symmetry

MDPI

Article

Software Security Estimation Using the Hybrid Fuzzy ANP-TOPSIS Approach: Design Tactics Perspective

Alka Agrawal [1], Adil Hussain Seh [1], Abdullah Baz [2], Hosam Alhakami [3], Wajdi Alhakami [4], Mohammed Baz [5], Rajeev Kumar [1,*] and Raees Ahmad Khan [1]

1 Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow 226025, India; dralka@bbau.ac.in (A.A.); ahseh.rs@bbau.ac.in (A.H.S.); khanraees@bbau.ac.in (R.A.K.)
2 Department of Computer Engineering, College of Computer and Information Systems, Umm Al-Qura University, Makkah 715, Saudi Arabia; aobaz01@uqu.edu.sa
3 Department of Computer Science, College of Computer and Information Systems, Umm Al-Qura University, Makkah 715, Saudi Arabia; hhhakam@uqu.edu.sa
4 Department of Information Technology, College of Computers and Information Technology, Taif University, Taif 26571, Saudi Arabia; whakami@tu.edu.sa
5 Computer Engineering Department, College of Computers and Information Technology, Taif University, Taif 26571, Saudi Arabia; mo.baz@tu.edu.sa
* Correspondence: rs0414@gmail.com or rajeevkr.rs@bbau.ac.in; Tel.: +91-9548716538

Received: 6 March 2020; Accepted: 7 April 2020; Published: 9 April 2020

Abstract: Increasing the number of threats against software vulnerabilities and rapidly growing data breaches have become a key concern for both the IT industry and stakeholders. Developing secure software systems when there is a high demand for software products from individuals as well as the organizations is in itself a big challenge for the designers and developers. Meanwhile, adopting traditional and informal learnings to address security issues of software products has made it easier for cyber-criminals to expose software vulnerabilities. Hence, it is imperative for the security practitioners to employ a symmetric mechanism so as to achieve the desired level of software security. In this context, a decision-making approach is the most symmetrical technique to assess the security of software in security tactics perspective. Since the security tactics directly address the quality attribute concerns, this symmetric approach will be highly effective in making the software systems more secure. In this study, the authors have selected three main attributes and fifteen sub-attributes at level 1 and level 2, respectively, with ten different software of an institute as alternatives. Furthermore, this study uses a fuzzy-based symmetrical decision-making approach to assess the security of software with respect to tactics. Fuzzy Analytic Network Process (F-ANP) is applied to evaluate the weights of criteria and fuzzy-Symmetrical technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) is used to determine impact of alternatives. The proposed symmetrical assessment in this study will be beneficial for both the designers and developers to categorize and prioritize the security attributes and understand the importance of security tactics during software development life cycle.

Keywords: software security; symmetrical assessment; security tactics; fuzzy logic; fuzzy-ANP; fuzzy-TOPSIS

1. Introduction

The increased use of information and communication technology [1] reveals that the use of software has also increased correspondingly. This has also led to an increase in the number of threats and attacks against software vulnerabilities. Hence, software security has become the main concern [2]. Physical devices, software and data assets of individuals, as well as organizations, are at risk [3]

because of many reasons that mainly include following traditional and informal approaches to deal with software security issues. As per the Research and Markets' report, software market throughout the world will increase by 55%, from $57.6 billion in 2017 to $89.3 billion, in 2022 [4]. Thus, the increasing demand of software has made software security an even more serious and challenging issue for both the developers and users. Despite the increased spending on security services, the instances of attacks and data breaches have also grown rapidly. Every 39 s, there is a hacker attack and since 2013 the average number of stolen records from data breaches is more than 3.8 million per day [5]. According to an IBM report, the average cost of a data breach is $3.92 million and this cost is maximum in USA where a data breach would fetch $ 8.19 million [6].

Evidently, the well-known and proven security tactics and formal guidelines are not being adopted by the developers during symmetrical software development. The availability of security tactics to practitioners is as old as its introduction. Unfortunately, a lack of awareness about security tactics makes many developers follow their traditional and informal approaches to address software security issues [7]. So, identification of security requirements, symmetrical approaches and adoption of specific security tactics is important for the architects and developers to build secure software systems. The symmetrical technique of reusing well-proven solutions or design decisions that affect the control of a response of quality attribute in software architectures is commonly known as tactics [8,9]. It depicts that security tactics should be the main concern of architects and developers and focus should be on it to build a secure software system.

