begin{bmatrix} \widetilde{x^z_{11}} & \widetilde{x^z_{12}} \ldots\ldots & \widetilde{x^z_{1m}} \\ \widetilde{x^z_{21}} & \widetilde{x^z_{22}} \ldots\ldots & \widetilde{x^z_{2m}} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots \\ \widetilde{x^z_{m1}} & \widetilde{x^z_{m2}} \ldots\ldots & \widetilde{x^z_{mm}} \end{bmatrix} \tag{7}$$

where $\widetilde{x^z_{jk}}$ represents the z^{th} decision maker's preference of the j^{th} criteria over the k^{th} criteria. When there are multiple decision-makers, Equation (8) is used to calculate the average of each decision-maker's preferences.

$$\widetilde{x_{jk}} = \sum_1^d \widetilde{x^z_{jk}} \tag{8}$$

After that, with the help of Equation (9) and based on average preferences, pair-wise comparison matrices are updated for all the factors in the hierarchy.

$$\widetilde{P} = \begin{bmatrix} \widetilde{x_{11}} & \ldots\ldots\ldots & \widetilde{x_{1m}} \\ \widetilde{x_{21}} & \ldots\ldots\ldots & \widetilde{x_{2m}} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots \\ \widetilde{x_{m1}} & \ldots\ldots\ldots & \widetilde{x_{mm}} \end{bmatrix} \tag{9}$$

The fuzzy geometrical mean and fuzzy weights of each factor are then described using the geometrical mean technique, as indicated in Equation (10). After that, with the help of Equation (11), the fuzzy weight of the factor is concluded.

$$\widetilde{a_i} = \left(\prod_{i=1}^n \widetilde{x_{jk}}\right)^{1/n},\ j = \{1, 2, 3, \ldots, n\} \tag{10}$$

$$\widetilde{wt_i} = \widetilde{a_i} \otimes \left(\widetilde{a_1} \bigoplus \widetilde{a_2} \bigoplus \widetilde{a_3} \ldots\ldots \bigoplus \widetilde{a_n}\right)^{-1} \tag{11}$$

Further, with the help of Equations (12) and (13), the average and normalized weight criteria may be calculated.

$$Avg_i = \frac{\widetilde{wt_1} \oplus \widetilde{wt_2} \ldots\ldots \oplus \widetilde{wt_n}}{n} \tag{12}$$

$$N\_wt_i = \frac{Avg_i}{Avg_1 \oplus Avg_2 \oplus \ldots .. \oplus Avg_n} \tag{13}$$

Furthermore, to compute the BNP value of the fuzzy weights, the Centre of Area (COA) approach is applied for every measurement with the help of Equation (14).

$$BNP_{Wt} = \frac{\left[\left(\mathrm{u_p}wt1 - l_owt1\right) + \left(m_iwt1 - l_owt1\right)\right]}{3} + l_owt1 \tag{14}$$

4.2. Fuzzy TOPSIS

Fuzzy TOPSIS is one of the foremost approaches for determining the ideal solution among analogous alternatives. Besides this, it can be preferred to automate the procedure and eliminate confusion and ambiguity in the selected criteria. This is a linear weighting technique that was first put forth by Chen and Hwang (1992), citing Hwang and Yoon (1981). TOPSIS contemplates the MCDM view with m choices as a geometric arrangement with m points in the n-dimensional space of factors. The method utilized in this study is based on the assumption, i.e., the maximum and minimum ideal solutions, respectively.

To induce an ideal solution, the selected alternative must have the closest and farthest distance from the Fuzzy Positive Ideal Solution (FPIS) and Fuzzy Negative Ideal Solution (FNIS) [54]. Shadbegian and Gray stated that security experts might encounter some issues with the allocation of specific performance ratings of any alternative on the basis of factors. The relevant phases of the Fuzzy AHP-TOPSIS method are presented in the flow chart below (see Figure 4).

This procedure allocates fuzzy numbers in place of specific numbers to represent the relative significance of a factor for consistency with real-world fuzzy surroundings. Furthermore, the fuzzy AHP-TOPSIS technique is well suited to solve group decision-making problems in fuzzy contexts. Figure 4 illustrates the comprehensive procedure for achieving weights as well as the estimation of the viability of the fuzzy AHP-TOPSIS method. Firstly, the researcher determines the weights of the evaluation factors. With the help of Equations (1)–(14), the current research applies the fuzzy AHP process to derive fuzzy weight. In addition, a fuzzy decision matrix is created by researchers with the help of Table 3 and Equation (15), and relevant linguistic variables are chosen as alternatives for the criterion.

$$\widetilde{X} = \begin{array}{c} \\ P_1 \\ \vdots \\ P_m \end{array} \begin{array}{c} \begin{array}{cccc} Q_1 & \ldots\ldots & Q_n \end{array} \\ \begin{bmatrix} \widetilde{y_{11}} & \ldots\ldots\ldots & \widetilde{y_{1n}} \\ \widetilde{y_{21}} & \ldots\ldots\ldots & \widetilde{y_{2n}} \\ \ldots.. & \ldots.. & \ldots.. \\ \widetilde{y_{m1}} & \ldots\ldots\ldots & \widetilde{y_{mn}} \end{bmatrix} \end{array} \tag{15}$$

where $\widetilde{y}_{jk} = \frac{1}{Z}(\widetilde{y}^1_{jk} \ldots \oplus \widetilde{y}^z_{jk} \oplus \ldots\ldots \widetilde{y}^Z_{jk})$, and $\widetilde{y}^z_{jk}$ is the performance rating of the alternative P_j with respect to factor Q_k estimated by the zth practitioner and $\widetilde{y}^z_{jk} = (l_{0^z_{jk}}, m_{i^z_{jk}}, u_{p^z_{jk}})$. With the help of Equation (16), the fuzzy decision matrix is normalized and represented by $\widetilde{D}$. After that, with the help of Equation (17), the normalization process can be achieved.

$$\widetilde{y}^z_{jk} = \left(l_{0^z_{jk}}, m_{i^z_{jk}}, u_{p^z_{jk}}\right), \widetilde{D} = \left[\widetilde{a}_{jk}\right]_{m\times n} \tag{16}$$

$$\widetilde{a}_{jk} = \left(\frac{l_{o_{jk}}}{u_{p_k}^+}, \frac{m_{i_{jk}}}{u_{p_k}^+}, \frac{u_{p_{jk}}}{u_{p_k}^+}\right), \; u_{p_k}^+ = max(u_{p_{jk}}), \; j = \{1,2,\ldots,n\}; \; \mathrm{k} = \{1,2,\ldots,\mathrm{n}\} \tag{17}$$

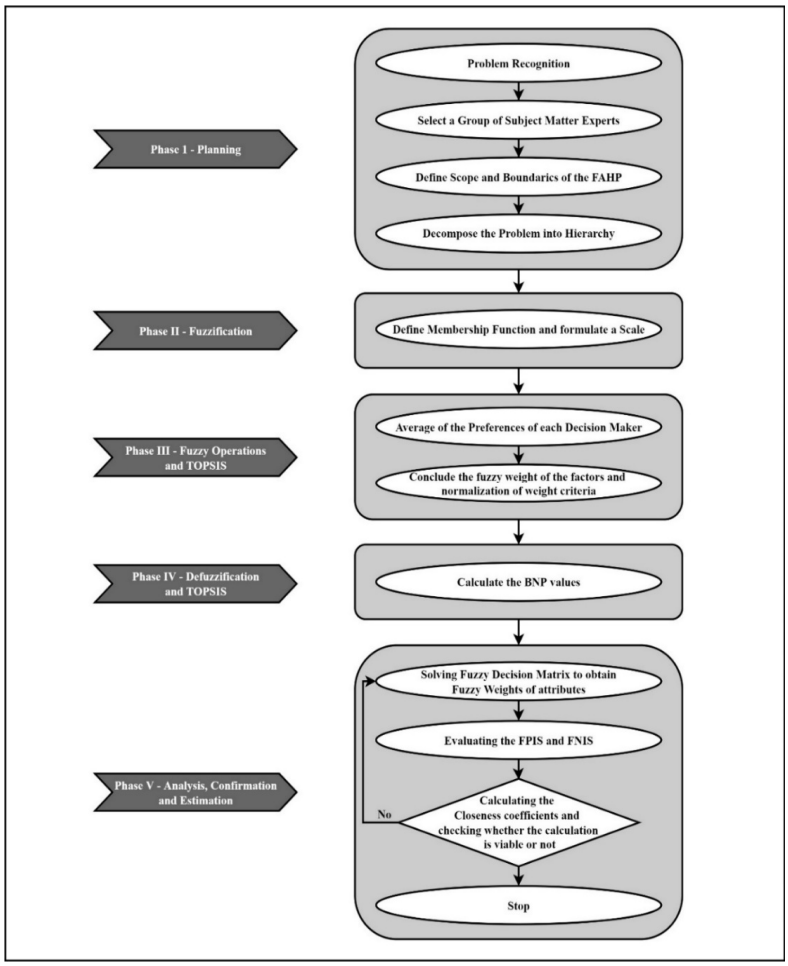

Figure 4. Flow chart of the fuzzy AHP-TOPSIS method.

Table 3. Linguistic scales for the rating.

Linguistic Variable	Corresponding Triangular Fuzzy Number
Very Poor (VP)	(0, 1, 3)
Poor (P)	(1, 3, 5)
Fair (F)	(3, 5, 7)
Good (G)	(5, 7, 9)
Very Good (VG)	(7, 9,10)

Alternatively, we can set the best-desired level $u_{p_k^+}$ equal to 1; otherwise, the worst is 0. The normalized $\widetilde{a}_{jk}$ continues to be a TFN. The decision matrix $(\widetilde{D}_w)$ is normalized by weighted fuzzy numbers and is quantified through Equation (18).

$$\widetilde{D}_w = \left[\widetilde{b}_{jk}\right]_{m\times n}, \;\; j = \{1, 2, \ldots, m\}; \;\; k = \{1, 2, \ldots, n\} \tag{18}$$

where $\widetilde{b}_{jk} = \widetilde{a}_{jk} \otimes \widetilde{w}t_{jk}$, are normalized to the positive TFN, and their ranges belong to the closed interval [0, 1]. Thereafter, FPIS A_s^+ (aspiration levels) and FNIS A_s^- (the worst levels) are computed for each criterion to address maximum benefit criteria while minimizing cost criteria, as shown in Equations (19) and (20).

$$A_s^+ = \left(\widetilde{b}_1^+, \ldots\ldots \widetilde{b}_k^+, \ldots\ldots \widetilde{b}_n^+\right) \tag{19}$$

$$A_s^- = \left(\tilde{b}_1^-, \ldots\ldots \tilde{b}_k^-, \ldots\ldots \tilde{b}_n^-\right) \tag{20}$$

where $\tilde{b}_{jk}^+ = (1,1,1) \otimes \tilde{wt}_{jk} = (Lwt_k, Mwt_k, Hwt_k)$ and $\tilde{b}_{jk}^- = (0,0,0), k = \{1,2,3,4,\ldots,n\}$. For calculating the distance of each alternative from FPIS and FNIS, the distances ($\tilde{Dis}_j^+$ *and* $\tilde{Dis}_j^-$) of each alternative from A_s^+ *and* A_s^- can be estimated using the area compensation technique, as elucidated in Equations (21) and (22).

$$\tilde{Dis}_j^+ = \sum_{k=1}^{n} Dis\left(\tilde{b}_{jk}, \tilde{b}_{jk}^+\right),\ j = \{1,2,\ldots m\};\ \ k = \{1,2,\ldots,n\} \tag{21}$$

$$\tilde{Dis}_j^- = \sum_{k=1}^{n} Dis\left(\tilde{b}_{jk}, \tilde{b}_{jk}^-\right),\ j = \{1,2,\ldots m\};\ \ k = \{1,2,\ldots,n\} \tag{22}$$

In addition, researchers discovered the closeness coefficients (i.e., relative gaps–degree) and generated alternatives for the achievement of aspiration levels in each factor. To improve the alternatives, Chou et al. proposed that $\tilde{QQ}_j$ is cleared to evaluate the fuzzy gaps–degree on the basis of the fuzzy closeness coefficients [51]. The similarity to the ideal solution is determined after evaluating the $\tilde{Dis}_j^+$ and $\tilde{Dis}_j^-$ of each alternative and is depicted in Equation (23).

$$\tilde{QQ}_j = \frac{\tilde{x}_j^-}{\tilde{x}_j^+ + \tilde{x}_j^-} = 1 - \frac{\tilde{x}_j^+}{\tilde{x}_j^+ + \tilde{x}_j^-},\ \ j = \{1,2,3,\ldots,m\} \tag{23}$$

4.3. Empirical Data Analysis and Results

Generally, qualitative assessment seems to be suitable for the assessment of long-term security. It is quite difficult to perform a qualitative assessment of healthcare web application security. Security strategy is prepared on the basis of results drawn from global collaborative activities. In recent years, security professionals have amassed a large number of security policies [52]. Several firms are currently adopting high-end security healthcare web applications. The impact of security attributes on healthcare web applications plays a crucial role in ensuring security [55–60]. This study identifies various security attributes and risk factors. For the purpose of assessment, the identified security attributes and risk factors are linked together to establish a relationship among them. For assessment, T11, T12, and T13 are represented as the attributes of confidentiality at level 2 with respect to security. T21, T22, T23, T24, T25, T26, T27, and T28 are represented as the attributes of integrity at level 2 with respect to security. T31 is represented as the attribute of availability at level 2 with respect to security. T41, T42, T43, and T44 are represented as the attributes of access control at level 2 with respect to security. T51 and T52 are represented as the attributes of authentication at level 2 with respect to security. This study uses the opinions of 70 professionals from academia and industry in order to compile the data. The estimation of security via fuzzy AHP-TOPSIS has been assessed by using Equations (1)–(23) as follows:

The researcher converted the linguistic values into numeric values as well as aggregated TFN values by using Table 2 and Equations (1)–(6). Additionally, Equation (7) was used to create the pair-wise comparison matrixes for level 1 attributes, as shown in Table 4. Similarly, Tables 5–8 show the fuzzy pair-wise comparison matrixes through the hierarchy at level 2.

Table 4. Fuzzy aggregated pair-wise comparison matrix at level 1.

	T1	T2	T3	T4	T5
T1	1.0000, 1.0000, 1.0000	0.3127, 0.4395, 0.6252	0.8733, 0.9012, 0.9465	0.2261, 0.2928, 0.4166	0.2580, 0.3386, 0.5055
T2	-	1.0000, 1.0000, 1.0000	2.0451, 3.1699, 4.2330	0.2665, 0.3657, 0.5911	0.6906, 1.0059, 1.5117
T3	-	-	1.0000, 1.0000, 1.0000	0.3667, 0.5251, 0.9659	0.3604, 0.5220, 0.8074
T4	-	-	-	1.0000, 1.0000, 1.0000	0.8960, 1.1486, 1.3903
T5	-	-	-	-	1.0000, 1.0000, 1.0000

Table 5. Fuzzy aggregated pair-wise comparison matrix at level 2 for confidentiality.

	T11	T12	T13
T11	1.0000, 1.0000, 1.0000	0.6951, 0.9501, 1.3457	1.1048, 1.4380, 1.6906
T12	-	1.0000, 1.0000, 1.0000	1.1902, 1.5820, 2.1497
T13	-	-	1.0000, 1.0000, 1.0000

Table 6. Fuzzy aggregated pair-wise comparison matrix at level 2 for integrity.

	T21	T22	T23	T24	T25	T26	T27	T28
T21	1.0000, 1.0000, 1.0000	1.1121, 1.5105, 1.9331	0.4891, 0.6301, 1.5241	0.4101, 0.5744, 1.6523	0.2210, 0.2870, 0.4152	0.3141, 0.4611, 0.8712	0.6574, 1.1652, 1.6882	0.2442, 0.3234, 0.4865
T22	-	1.0000, 1.0000, 1.0000	0.5704, 0.6654, 0.8021	0.3045, 0.3934, 0.5661	0.2678, 0.3523, 0.5175	0.1668, 0.1968, 0.2531	0.3938, 0.5745, 1.0564	0.1695, 0.2135, 0.2751
T23	-	-	1.0000, 1.0000, 1.0000	1.1141, 1.3195, 1.5517	0.3112, 0.4311, 0.8112	0.8441, 0.8711, 1.1253	1.2611, 1.8245, 2.4312	0.1711, 0.2044, 0.2641
T24	-	-	-	1.0000, 1.0000, 1.0000	0.5384, 0.9147, 1.5835	0.6082, 1.0591, 1.6828	0.7545, 1.3462, 1.9615	0.6785, 0.7474, 0.8725
T25	-	-	-	-	1.0000, 1.0000, 1.0000	0.4147, 0.6344, 1.1711	0.9474, 1.1095, 1.2457	0.2511, 0.3344, 0.5114
T26	-	-	-	-	-	1.0000, 1.0000, 1.0000	1.8884, 2.5515, 3.1694	0.8112, 1.0352, 1.3166
T27	-	-	-	-	-	-	1.0000, 1.0000, 1.0000	0.2136, 0.2574, 0.3194
T28	-	-	-	-	-	-	-	1.0000, 1.0000, 1.0000

Table 7. Fuzzy aggregated pair-wise comparison matrix at level 2 for access control.