Different symmetrical techniques have been used by researchers to assess the security of software and plenty of research work has been done to prioritize software security attributes. Research work has also been done on what security tactics is: its hierarchical classification and adoption [7,10]. However, authors of this work have not found any study that focuses on assessing the security of software in the security tactics perspective by employing the fuzzy-Analytic Network Process (ANP)-Symmetrical technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) approach. Hence our study, in particular, has assessed the security of software by using the symmetrical method of fuzzy-ANP-TOPSIS.

Fuzzy logic was first coined by Lotfi Zadeh [11] and it surmounts the limitations of traditional logic (Boolean logic) by taking some other cases in between the two extreme cases of truth which could either be true or false. By addressing imprecise information and considering uncertainties of a decision-making problem, it provides better results in decision-making problems [12]. To determine the weights of attributes (criteria) fuzzy-ANP is applied. ANP is a multi-criteria decision analysis approach used in decision-making problems [13–16]. It represents the dependencies among criteria or alternatives to solve the problems having dependencies and is represented by a network because interactions and dependencies among the factors of the problem are shown in a network. While to generate alternative ranking, fuzzy-TOPSIS is used. TOPSIS is the best-known approach for alternative ranking in MCMD problems. The main idea of TOPSIS is that the best alternative among all competitive alternatives should be at the minimum distance from a positive ideal solution (PIS) and have maximum distance from negative ideal solution (NIS) [17–21].

The core intent of this study is two-pronged: first, to bridge the gap between proven and well-known security tactics; second, actual implementation through the assessment of the security of software to provide guidelines for developing secure software systems. In addition, for assessment every organization has its own policies and procedures; so, assessing the security of software is a decision-making problem [22–26]. Hence, this evaluation will be very helpful for designers and developers to understand the attribute priorities and to make appropriate decisions while ensuring the security of software. Effective evaluation of security attributes is not only beneficial for security services of software but it improves the overall quality of software. The significant aspects of this study are:

- Evaluate software security in a security design tactics perspective with the intent to provide guidelines for secure software development.

- Fuzzy-ANP and fuzzy-TOPSIS approach is used to assess the software security. Both approaches are well known and popular in the MCDM problem-solving domain. The proposed symmetrical technique in the study provides precise and efficient results while solving MCMD problems.
- The attribute (criteria) set used in this study to assess software security in the security design tactics perspective through fuzzy-ANP and fuzzy-TOPSIS approach is unique.
- Ten different software have been taken as alternatives for this case study to validate software security in the design tactics perspective.
- This study's empirical initiative aims at providing insights about determining how formal and well-proven security design tactics are followed throughout the software development life cycle.

The remaining part of this research work is divided into the following sections: sub-Section Related Work provides an insight of previous related work; Section 2 discusses materials and methods and includes software security tactics and methodology as two different sub-sections; Section 3 gives the data analysis and results and contains a comparison through the fuzzy-ANP-TOPSIS method and sensitivity analysis as two sub-sections; Section 4 details the discussion of the proposed work, and Section 5 gives the conclusion of our work.

Related Work

Various studies are already available on assessing the security of web application software by using different approaches and symmetrical techniques. Meanwhile, to solve problems like multi-criteria decision making (MCDM) fuzzy-ANP, TOPSIS and fuzzy-ANP TOPSIS symmetrical techniques have also been used in different areas of interest. Some recent and important studies in this regard are:

- Jungwoo Ryoo et al. (2015) estimated the gap between security tactics (architect's vision) and its actual implementation (source code) [7]. Security tactics are examined at the design level as well as implementation level and ideal solutions for the adoption of security tactics are provided. Open sources software has been taken for this assessment to access source code and documentation easily.
- G.P. Garcia et al. (2014) did a study in which they applied a set of security tactics in software system designing [8]. Early Tsunami-warning alert system is used by authors for a case study to achieve the applicability of security tactics. Authors of this study provide a systematic approach to address security as a quality attribute during software designing, and also describe the importance of tactics in software designing.
- Felipe Osses et al. (2018) presented a card game named as security tactics selection poker and a planning-porker based consensus building symmetrical technique that would help the developers to identify and select security tactics to satisfy maximum security requirements on the basis of priority and objectives [9]. The effectiveness of the symmetrical technique is examined in different scenarios by a security software team of 21 practitioners.
- J.J. Zhao and S.Y. Zhao (2010) used three security assessment approaches viz. web content analysis, information security auditing, and computer security network mapping to assess e-government websites of US to determine the opportunities for website threats in their study [12]. The study shows that there is a gap between stated privacy and security policies and implemented security measures of most of the e-government websites, and maximum websites use SSL encryption for data transmission. The study suggests the best possible solutions to improve e-government websites.
- Z. Ravasan and M.A. Zare (2018) proposed a hybrid model based on information system quality assessment and fuzz-ANP to evaluate the e-government website quality [13]. Six Iranian free trade zone portals were used to validate the proposed model and final evaluation results were determined.
- S. Kr. Jha and R. K. Mishra (2018), in their paper, proposed a framework of component security to determine and predict the functional and non-functional security factors for the development of

secure and reliable component-based software. Security issues were examined at three different levels- component level, interface level and at application level [14].

- G. Marquez and H. Astudillo (2019) conducted an experimental study to analyze the availability tactics that would be beneficial for security-design decisions in micro-service based systems (MBS) [15]. 17 Open source MBS were inspected by using their source code and documentation. It was found that fault prevention is mainly focused on availability tactics rather than fault identification and mitigation.
- Keon Chul Park et al. (2014) derived the most appropriate and ideal method of authentication for smartphone banking service using ANP symmetrical technique [16]. The results of the analysis show that biometric authentication is most appropriate in the aspect of security, OTP is most appropriate in the aspect of convenience, and a public key certificate is most ideal in the aspect of cost. In the context of the overall performance in security, convenience and cost, OTP has been found to be the most ideal and appropriate authentication method.
- Bijoyeta Roy, Santanu Kr. Misra (2018) did a study of fuzzy ANP and TOPSIS symmetrical techniques for best software selection [17]. Fuzzy-ANP is applied to determine the attribute weights and also measure their degree of interdependence on each other. Lastly, the criteria weights are given as input to the TOPSIS model to evaluate the final ranking of alternatives.
- Wei Bai et al. (2017) examined the usable-security evaluation results in encrypted messages [18]. 52 participants for this evaluation were taken by the authors. The less-convenient key exchange model has been recognized by participants as more secure overall, but for most day-to-day activities, the key–directory approach has been considered as sufficient security.

From the review of relevant literature, the authors of the present study found that fuzzy-ANP and fuzzy-TOPSIS has been used in various studies to find the best ideal solutions in multi-criteria decision-making problems. There are also some studies that define security tactics with its goals, estimation of the gap between security tactics and its actual implementation, and identification and selection of security tactics to satisfy maximum security requirements [26–30]. However, we did not find any such study in which fuzzy-ANP and fuzzy-TOPSIS is used to assess the software security in a security-tactics perspective. Therefore, our research endeavor will make an assessment to evaluate 10 different software of an educational institute, Babasaheb Bhimrao Ambedkar University in Lucknow, India, in security tactics perspective by using fuzzy-ANP TOPSIS. This assessment mechanism will not only be more effective in developing secure software products but will also enable the higher education institutes to analyze their current software's security strength.

2. Materials and Methods

In this section, the authors discuss the concept and methodology used to implement the said concept in two different sub-sections. First, Section 2.1 discusses the concept named as software security tactics and other necessary concepts related to software security assessment. Section 2.2 provides a description of the methodology used in this study to implement the defined concept in Section 2.1. fuzzy-ANP and fuzzy-TOPSIS approach is discussed in Section 2.2 as a methodology to assess the security of software in the design tactics perspective.

2.1. Software Security Tactics

The literal meaning of security is being secure from all internal as well as external attacks or threats. Tactics literally means, "smartly-planned strategies to accomplish a definite goal". In the context of software architecture, security tactics is defined as "basic decisions (building-blocks) for software architecture that directly concerns the quality attribute of software" [7,19]. Security tactics are also defined as steps taken to enhance the quality attribute of software [8]. Security tactics provide guidelines for the conformity of quality attributes and adoption of these guidelines will help the

developers to develop secure and trustworthy systems. Attack detection, resist against attacks, react to attacks, and recovery from attacks is the main objective of security tactics [20].