	T41	T42	T43	T44
T41	1.0000, 1.0000, 1.0000	1.0784, 1.5991, 2.1134	0.8244, 1.1125, 1.6144	0.5674, 0.7132, 0.8734
T42	-	1.0000, 1.0000, 1.0000	0.3237, 0.4488, 0.6052	0.2588, 0.3174, 0.4164
T43	-	-	1.0000, 1.0000, 1.0000	0.6667, 1.0564, 1.5444
T44	-	-	-	1.0000, 1.0000, 1.0000

Table 8. Fuzzy aggregated pair-wise comparison matrix at level 2 for authentication.

	T51	T52
T51	1.0000, 1.0000, 1.0000	0.6664, 1.0506, 1.5428
T52	-	1.0000, 1.0000, 1.0000

The researcher calculated the fuzzy weights of factors with the help of Equations (8)–(10), and the weight of each element is calculated using Equations (11)–(13). Additionally, the BNP values (i.e., best non-fuzzy performance) of each attribute are calculated via Equation (14). Thereafter, the weights for the continuing attributes may be determined and shown in Tables 9–13, which depict the local and dependent weight of attributes according to Figure 4. Table 14 shows the global weight of every attribute of security.

Table 9. Combined pair-wise comparison matrix at level 1.

	T1	T2	T3	T4	T5	Weight
T1	1.0000	2.5540	1.7017	2.4274	0.5909	0.2391
T2	0.3914	1.0000	0.7964	0.9706	0.2070	0.0950
T3	0.5876	1.2556	1.0000	1.0563	0.2532	0.1199
T4	0.4121	1.0236	0.9467	1.0000	0.2357	0.1032
T5	1.6686	4.8239	3.9495	4.2427	1.0000	0.4426
C.R. = 0.0025						

Table 10. Combined pair-wise comparison matrix at level 2 for confidentiality.

	T11	T12	T13	Weight
T11	1.0000	0.9853	1.3577	0.3610
T12	1.0149	1.0000	1.6261	0.3872
T13	0.7365	0.6147	1.0000	0.2516
C.R. = 0.0026				

Table 11. Combined pair-wise comparison matrix at level 2 for integrity.

	T21	T22	T23	T24	T25	T26	T27	T28	Weight
T21	1.0000	1.4912	0.6912	0.6418	0.3114	0.5206	1.1697	0.3438	0.0734
T22	0.6741	1.0000	0.6778	0.4104	0.3724	0.2033	0.6497	0.2150	0.0496
T23	1.4474	1.4771	1.0000	1.2977	0.4935	0.8502	1.8364	0.2147	0.1032
T24	1.5644	2.4138	0.7711	1.0000	0.9631	1.1024	1.3511	0.7319	0.1272
T25	3.3141	2.6852	2.0263	1.0378	1.0000	0.7172	1.1028	0.4358	0.1407
T26	1.8981	4.9188	1.1737	0.9071	1.3943	1.0000	2.3852	1.0473	0.1731
T27	0.8551	1.5396	0.5444	0.7404	0.9067	0.4192	1.0000	0.2621	0.0760
T28	2.9154	4.6484	4.6729	1.3663	2.2989	0.9548	3.8153	1.0000	0.2563
C.R. = 0.0330									

Table 12. Combined pair-wise comparison matrix at level 2 for access control.

	T41	T42	T43	T44	Weight
T41	1.0000	1.5973	1.1648	0.7168	0.2543
T42	0.6262	1.0000	0.4561	0.3274	0.1301
T43	0.8585	2.1922	1.0000	1.0804	0.2829
T44	1.3951	3.0544	0.9256	1.0000	0.3325
CR = 0.0187					

Table 13. Combined pair-wise comparison matrix at level 2 for authentication.

	T51	T52	Weight
T51	1.0000	1.0804	0.5193
T52	0.9256	1.0000	0.4806
CR = 0.0000			

Now, the researcher must figure out the impact of risk factors on altering preferences with respect to criteria. Ten successive healthcare web applications (i.e., HWA1, HWA2, HWA3, HWA4, HWA5, HWA6, HWA7, HWA8, HWA9, and HWA10) from the local hospitals of Uttar Pradesh, India, were taken to estimate the security risk. The researcher gathered input on the technological data with the help of Table 3 for all 10 alternatives, as depicted in Table 15. The researcher assessed the normalized fuzzy decision matrix, as shown in Table 16, by using Equations (15)–(18), and evaluated the weighted normalized fuzzy decision matrix, as shown in Table 17. Additionally, the researcher assessed the satisfaction degree and gap degree by using Equations (22) and (23), as depicted in Table 18.

Table 14. Final weights of hierarchy.

Characteristics of Level 1	Local Weights of Level 1	Characteristics of Level 2	Local Weights of Level 2	Global Weights of Level 2
T1	0.2391	T11	0.3610	0.0863
		T12	0.3872	0.0926
		T13	0.2516	0.0601
T2	0.0950	T21	0.0734	0.0069
		T22	0.0496	0.0047
		T23	0.1032	0.0098
		T24	0.1272	0.0120
		T25	0.1407	0.0133
		T26	0.1731	0.0164
		T27	0.0760	0.0072
		T28	0.2563	0.0243
T3	0.1199	T31	-	0.1199
T4	0.1032	T41	0.2543	0.0262
		T42	0.1301	0.0134
		T43	0.2829	0.0292
		T44	0.3325	0.0343
T5	0.4426	T51	0.5193	0.2298
		T52	0.4806	0.2127

Finally, the obtained global weight of factors from fuzzy AHP is considered as input data for the fuzzy TOPSIS approach, which proliferates a rank for alternatives. Now, the performance may be tested by using fuzzy AHP-TOPSIS. The determined performance of ten healthcare web application alternatives is as follows: HWA1, HWA7, HWA10, HWA4, HWA2, HWA3, HWA5, HWA9, HWA8, and HWA6. According to the findings of this study, HWA1 produced the finest result (see Table 18 and Figure 5).

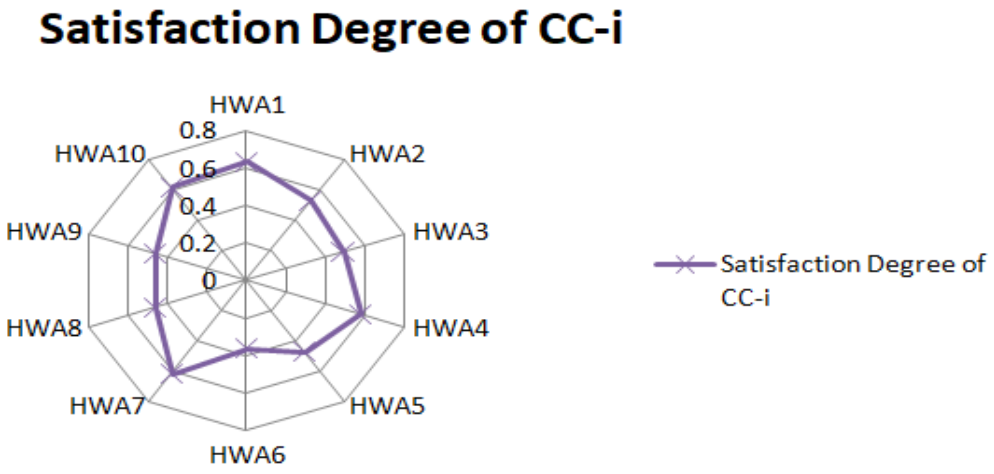

Figure 5. Satisfaction degree of CC-i.

Table 15. Subjective cognition results of evaluators in linguistic terms.

	HWA1	HWA2	HWA3	HWA4	HWA5	HWA6	HWA7	HWA8	HWA9	HWA10
	4.0900,	3.0900,	5.1800,	4.0900,	3.0900,	5.1800,	4.0900,	3.0900,	5.1800,	4.8200,
T11	6.0900,	5.0000,	7.1800,	6.0900,	5.0000,	7.1800,	6.0900,	5.0000,	7.1800,	6.8200,
	7.9100	6.8200	8.9100	7.9100	6.8200	8.9100	7.9100	6.8200	8.9100	8.5500
	4.8200,	2.0900,	5.1800,	4.8200,	2.0900,	5.1800,	4.8200,	2.0900,	2.0900,	4.0900,
T12	6.8200,	3.9100,	7.1800,	6.8200,	3.9100,	7.1800,	6.8200,	3.9100,	3.9100,	6.0900,
	8.5500	5.8200	8.9100	8.5500	5.8200	8.9100	8.5500	5.8200	5.8200	7.9100
	4.0900,	4.0900,	3.0900,	5.1800,	4.0900,	3.0900,	5.1800,	4.0900,	3.0900,	5.1800,
T13	6.0900,	6.0900,	5.0000,	7.1800,	6.0900,	5.0000,	7.1800,	6.0900,	5.0000,	7.1800,
	7.9100	7.9100	6.8200	8.9100	7.9100	6.8200	8.9100	7.9100	6.8200	8.9100
	2.4500,	4.8200,	2.0900,	5.1800,	4.8200,	2.0900,	5.1800,	4.8200,	2.0900,	2.0900,
T21	4.2700,	6.8200,	3.9100,	7.1800,	6.8200,	3.9100,	7.1800,	6.8200,	3.9100,	3.9100,
	6.2700	8.5500	5.8200	8.9100	8.5500	5.8200	8.9100	8.5500	5.8200	5.8200
	4.0900,	4.0900,	3.0900,	5.1800,	4.0900,	3.0900,	5.1800,	4.0900,	3.0900,	3.0900,
T22	6.0900,	6.0900,	5.0000,	7.1800,	6.0900,	5.0000,	7.1800,	6.0900,	5.0000,	5.0000,
	7.9100	7.9100	6.8200	8.9100	7.9100	6.8200	8.9100	7.9100	6.8200	6.8200
	4.8200,	4.8200,	2.0900,	5.1800,	4.8200,	2.0900,	5.1800,	4.8200,	2.0900,	4.8200,
T23	6.8200,	6.8200,	3.9100,	7.1800,	6.8200,	3.9100,	7.1800,	6.8200,	3.9100,	6.8200,
	8.5500	8.5500	5.8200	8.9100	8.5500	5.8200	8.9100	8.5500	5.8200	8.5500
	4.0900,	4.0900,	2.3600,	2.0900,	4.0900,	2.3600,	2.0900,	4.0900,	2.3600,	4.0900,
T24	6.0900,	6.0900,	4.2700,	3.9100,	6.0900,	4.2700,	3.9100,	6.0900,	4.2700,	6.0900,
	7.9100	7.9100	6.2700	5.8200	7.9100	6.2700	5.8200	7.9100	6.2700	7.9100
	5.1800,	4.8200,	4.0900,	3.0900,	5.1800,	4.0900,	3.0900,	5.1800,	4.0900,	3.0900,
T25	7.1800,	6.8200,	6.0900,	5.0000,	7.1800,	6.0900,	5.0000,	7.1800,	6.0900,	5.0000,
	8.9100	8.5500	7.9100	6.8200	8.9100	7.9100	6.8200	8.9100	7.9100	6.8200
	4.8200,	2.0900,	4.8200,	2.0900,	5.1800,	4.8200,	2.0900,	5.1800,	4.8200,	2.0900,
T26	6.8200,	3.9100,	6.8200,	3.9100,	7.1800,	6.8200,	3.9100,	7.1800,	6.8200,	3.9100,
	8.5500	5.8200	8.5500	5.8200	8.9100	8.5500	5.8200	8.9100	8.5500	5.8200
	4.0900,	4.0900,	3.0900,	5.1800,	4.0900,	3.0900,	5.1800,	4.0900,	3.0900,	2.3600,
T27	6.0900,	6.0900,	5.0000,	7.1800,	6.0900,	5.0000,	7.1800,	6.0900,	5.0000,	4.2700,
	7.9100	7.9100	6.8200	8.9100	7.9100	6.8200	8.9100	7.9100	6.8200	6.2700
	5.1800,	4.0900,	3.0900,	5.1800,	4.0900,	3.0900,	5.1800,	4.0900,	3.0900,	5.1800,
T28	7.1800,	6.0900,	5.0000,	7.1800,	6.0900,	5.0000,	7.1800,	6.0900,	5.0000,	7.1800,
	8.9100	7.9100	6.8200	8.9100	7.9100	6.8200	8.9100	7.9100	6.8200	8.9100
	2.4500,	4.8200,	2.0900,	5.1800,	4.8200,	2.0900,	5.1800,	4.8200,	2.0900,	2.0900,
T31	4.2700,	6.8200,	3.9100,	7.1800,	6.8200,	3.9100,	7.1800,	6.8200,	3.9100,	3.9100,
	6.2700	8.5500	5.8200	8.9100	8.5500	5.8200	8.9100	8.5500	5.8200	5.8200
	4.0900,	4.0900,	2.3600,	2.0900,	4.0900,	2.3600,	2.0900,	4.0900,	2.3600,	3.0900,
T41	6.0900,	6.0900,	4.2700,	3.9100,	6.0900,	4.2700,	3.9100,	6.0900,	4.2700,	5.0000,
	7.9100	7.9100	6.2700	5.8200	7.9100	6.2700	5.8200	7.9100	6.2700	6.8200
	4.8200,	4.0900,	3.0900,	5.1800,	4.0900,	3.0900,	5.1800,	4.0900,	3.0900,	4.8200,
T42	6.8200,	6.0900,	5.0000,	7.1800,	6.0900,	5.0000,	7.1800,	6.0900,	5.0000,	6.8200,
	8.5500	7.9100	6.8200	8.9100	7.9100	6.8200	8.9100	7.9100	6.8200	8.5500
	4.0900,	4.8200,	2.0900,	5.1800,	4.8200,	2.0900,	5.1800,	4.8200,	2.0900,	4.0900,
T43	6.0900,	6.8200,	3.9100,	7.1800,	6.8200,	3.9100,	7.1800,	6.8200,	3.9100,	6.0900,
	7.9100	8.5500	5.8200	8.9100	8.5500	5.8200	8.9100	8.5500	5.8200	7.9100
	5.1800,	4.0900,	2.3600,	2.0900,	4.0900,	2.3600,	2.0900,	4.0900,	2.3600,	5.1800,
T44	7.1800,	6.0900,	4.2700,	3.9100,	6.0900,	4.2700,	3.9100,	6.0900,	4.2700,	7.1800,
	8.9100	7.9100	6.2700	5.8200	7.9100	6.2700	5.8200	7.9100	6.2700	8.9100
	2.4500,	2.0900,	4.0900,	2.0900,	2.4500,	2.0900,	2.4500,	2.0900,	4.0900,	2.0900,
T51	4.2700,	3.9100,	6.0900,	3.9100,	4.2700,	3.9100,	4.2700,	3.9100,	6.0900,	3.9100,
	6.2700	5.8200	7.9100	5.8200	6.2700	5.8200	6.2700	5.8200	7.9100	5.8200

Table 16. The normalized fuzzy decision matrix.