On the basis of security tactics, this study will assess the security of 10 different software of Babasaheb Bhimrao Ambedkar University (BBAU), Lucknow, UP, India. Analysis of previous high-quality research papers and other authentic relevant sources are used for attribute identification and selection for security assessment of 10 different software of the university. In this study, the authors consider three criteria at level 1, 15 sub-criteria at level 2 with 10 alternatives. Level 1 attributes detect attacks, resist attacks, and react and recover from attacks. Level 2 attributes detect intrusion, detect service denial, verify message integrity, detect message delay, verify repudiation as sub-attributes detect attacks, identification, authentication, authorization, encryption, limit access as sub-attributes of resist attacks, and revoke access, lock computer, inform actors, maintain audit trail, availability as sub-attributes of react and recover from attacks.

The ten software of the BBAU as alternatives are represented as US-1, US-2, US-3, US-4, US-5, US-6, US-7, US-8, US-9, and US-10 in this study. The attribute identification and selection for this study to assess software security in the security tactics perspective is fundamentally based on the Security Tactics Hierarchy Tree. Figure 1, presents Software Security Attributes in Security Tactics Perspective [31–34]. Further, verify repudiation is added as sub-attribute because repudiation allows any legitimate or illegitimate person to deny the performed action or transaction which can take software system in a catastrophic state. Moreover, repudiation is part of the STRIDE security threat model devised by IBM that maximizes its priority. The reaction to attacks and recovery from attacks are two separate sub-goals of security tactics [20]. However, in this study, these are taken together as a single attribute named "react and recover from attacks" because these two have a high level of dependency on each other, and after reacting to attacks we can achieve the recovery from attacks.

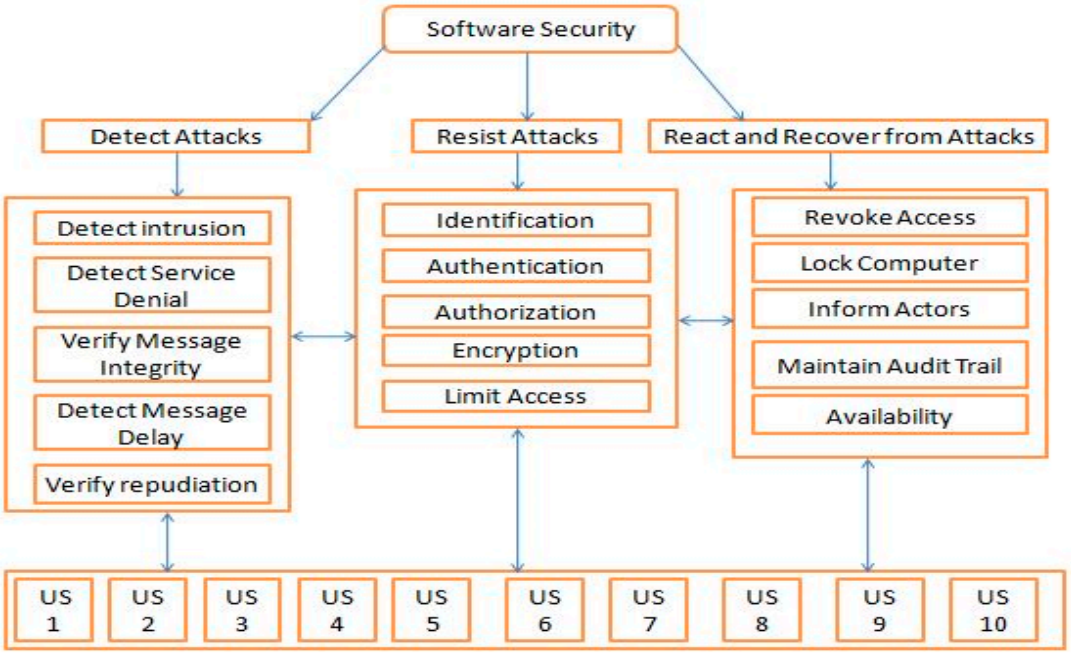

Figure 1. Software security attributes in a security-tactics perspective.