	HWA1	HWA2	HWA3	HWA4	HWA5	HWA6	HWA7	HWA8	HWA9	HWA10
T11	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900	0.5900, 0.8000, 0.9700	0.5200, 0.7400, 0.9400	0.5200, 0.7400, 0.9400	0.5100, 0.7200, 0.9000
T12	0.5200, 0.7400, 0.9400	0.4200, 0.6900, 0.9900	0.5000, 0.7100, 0.8900	0.5200, 0.7400, 0.9400	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900
T13	0.5000, 0.7100, 0.8900	0.5200, 0.7400, 0.9400	0.4200, 0.6900, 0.9900	0.5900, 0.8000, 0.9700	0.5200, 0.7400, 0.9400	0.4200, 0.6900, 0.9900	0.5000, 0.7100, 0.8900	0.5200, 0.7400, 0.9400	0.4200, 0.6900, 0.9900	0.5000, 0.7100, 0.8900
T21	0.4200, 0.6900, 0.9900	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900	0.5900, 0.8000, 0.9700	0.1600, 0.4200, 0.7200	0.4200, 0.6900, 0.9900
T22	0.5200, 0.7400, 0.9400	0.5200, 0.7400, 0.9400	0.4200, 0.6900, 0.9900	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900	0.5900, 0.8000, 0.9700
T23	0.6000, 0.8100, 1.0000	0.5200, 0.7400, 0.9400	0.5200, 0.7400, 0.9400	0.5200, 0.7400, 0.9400	0.4200, 0.6900, 0.9900	0.5000, 0.7100, 0.8900	0.5200, 0.7400, 0.9400	0.4200, 0.6900, 0.9900	0.5000, 0.7100, 0.8900	0.5200, 0.7400, 0.9400
T24	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900	0.5900, 0.8000, 0.9700	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.4300, 0.6400, 0.8600
T25	0.5200, 0.7400, 0.9400	0.4200, 0.6900, 0.9900	0.5000, 0.7100, 0.8900	0.5200, 0.7400, 0.9400	0.4200, 0.6900, 0.9900	0.5000, 0.7100, 0.8900	0.5200, 0.7400, 0.9400	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900	0.5900, 0.8000, 0.9700
T26	0.4200, 0.6900, 0.9900	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5200, 0.7400, 0.9400	0.4200, 0.6900, 0.9900	0.5000, 0.7100, 0.8900	0.5200, 0.7400, 0.9400	0.4200, 0.6900, 0.9900	0.5000, 0.7100, 0.8900	0.5200, 0.7400, 0.9400
T27	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900	0.5900, 0.8000, 0.9700	0.5200, 0.7400, 0.9400	0.1600, 0.4200, 0.7200	0.5700, 0.7800, 0.9600
T28	0.5200, 0.7400, 0.9400	0.4200, 0.6900, 0.9900	0.5000, 0.7100, 0.8900	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900	0.5900, 0.8000, 0.9700
T31	0.5200, 0.7400, 0.9400	0.5000, 0.7100, 0.8900	0.5200, 0.7400, 0.9400	0.5200, 0.7400, 0.9400	0.4200, 0.6900, 0.9900	0.5000, 0.7100, 0.8900	0.5200, 0.7400, 0.9400	0.4200, 0.6900, 0.9900	0.5000, 0.7100, 0.8900	0.5200, 0.7400, 0.9400
T41	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900	0.5900, 0.8000, 0.9700	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900
T42	0.5200, 0.7400, 0.9400	0.4200, 0.6900, 0.9900	0.5000, 0.7100, 0.8900	0.5200, 0.7400, 0.9400	0.5200, 0.7400, 0.9400	0.4200, 0.6900, 0.9900	0.5000, 0.7100, 0.8900	0.5200, 0.7400, 0.9400	0.4200, 0.6900, 0.9900	0.5000, 0.7100, 0.8900
T43	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900	0.5900, 0.8000, 0.9700	0.5200, 0.7400, 0.9400	0.4200, 0.6900, 0.9900	0.4300, 0.6400, 0.8600
T44	0.5200, 0.7400, 0.9400	0.4200, 0.6900, 0.9900	0.5000, 0.7100, 0.8900	0.5200, 0.7400, 0.9400	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900
T51	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900	0.5900, 0.8000, 0.9700	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5000, 0.7100, 0.8900
T52	0.5200, 0.7400, 0.9400	0.4200, 0.6900, 0.9900	0.5000, 0.7100, 0.8900	0.5200, 0.7400, 0.9400	0.5200, 0.7400, 0.9400	0.4200, 0.6900, 0.9900	0.5000, 0.7100, 0.8900	0.5200, 0.7400, 0.9400	0.4200, 0.6900, 0.9900	0.5000, 0.7100, 0.8900

Table 17. The weighted normalized fuzzy decision matrix.

	HWA1	HWA2	HWA3	HWA4	HWA5	HWA6	HWA7	HWA8	HWA9	HWA10
T11	0.0000, 0.0020, 0.0090	0.0020, 0.0090, 0.0300	0.0050, 0.0160, 0.0480	0.0010, 0.0050, 0.0180	0.0020, 0.0070, 0.0240	0.0050, 0.0160, 0.0480	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090	0.0020, 0.0070, 0.0220	0.0020, 0.0070, 0.0240
T12	0.0040, 0.0140, 0.0440	0.0030, 0.0120, 0.0410	0.0020, 0.0100, 0.0370	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090	0.0020, 0.0090, 0.0300	0.0050, 0.0160, 0.0480	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090	0.0020, 0.0070, 0.0220
T13	0.0040, 0.0140, 0.0440	0.0030, 0.0120, 0.0420	0.0010, 0.0050, 0.0190	0.0030, 0.0110, 0.0360	0.0040, 0.0140, 0.0440	0.0030, 0.0120, 0.0410	0.0000, 0.0020, 0.0090	0.0020, 0.0090, 0.0300	0.0050, 0.0160, 0.0480	0.0010, 0.0050, 0.0180
T21	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090	0.0020, 0.0070, 0.0220	0.0050, 0.0160, 0.0480	0.0040, 0.0140, 0.0440	0.0030, 0.0120, 0.0420	0.0040, 0.0140, 0.0440	0.0030, 0.0120, 0.0410	0.0020, 0.0100, 0.0370	0.0010, 0.0050, 0.0180
T22	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090	0.0020, 0.0070, 0.0220	0.0020, 0.0070, 0.0240	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090	0.0040, 0.0140, 0.0440	0.0030, 0.0120, 0.0420	0.0010, 0.0050, 0.0190	0.0030, 0.0110, 0.0360
T23	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090	0.0050, 0.0160, 0.0480	0.0010, 0.0050, 0.0180	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090	0.0020, 0.0070, 0.0220	0.0050, 0.0160, 0.0480
T24	0.0000, 0.0020, 0.0090	0.0020, 0.0090, 0.0300	0.0050, 0.0160, 0.0480	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090	0.0020, 0.0090, 0.0300	0.0050, 0.0160, 0.0480	0.0010, 0.0050, 0.0180	0.0020, 0.0070, 0.0220	0.0020, 0.0070, 0.0240
T25	0.0040, 0.0140, 0.0440	0.0030, 0.0120, 0.0410	0.0020, 0.0100, 0.0370	0.0010, 0.0050, 0.0180	0.0040, 0.0140, 0.0440	0.0030, 0.0120, 0.0410	0.0020, 0.0100, 0.0370	0.0010, 0.0050, 0.0180	0.0050, 0.0160, 0.0480	0.0010, 0.0050, 0.0180
T26	0.0040, 0.0140, 0.0440	0.0030, 0.0120, 0.0420	0.0010, 0.0050, 0.0190	0.0030, 0.0110, 0.0360	0.0040, 0.0140, 0.0440	0.0030, 0.0120, 0.0420	0.0010, 0.0050, 0.0190	0.0030, 0.0110, 0.0360	0.0020, 0.0100, 0.0370	0.0010, 0.0050, 0.0180
T27	0.0000, 0.0020, 0.0090	0.0020, 0.0090, 0.0300	0.0050, 0.0160, 0.0480	0.0010, 0.0050, 0.0180	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090	0.0020, 0.0070, 0.0220	0.0050, 0.0160, 0.0480	0.0010, 0.0050, 0.0190	0.0030, 0.0110, 0.0360
T28	0.0040, 0.0140, 0.0440	0.0030, 0.0120, 0.0410	0.0020, 0.0100, 0.0370	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090	0.0020, 0.0090, 0.0300	0.0050, 0.0160, 0.0480	0.0010, 0.0050, 0.0180	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090
T31	0.0040, 0.0140, 0.0440	0.0030, 0.0120, 0.0420	0.0010, 0.0050, 0.0190	0.0030, 0.0110, 0.0360	0.0040, 0.0140, 0.0440	0.0030, 0.0120, 0.0410	0.0020, 0.0100, 0.0370	0.0010, 0.0050, 0.0180	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090
T41	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090	0.0020, 0.0070, 0.0220	0.0050, 0.0160, 0.0480	0.0040, 0.0140, 0.0440	0.0030, 0.0120, 0.0420	0.0000, 0.0020, 0.0090	0.0020, 0.0090, 0.0300	0.0050, 0.0160, 0.0480	0.0010, 0.0050, 0.0180
T42	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090	0.0020, 0.0070, 0.0220	0.0020, 0.0070, 0.0240	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090	0.0040, 0.0140, 0.0440	0.0030, 0.0120, 0.0410	0.0020, 0.0100, 0.0370	0.0010, 0.0050, 0.0180
T43	0.0000, 0.0020, 0.0090	0.0020, 0.0090, 0.0300	0.0050, 0.0160, 0.0480	0.0010, 0.0050, 0.0180	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090	0.0040, 0.0140, 0.0440	0.0030, 0.0120, 0.0420	0.0010, 0.0050, 0.0190	0.0030, 0.0110, 0.0360
T44	0.0040, 0.0140, 0.0440	0.0030, 0.0120, 0.0410	0.0020, 0.0100, 0.0370	0.0010, 0.0050, 0.0180	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090	0.0020, 0.0070, 0.0220	0.0050, 0.0160, 0.0480
T51	0.0040, 0.0140, 0.0440	0.0030, 0.0120, 0.0420	0.0010, 0.0050, 0.0190	0.0030, 0.0110, 0.0360	0.0030, 0.0110, 0.0360	0.0040, 0.0140, 0.0440	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090	0.0020, 0.0070, 0.0220	0.0020, 0.0070, 0.0240
T52	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090	0.0020, 0.0070, 0.0220	0.0050, 0.0160, 0.0480	0.0010, 0.0050, 0.0180	0.0040, 0.0140, 0.0440	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090	0.0050, 0.0160, 0.0480	0.0010, 0.0050, 0.0180

Table 18. Closeness coefficients to the aspired level among the different alternatives.