Detect attacks (F1): detecting attacks means that a software system should provide a security mechanism that will help to identify the attacks when any illegitimate user tries to access the information or any information system. It includes detect intrusion, detect denial of services, verify message integrity, detect message delay, and verify repudiation [3].

Detect intrusion (F11): ensures that the security system should have the automatic ability to alert the admins whenever someone or something tries to compromise information system through malicious activities or through violation of security policies 4].

Detect denial of services (F12): it ensures that the security system should detect the malicious attacks that try to make the system or system resources unavailable to its authentic users [5].

Verify message integrity (F13): implies that the security system has the ability to verify the accuracy and completeness of the information sent by the sender [6].

Detect message delay (F14): ensures that the security system should have the ability to detect the reasons behind message delay or in other words detect the man-in-middle attacks [7].

Verify repudiation (F15): it ensures that there should be a strong mechanism that will prove that the activity performed by a particular user in the system is done by him/her when he/she refuses to accept [8].

Resist Attacks (F2): resisting attacks means that a system should come up with a strong security mechanism that will help it to combat when any unauthorized or illegitimate user/process tries to access the system or system resources [9]. It includes Identification, authentication, and authorization, encryption, and limit access. These are the main attributes that will help software system designers and developers to make software systems attack resistive.

Identification (F21): identification occurs when a user, program or process claims an identity [10]. In other words, it is a representation of one's identity where the user or any other entity is not known.

Authentication (F22): authentication is a process of proving a user's claimed identity and it occurs when the users provide correct credentials to prove their identity [11].

Authorization (F23): authorization is a process of granting privileges to access the system resources [12].

Encryption (F24): encryption means encoding of plain text (normal data) into cypher-text (encrypted data) to secure data from unauthorized users [13].

Limit access (F25): it defines that there should be a limit access protocol to access the system resources on the basis of user's needs. It can be defined at the group level or at the individual level [14].

React and recover from attacks (F3): react to an attack means that a software system should have a security mechanism that responds in a particular way when the system faces a potential attack, while recover from an attack means that the system should also have the ability to return to a normal state after facing a potential attack [15–18]. In other words, we can say that the system should provide normal services to its authentic users when or after facing a potential attack. The attributes that will help software designers and developers to make secure software systems that react to attacks and also recover from attacks are: revoke access, lock computer, inform actors, maintain audit trail, and availability.

Revoke access (F31): implies that when system admins realize any type of potential threat or attack, they can severely limit the access to sensitive resources [15].

Lock computer (F32): when there is a repeated failed login from a specific compute, admins can lock the specific computer for some specific time because continuous unsuccessful logins may indicate a malicious attack [15].

Inform actors (F33): malicious attacks sometimes need action by authentic users to execute their attacks, so the administrators shall inform the system users when the system has detected an attack [16].

Maintain audit trail (F34): the security system should also maintain audit trail automatically to keep the user actions and system records and their effects for future use when necessary [17].

Availability (F35): it ensures timely and reliable access to all the authentic users to access information and other resources when needed [18].

2.2. Methodology

Research methodology provides a framework within which a researcher conducts the research [21]. The research methodology used in this study to accomplish the goal of assessing the security of web

application software in the perspective of design tactics is based on fuzzy ANP-TOPSIS, a symmetrical method of MCMD. Fuzzy-ANP is used to estimate the weights of the factors and their interdependence on each other in the ANP network. The TOPSIS symmetrical technique is finally used for the ranking of the alternates. A thorough explanation of these symmetrical techniques has been given below.

Fuzzy-ANP: fuzzy logic is an advanced form of traditional logic first coined by Lotfi Zadeh [11] which is based on mathematical fuzzy-set theory. Fuzzy-logic considers all uncertainties of a problem where it is difficult to determine the solution of the problem to be either completely true or completely false. It considers 0 and 1 as two extreme cases of truth and represents some other cases in between 0 and 1 to address and handle uncertain and imprecise information in decision-making problems [22]. The ANP is a multi-criteria decision analysis approach used in decision-making problems. It is the generalization of the AHP [23].

The analytic hierarchy process (AHP) method was devised by T.L. Saaty in 1980 for MCDM problems [24], but due to the limitation of not measuring the possible dependencies among the criteria [25], T.L. Saaty later introduced ANP to surmount the limitation of AHP [25,26]. ANP represents the dependencies among criteria or alternatives to solve the problems having dependencies [27]. AHP is represented by a hierarchy while ANP is represented by a network [23] because interactions and dependencies among the factors of the problem are shown in a network. ANP also determines the overall influence of these dependencies on the network. ANP also represents inter-dependencies among elements of the same cluster using loops and with other clusters of the same network along with feedback [23]. The fuzzy-ANP approach is the integration of fuzzy logic with ANP to handle imprecise information and make the results more precise and accurate.

Fuzzy-TOPSIS: TOPSIS was originally devised by Ching-Lai Hwang and Yoon as a multi-criteria decision analysis approach used to solve MCDM problems [28]. It is an improved form of displaced ideal solution concept given by Zelany. To address the rank reversal issue, TOPSIS has been found to be the best multi-criteria decision analysis approach which defines that when a non-optimal alternative is found, the alternative ranking can be changed [26]. The main idea of TOPSIS is that the best alternative among all competitive alternatives should be at the minimum distance from PIS and have maximum distance NIS [29]. PIS maximizes the benefit-criteria and minimize the cost-criteria while NIS minimizes benefit criteria and maximizes cost-criteria [30]. TOPSIS is the best-known approach for alternative ranking in MCMD problems.

In this research study, the authors use a hybrid approach of fuzzy-ANP TOPSIS to assess the security design tactics of software for precise, more accurate and efficient results. The step-by-step procedure for evaluating weightage and ranking through fuzzy-ANP-TOPSIS approach is specified below and Figure 2 depicts an overview of the overall working of fuzzy-ANP-TOPSIS approach.

According to Figure 2, the step-by-step procedure for evaluating weightage and ranking through fuzzy ANP-TOPSIS is specified as follows:

Step1: First linguistic terms were converted into crisp numeric values and then a triangular fuzzy number (TFN). TFN can be defined as (p, q, r), where $(p \le q \le r)$ and p, q, r are parameters indicating the smallest, the middle value, and the largest value in the TFN, respectively. Suppose A be a fuzzy number and its membership function can be defined as in Equations (1)–(2) and shown in Figure 3 [26].

$$\mu_A(x) = F \to [0, 1] \tag{1}$$

$$\mu_A(x) = \begin{cases} \frac{x-p}{q-p}, & p \le x \le q \\ \frac{r-x}{r-q}, & q \le x \le r \\ 0, & x > r \end{cases} \tag{2}$$

Otherwise.