Alternatives (A)	di+	di−	Gap Degree of CCi+	Satisfaction Degree
HWA1	0.0454	0.0268	0.3667	0.6322
HWA2	0.0368	0.0345	0.4694	0.5224
HWA3	0.0364	0.0421	0.5838	0.4851
HWA4	0.0367	0.0259	0.4831	0.5748
HWA5	0.0401	0.0468	0.5348	0.4679
HWA6	0.0327	0.0477	0.6447	0.3597
HWA7	0.0452	0.0265	0.3961	0.6138
HWA8	0.0349	0.0433	0.5367	0.4638
HWA9	0.0390	0.0468	0.5335	0.4667
HWA10	0.0450	0.0265	0.3961	0.6130

4.4. Sensitivity Analysis

Sensitivity analysis is a threat to the validity procedure that allows security practitioners to validate their results through numerical calculations. Additionally, the threat to validity confers the idea to security experts on how various sources of outcomes may affect the proposed model. This section provides a clear perception of the effectiveness as well as the certainty of the results by altering the crucial criteria. To test the sensitivity analysis, the researcher has chosen 10 alternatives in order to implement a threat to validity. The detail of the analyzed results of the sensitivity analysis is shown in Table 19. Furthermore, a graphical representation of the sensitivity analysis is depicted in Figure 6 for easy and detailed information.

The first row of Table 19 shows the original weights of this study. The calculated results are acceptable, and this is clear from the above table that the deviation in the whole security risk factors is negligible. The results of sensitivity analysis are dependent on the weight of the security risk factors.

Table 19. Sensitivity analysis.

	HWA1	HWA2	HWA3	HWA4	HWA5	HWA6	HWA7	HWA8	HWA9	HWA10
T0	0.6322	0.5224	0.4851	0.5748	0.4679	0.3597	0.6138	0.4638	0.4667	0.6130
T11	0.6255	0.5175	0.4742	0.5694	0.4615	0.3593	0.6111	0.4552	0.4615	0.6111
T12	0.6478	0.5275	0.4872	0.5809	0.4710	0.3598	0.6161	0.4712	0.4710	0.6161
T13	0.6442	0.5330	0.4802	0.5869	0.4755	0.3613	0.6191	0.4792	0.4755	0.6191
T21	0.6352	0.7105	0.4928	0.5968	0.4663	0.3703	0.6158	0.4562	0.4663	0.6158
T22	0.7213	0.6141	0.5708	0.6554	0.5543	0.4428	0.6381	0.5487	0.5543	0.6381
T23	0.6740	0.5651	0.5260	0.6121	0.5079	0.3991	0.6508	0.4952	0.5079	0.6508
T24	0.6295	0.5272	0.4810	0.5625	0.4661	0.3541	0.6081	0.4432	0.4661	0.6081
T25	0.6250	0.5311	0.4764	0.5482	0.4659	0.3486	0.6005	0.4382	0.4659	0.6005
T26	0.6449	0.5155	0.4832	0.5769	0.4592	0.3692	0.6141	0.4642	0.4592	0.6141
T27	0.6432	0.5265	0.4847	0.5755	0.4629	0.3648	0.6141	0.4642	0.4629	0.6141
T28	0.6272	0.5025	0.4862	0.5735	0.4702	0.3552	0.6126	0.4622	0.4702	0.6126
T31	0.6196	0.4975	0.4870	0.5725	0.4735	0.3502	0.6116	0.4612	0.4735	0.6116
T41	0.7072	0.7480	0.5647	0.6712	0.5545	0.4422	0.6586	0.5547	0.5545	0.6586
T42	0.6699	0.5545	0.5232	0.6202	0.5085	0.4085	0.6581	0.5087	0.5085	0.6581
T43	0.6742	0.5615	0.5137	0.6859	0.5050	0.3998	0.5821	0.5042	0.5050	0.5821
T44	0.7292	0.6020	0.5532	0.6589	0.5460	0.4418	0.6921	0.5472	0.5460	0.6921
T51	0.5908	0.4821	0.4482	0.6065	0.4291	0.3238	0.5225	0.4050	0.4291	0.5225
T52	0.5908	0.4855	0.4407	0.5364	0.4290	0.3218	0.5761	0.4242	0.4290	0.5761

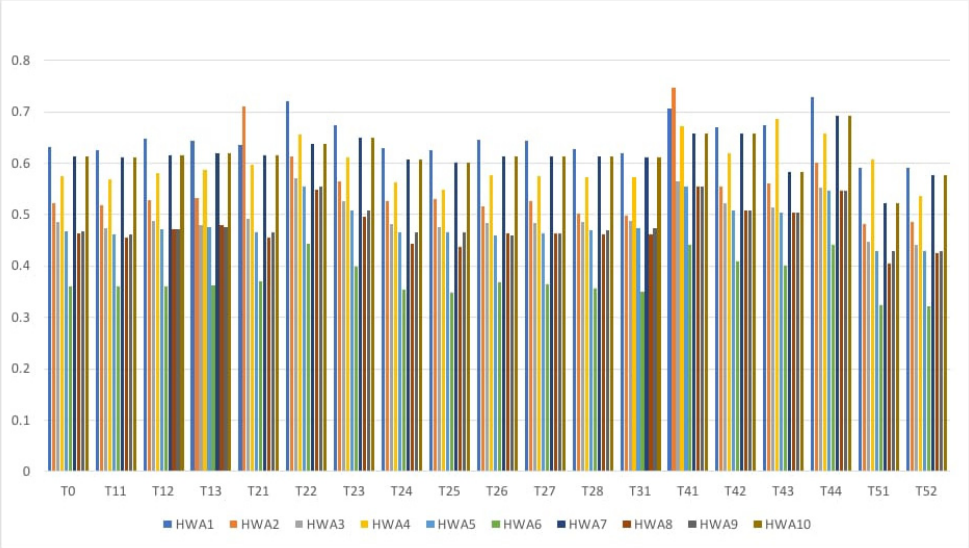

Figure 6. Graphical view of sensitivity analysis.

4.5. Comparison of the Results

MCDM approaches are used in a number of research initiatives to assess various factors and their impact on various fields. A comparison of results from different approaches may provide a considerable as well as clear perspective on computed results. In addition, comparing the outcomes of the same data through different approaches is a crucial part of scientific calculation. For comparing the results of fuzzy AHP-TOPSIS, the researcher used various techniques, including classical ANP-TOPSIS, classical AHP-TOPSIS, and the Simple Average Method.

This type of comparison illustrates the capabilities and accuracy of the chosen approach. In comparison to the preceding techniques, the results of the fuzzy AHP-TOPSIS can confer a more precise and preferable result, as shown in Table 20 and Figure 7.

Table 20. Comparison of the fuzzy AHP-TOPSIS technique.

Alternatives	Fuzzy AHP-TOPSIS	Classical AHP-TOPSIS	Classical ANP-TOPSIS	Simple Average Method
HWA1	0.6322	0.6245	0.6222	0.6202
HWA2	0.5224	0.5169	0.5035	0.5130
HWA3	0.4851	0.4731	0.4611	0.4727
HWA4	0.5748	0.5685	0.5618	0.5639
HWA5	0.4679	0.4586	0.4554	0.4575
HWA6	0.3597	0.3683	0.3958	0.3583
HWA7	0.6138	0.6161	0.6310	0.6071
HWA8	0.4638	0.4616	0.4362	0.4482
HWA9	0.4667	0.4586	0.4554	0.4575
HWA10	0.6130	0.6161	0.6310	0.6071

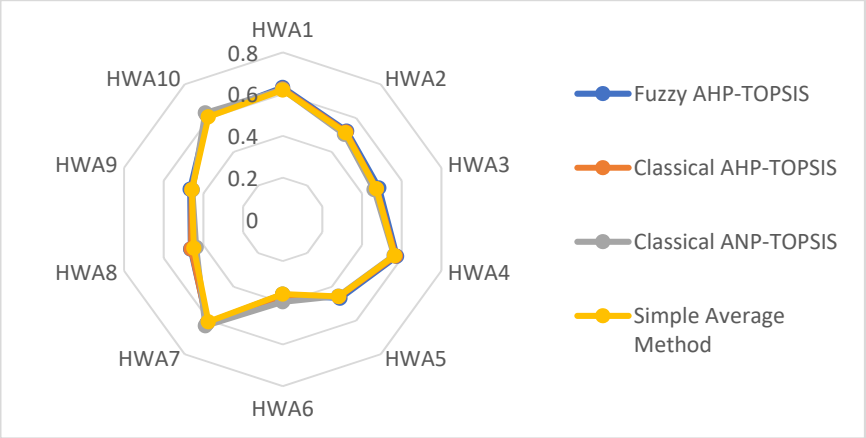

Figure 7. Comparison of results.

5. Discussion and Conclusions

The design phase is the backbone of any application irrespective of its nature and area of use. Software development organizations have shown enormous growth that urges highly secured web applications. Recent trends demonstrate that the healthcare industry has turned to deploying web applications rather than conventional forms. This dependency on technology raises security concerns as securing patients' sensitive data and hospital data becomes a critical priority. IT Industries and researchers are currently paying more attention to security. Developers should strive to develop an end-to-end framework for assessing the security risks associated with healthcare web applications to detect, evaluate, and reduce security risks as a solution to these issues. This paper proposed an integrated approach of fuzzy AHP and fuzzy TOPSIS to evaluate the security risk factors. The aim of this study was to determine the priorities based on the ranking and weighting of security attributes using the MCDM process, which demonstrates the use of an analytical hierarchical approach, through which the application becomes more secure and trustworthy. The fuzzy AHP approach can be used to prioritize the security attributes in terms of well-profiling because no attempts have been made to quantitatively prioritize and rank the security attributes that may affect the functionality of HWA security and their trade-offs. For the estimation of security risk, this combined fuzzy AHP-TOPSIS approach was applied. This proposed model was examined for ten successive healthcare web applications from the local hospitals of Uttar Pradesh, India, to determine the impact of risk factors on altering preferences with respect to criteria.

The weight and priority of risk factors are quantified by fuzzy AHP, whereas the impact of attributes on different alternatives is determined with the help of fuzzy AHP-TOPSIS. The fuzzy TOPSIS approach uses the global weight of components produced from fuzzy AHP as input to generate a rank for alternatives. The performance has now been evaluated with fuzzy AHP-TOPSIS, and with a performance score of 0.6322, HWA1 was deemed to be the best among the 10 alternatives. It provides the finest security system in terms of security methods. The determined performance of the other healthcare web application's alternatives is, in order, HWA7, HWA10, HWA4, HWA2, HWA3, HWA5, HWA9, HWA8, and HWA6, with performance scores of 0.6138, 0.6130, 0.5748, 0.5224, 0.4851, 0.4679, 0.4667, 0.4638, and 0.3597. The findings of this study corroborate that mitigating risk in the design phase assists the developer in building a more secure web application. As security breaches are becoming more frequent, it is imperative to create security standards that also emphasize security benchmarks. Consequently, prioritizing security attributes would undoubtedly aid web application developers in enhancing security. In addition, the researcher advised that the proposed framework may be used to set the benchmark for any organization. This may also form the basis for the development of new, modified, or refined approaches that may encourage other researchers to undertake the development of other new methods in this area.

Author Contributions: A.A. (Abdulaziz Attaallah), K.a.-S. and S.A.A. were primarily responsible for conceptualization; A.A. (Areej Alasiry) and M.M., writing—review and editing; investigation, data validation, and analysis, A.A. (Alka Agrawal), S.A.A. and M.T.J.A.; writing—original draft preparation, S.A.A.; visualization and supervision, R.A.K. All authors reviewed the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Deanship of Scientific Research at the Umm Al-Qura University by grant code (23UQU4281460DSR001). The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through a large-group research project under grant number RGP2/249/44.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data used in this study are available upon request from the corresponding author.

Acknowledgments: The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by grant code (23UQU4281460DSR001). The authors would like to thank the Deanship of Scientific Research at King Khalid University for funding this work through a large-group research project under grant number RGP2/249/44.

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

References

1. Tiwari, N.; Kumar, R.; Sahani, A.; Maurya, A. Survey Paper on Hospital Management System (HMS). *Int. J. Sci. Res. Rev.* **2019**, *7*, 3.
2. Samydurai, A.; Revathi, K.; Karthikeyan, L.; Vanathi, B.; Devi, K. An Enhanced Entity Model for Converting Relational to Non-Relational Documents in Hospital Management System Based on Cloud Computing. *IETE Technol. Rev.* **2022**, *39*, 1–14. [CrossRef]
3. Abernethy, A.; Adams, L.; Barrett, M.; Bechtel, C.; Brennan, P.; Butte, A.; Faulkner, J.; Fontaine, E.; Friedhoff, S.; Halamka, J.; et al. The promise of digital health: Then, now, and the future. *NAM Perspect.* **2022**, *2022*, 1–24. [CrossRef] [PubMed]
4. Maishman, E. 'Small Number' of NHS Lothian Patients Affected by Staff Medical Records Data Breach. Available online: https://www.scotsman.com/health/small-number-nhs-lothian-patients-affected-staff-medical-records-data-breach-3139696 (accessed on 27 March 2023).
5. Department of Veterans Affairs Office of Inspector General. Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans; Report No. 06-02238-163. 11 July 2006. Available online: https://www.va.gov/oig/pubs/VAOIG-06-02238-163.pdf (accessed on 27 March 2023).
6. Rothstein, M.A.; Talbott, M.K. Compelled Authorizations for Disclosure of Health Records: Magnitude and Implications. *Am. J. Bioeth.* **2007**, *7*, 38–45. [CrossRef] [PubMed]
7. Legislative Proposals to Protect Online Privacy and Security. Available online: https://www.justice.gov/archives/opa/blog/legislative-proposals-protect-online-privacy-and-security (accessed on 29 March 2023).
8. Prosecuting the Sale of Botnets and Malicious Software. Available online: https://www.justice.gov/archives/opa/blog/prosecuting-sale-botnets-and-malicious-software (accessed on 29 March 2023).
9. Ansar, S.A.; Alka; Khan, R.A. A Phase-wise Review of Software Security Metrics. In *Networking Communication and Data Knowledge Engineering; Lecture Notes on Data Engineering and Communications Technologies*; Springer: Singapore, 2018; Volume 4. [CrossRef]
10. Parthiban, R.; Kumar, K.S. Effective Resource Scheduling Using Hybrid Gradient Descent Cuckoo Search Algorithm and Security Enhancement in Cloud via Blockchain for Healthcare 4.0. *Mater. Today Proc.* **2022**, *56*, 1802–1808. [CrossRef]
11. Haas, S.; Wohlgemuth, S.; Echizen, I.; Sonehara, N.; Müller, G. Aspects of Privacy for Electronic Health Records. *Int. J. Med. Inform.* **2011**, *80*, 26–31. [CrossRef]
12. Olivier, M.S. Database Privacy: Balancing Confidentiality, Integrity and Availability. *ACM SIGKDD Explor. Newsl.* **2002**, *4*, 20–27. [CrossRef]
13. Amro, A.; Gkioulos, V. Evaluation of a Cyber Risk Assessment Approach for Cyber–Physical Systems: Maritime-and Energy-Use Cases. *J. Mar. Sci. Eng.* **2023**, *11*, 744. [CrossRef]
14. de Hond, A.A.H.; Leeuwenberg, A.M.; Hooft, L.; Kant, I.M.J.; Nijman, S.W.J.; van Os, H.J.A.; Aardoom, J.J.; Debray, T.P.A.; Drenth-van Maanen, A.C.; Girbes, A.R.J.; et al. Guidelines and Quality Criteria for Artificial Intelligence-Based Prediction Models in Healthcare: A Scoping Review. *NPJ Digit. Med.* **2022**, *5*, 1–13. [CrossRef]
15. Quasim, M.T.; Shaikh, A.; Shuaib, M.; Sulaiman, A.; Alam, S.; Asiri, Y. *Fuzzy Decision-Making Method Based Evaluation of Smart Healthcare Management*; 2023. [CrossRef]
16. Prasad, R.S.; Rao, K.R.H.; Kantha, R.R.L. Software Reliability Measuring Using Modified Maximum Likelihood Estimation and SPC. *Int. J. Comput. Appl.* **2011**, *21*, 1–5. [CrossRef]

17. Priyadarshini, I.; Kumar, R.; Tuan, L.M.; Son, L.H.; Long, H.V.; Sharma, R.; Rai, S. A New Enhanced Cyber Security Framework for Medical Cyber Physical Systems. *SICS Softw. Intensive Cyber-Phys. Syst.* **2021**, *35*, 159–183.
18. Attaallah, A.; Alsuhabi, H.; Shukla, S.; Kumar, R.; Gupta, B.K.; Khan, R.A. Analyzing the Big Data Security Through a Unified Decision-Making Approach. *Intell. Autom. Soft Comput.* **2022**, *32*, 1071–1088. [CrossRef]
19. Ansar, S.A.; Aggarwal, S.; Arya, S.; Haq, M.A.; Mittal, V.; Gared, F. An intuitionistic approach for the predictability of anti-angiogenic inhibitors in cancer diagnosis. *Sci. Rep.* **2023**, *13*, 7051. [CrossRef] [PubMed]
20. Lotfi, R.; Kargar, B.; Rajabzadeh, M.; Hesabi, F.; Özceylan, E. Hybrid Fuzzy and Data-Driven Robust Optimization for Resilience and Sustainable Health Care Supply Chain with Vendor-Managed Inventory Approach. *Int. J. Fuzzy Syst.* **2022**, *24*, 1216–1231. [CrossRef]
21. Elibal, K.; Özceylan, E. Comparing industry 4.0 maturity models in the perspective of TQM principles using Fuzzy MCDM methods. *Technol. Forecast. Soc. Chang.* **2022**, *175*, 121379.
22. Abushark, Y.B.; Khan, A.I.; Alsolami, F.J.; Almalawi, A.; Alam, M.M.; Agrawal, A.; Khan, R.A. Usability Evaluation Through Fuzzy AHP-TOPSIS Approach: Security Requirement Perspective. *Comput. Mater. Contin.* **2021**, *68*, 1203–1218. [CrossRef]
23. Kumar, R.; Baz, A.; Alhakami, H.; Alhakami, W.; Agrawal, A.; Khan, R.A. A Hybrid Fuzzy Rule-Based Multi-Criteria Framework for Sustainable-Security Assessment of Web Application. *Ain Shams Eng. J.* **2021**, *12*, 2227–2240. [CrossRef]
24. Attaallah, A.; Algarni, A.; Khan, R.A. Managing Security-Risks for Improving Security-Durability of Institutional Web-Applications: Design Perspective. *Comput. Mater. Contin.* **2021**, *66*, 1849–1865.
25. 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.
26. Altowaijri, S.M. An Architecture to Improve the Security of Cloud Computing in the Healthcare Sector. In *Smart Infrastructure and Applications*; Springer: Cham, Switzerland, 2020; pp. 249–266.
27. Abu-Elezz, I.; Hassan, A.; Nazeemudeen, A.; Househ, M.; Abd-Alrazaq, A. The Benefits and Threats of Blockchain Technology in Healthcare: A Scoping Review. *Int. J. Med. Inform.* **2020**, *142*, 1–9. [CrossRef]
28. Pauli, J.; Xu, D. Integrating Functional and Security Requirements with Use Case De-composition. In Proceedings of the 11th IEEE International Conference on Engineering of Complex Computer Systems (ICECCS'06), Potsdam, Germany, 28–31 August 2006; pp. 57–66.
29. Confidentiality and Privacy in Healthcare. Available online: https://www.betterhealth.vic.gov.au/health/ServicesAndSupport/confidentiality-and-privacy-in-healthcare (accessed on 29 March 2023).
30. Firesmith, D.G. Security Use Cases. *J. Object Technol.* **2003**, *2*, 53–64. [CrossRef]
31. Whitten, A. Making Security Usable. Ph.D. Thesis, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, USA, 2004.
32. Jain, S.; Ingle, M. Software Security Requirements Gathering Instrument. *Int. J. Adv. Comput. Sci. Appl.* **2011**, *2*, 116–121. [CrossRef]
33. Walton, G.H.; Longstaff, T.A.; Linger, R.C. *Technology Foundations for Computational Evaluation of Software Security Attributes*; Carnegie-Mellon University Pittsburgh, Pa Software Engineering Institute: Pittsburgh, PA, USA, 2006.
34. Microsoft. Web Application Security Fundamentals, Chapter 1. Available online: https://msdn.microsoft.com/en-us/library/ff648636.aspx (accessed on 29 March 2023).
35. Ansar, S.A.; Kumar, S.; Khan, M.W.; Yadav, A.; Kha, R.A. Enhancement of Two-Tier ATM Security Mechanism: Towards Providing a Real-Time Solution for Network Issue. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 123–130. [CrossRef]
36. CWE-767. Available online: https://cwe.mitre.org/data/definitions/767.html (accessed on 29 March 2023).
37. CWE-260. Available online: https://cwe.mitre.org/data/definitions/260.html (accessed on 2 April 2023).
38. CWE-311. Available online: https://cwe.mitre.org/data/definitions/311.html (accessed on 2 April 2023).
39. Cybersecurity Help. Available online: https://www.cybersecurity-help.cz/vdb/cwe/620/ (accessed on 2 April 2023).
40. CWE-366. Available online: https://cwe.mitre.org/data/definitions/366.html (accessed on 2 April 2023).
41. CWE-426. Available online: https://cwe.mitre.org/data/definitions/426.html (accessed on 3 April 2023).
42. CVE Details. Available online: https://www.cvedetails.com/cwe-details/494/Download-of-Code-Without-Integrity-Check.html (accessed on 3 April 2023).
43. CWE-362. Available online: https://cwe.mitre.org/data/definitions/362.html (accessed on 3 April 2023).
44. CVE Details. Available online: https://www.cvedetails.com/cwe-details/454/External-Initialization-of-Trusted-Variables-or-Data-Stores.html (accessed on 5 April 2023).
45. CWE-915. Available online: https://cwe.mitre.org/data/definitions/915.html (accessed on 5 April 2023).
46. Chang, C.W.; Wu, C.R.; Lin, H.L. Integrating fuzzy Theory and Hierarchy Concepts to Evaluate Software Quality. *Softw. Qual. J.* **2008**, *16*, 263–276. [CrossRef]
47. Paradis, R.; Tran, B. Balancing Security/Safety and Sustainability Objectives. National Institute of Building Sciences. 2010. Available online: https://www.wbdg.org/resources/balancing-security-safety-and-sustainability-objectives (accessed on 5 April 2023).
48. Saaty, T.L. How to Make a Decision: The Analytic Hierarchy Process. *Eur. J. Oper. Res.* **1990**, *48*, 9–26. [CrossRef]
49. Dawood, K.A.; Sharif, K.Y.; Zaidan, A.A.; Abd Ghani, A.A.; Zulzalil, H.B.; Zaidan, B.B. Mapping and Analysis of Open-Source Software (OSS) Usability for Sustainable OSS Product. *IEEE Access* **2019**, *7*, 65913–65933. [CrossRef]

50. Ansari, M.T.J.; Pandey, D.; Alenezi, M. STORE: Security threat oriented requirements engineering methodology. *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34*, 191–203. [CrossRef]
51. Chen, J.F.; Hsieh, H.N.; Do, Q.H. Evaluating Teaching Performance based on Fuzzy AHP and Comprehensive Evaluation Approach. *Appl. Soft Comput.* **2015**, *28*, 100–108. [CrossRef]
52. Ishizaka, A.; Nemery, P. *Multi-Criteria Decision Analysis: Methods and Software*; John Wiley & Sons: Hoboken, NJ, USA, 2013.
53. Ansari, M.T.J.; Baz, A.; Alhakami, H.; Alhakami, W.; Kumar, R.; Khan, R.A. P-STORE: Extension of STORE methodology to elicit privacy requirements. *Arab. J. Sci. Eng.* **2021**, *46*, 8287–8310. [CrossRef]
54. Chou, Y.C.; Yen, H.Y.; Dang, V.T.; Sun, C.C. Assessing the Human Resource in Science and Technology for Asian Countries: Application of fuzzy AHP and fuzzy TOPSIS. *Symmetry* **2019**, *11*, 251. [CrossRef]
55. Alyami, H.; Ansari, M.T.J.; Alharbi, A.; Alosaimi, W.; Alshammari, M.; Pandey, D.; Agrawal, A.; Kumar, R.; Khan, R.A. Effectiveness evaluation of different IDSs using integrated fuzzy MCDM model. *Electronics* **2022**, *11*, 859. [CrossRef]
56. Alzahrani, F.A.; Ahmad, M.; Ansari, M.T.J. Towards design and development of security assessment framework for internet of medical things. *Appl. Sci.* **2022**, *12*, 8148. [CrossRef]
57. Memon, M.; Wagner, S.R.; Pedersen, C.F.; Beevi, F.H.A.; Hansen, F.O. Ambient assisted living healthcare frameworks, platforms, standards, and quality attributes. *Sensors* **2014**, *14*, 4312–4341. [CrossRef] [PubMed]
58. Agrawal, A.; Khan, R.A.; Ansari, M.T.J. Empowering Indian citizens through the secure e-governance: The digital India initiative context. In *Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2022, Volume 3*; Springer: Singapore, 2020; pp. 3–11.
59. Birman, K.P. Building secure and reliable network applications. In *Worldwide Computing and Its Applications: International Conference, WWCA'97 Tsukuba, Japan, March 10–11, 1997 Proceedings*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 15–28.
60. Carter, J. Coupling and Cohesion: A View of Software Design from the Inside Out. EHR Science. 12 November 2012. Available online: https://www.ehrscience.com/2012/11/12/coupling-and-cohesion-a-view-of-software-design-from-the-inside-out-2/ (accessed on 5 April 2023).