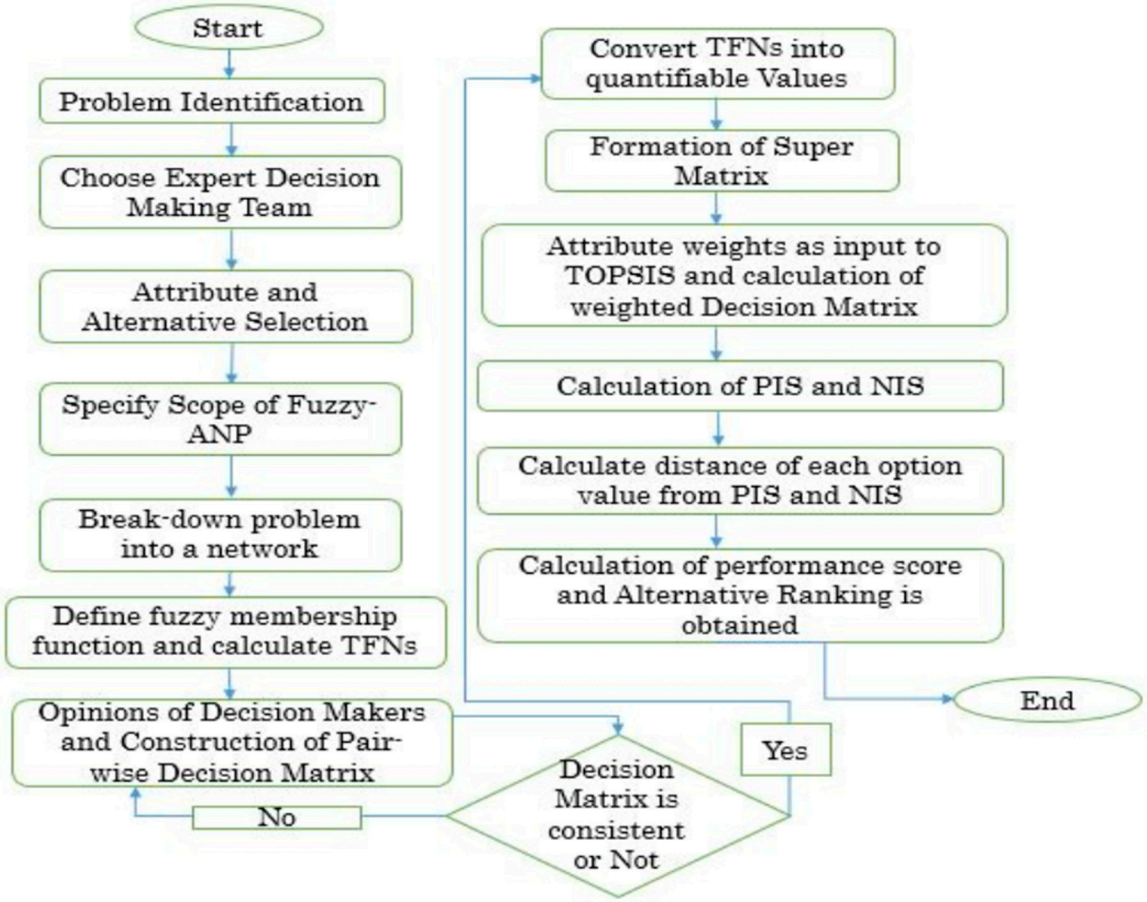

Figure 2. Fuzzy-ANP-TOPSIS procedure.

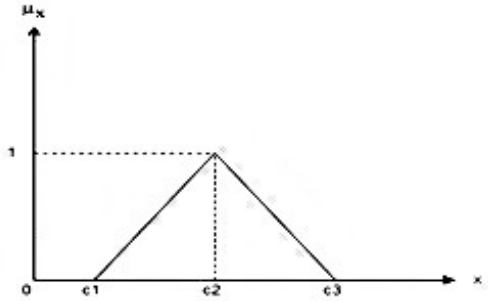

Figure 3. Triangular fuzzy number.

First, views were taken from fifty academics and industry experts who had a wealth of expertise in security design and maintenance for each collection of attributes and related data. The experts were invited in a virtual meeting atmosphere to collate their viewpoints and were briefed about the size of the qualities with respect to various classes as well as the linguistic values. Authors accumulated network structure to determine the weights of security attributes with respect to design tactics, using the data collected. Software development experts provided the answers by assigning scores according to the scale shown in Table 1 to the attributes that influenced each other in a measurable way [20].

Table 1. Saaty scale with corresponding triangular fuzzy numbers (TFNs).

Numeric Value	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)

The triangular fuzzy number is calculated from crisp numeric values by applying Equations (3)–(7) and represented as (p_{ij}, q_{ij}, r_{ij}) where, p_{ij} denotes low value, q_{ij} denotes mid-value and r_{ij} denotes high-value. In addition, TFN [ηij] is defined as the following:

$$\eta_{ij} = \left(p_{ij},\ q_{ij},\ r_{ij}\right) \tag{3}$$

where

$$p_{ij} \le q_{ij} \le r_{ij} \tag{4}$$

$$p_{ij} = min\left(J_{ijd}\right) \tag{5}$$

$$q_{ij} = \left(J_{ij1}, J_{ij2}, J_{ij3}\right)^{\frac{1}{x}} \tag{6}$$

and

$$r_{ij} = max\left(J_{ijd}\right) \tag{7}$$

J_{ijk} represents the relative importance of the values between two factors mentioned in above-given equations; and given by the experts' decision. Where, a pair of attributes judged by experts is represented by i and j. TFN (η_{ij}) is estimated based on the geometric mean of expert's opinions for a particular comparison. In addition, equation 8 to 10 helps to aggregate triangular fuzzy number values. A1 and A2 are two TFNs, A1= (p_1, q_1, r_1) and A2= (p_2, q_2, r_2). The rules of operations on them are as:

$$\left(p_1,\ q_1,\ r_1\right) + \left(p_2,\ q_2,\ r_2\right) = \left(p_1 + p_2,\ q_1 + q_2,\ r_1 + r_2\right) \tag{8}$$

$$\left(p_1,\ q_1,\ r_1\right) \times \left(p_2,\ q_2,\ r_2\right) = \left(p_1{*}p_2,\ q_1{*}q_2,\ r_1{*}r_2\right) \tag{9}$$

$$\left(p_1,\ q_1,\ r_1\right)^{-1} = \left(\frac{1}{p_1}, \frac{1}{q_1}, \frac{1}{r_1}\right) \tag{10}$$

Step 2: pair-wise comparison matrix is constructed by using the responses received from the decision-makers. Calculation of the consistency index (CI) is done by using the formula in Equation (11) as follows:

$$CI = (\gamma_{max} - t)/(t - 1) \tag{11}$$

Where, CI: consistency Index and t: number of compared elements. Further estimation of the consistency ratio (CR), using a random index is as following:

$$CR = CI/RI \tag{12}$$

If $CR < 0.1$ then the generated matrix is reasonably consistent. Where, RI defines a random index. The random index is derived from Saaty [20].

Step 3: After obtaining a reasonably consistent matrix, TFN values are converted to quantifiable value by using defuzzification method. Defuzzification method applied in this work is taken from [16,17] as formulated in Equations (13)–(15), commonly known as alpha-cut method.

$$\mu_{\alpha,\beta}\left(\eta_{ij}\right) = \left[\beta.\eta\alpha\left(p_{ij}\right) + (1-\beta).\ \eta\alpha\left(r_{ij}\right)\right] \tag{13}$$

where, $0 \le \alpha \le 1$ and $0 \le \beta \le 1$

Such that,

$$\eta\alpha\left(p_{ij}\right) = \left(q_{ij} - r_{ij}\right).\alpha + p_{ij} \tag{14}$$

$$\eta\alpha\left(r_{ij}\right) = r_{ij} - \left(r_{ij} - q_{ij}\right).\alpha \tag{15}$$

For experts' preferences, α and β are used in the above equations, also α and β values vary between 0 and 1.

Step 4: ANP handles dependence within a cluster and among different clusters. This step is the formation of the super-matrix which is the result of the priority vector from the paired comparisons between groups including goal, factors, sub-factors, and alternatives.

Step 5: to determine the performance ranking of every alternative over every normalized factor, TOPSIS needs this formula for normalizing the whole decision matrix.

$$X_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}} \tag{16}$$

where, i = 1, 2, ... m; and j = 1,2, ... n.

After that, the calculation of the normalized weighted-decision matrix is performed

$$M_{ij} = w_i X_{ij} \tag{17}$$

where, i = 1, 2, ... m and j = 1,2, ... n.

Step 6: estimation of positive-ideal solution I+ matrix and negative-ideal solution I_ matrix

$$I^+ = z_1^+, z_2^+, z_3^+ \ldots..z_n^+ \tag{18}$$

$$I^- = z_1^-, z_2^-, z_3^- \ldots..z_n^- \tag{19}$$

where, z_j^+ is Max zij if j is an advantage factor and Max zij if j is a cost factor; z_j^- is Min zij if j is an advantage factor and Min zij if j is a cost factor?

Step 7: the next step is identifying the distance of each option value with respect to the positive-ideal solution and the negative-ideal solution:

Positive ideal solution:

$$D_i^+ = \sqrt{\sum_{j=1}^{m}\left(z_i^+ - z_{ij}\right)^2} \tag{20}$$

where, i = 1, 2, 3 . . . .m.

Negative ideal solution:

$$D_i^- = \sqrt{\sum_{j=1}^{m}\left(z_{ij} - z_i^-\right)^2} \tag{21}$$

where, i = 1, 2, 3 . . . .m; where, D_j^+ defines the distance to the positive-ideal solution for i option and D_i^- is the distance to the negative-ideal solution. Calculating the performance value for every alternative (Pi)-

$$P = \frac{D_i^-}{D_i^- - D_i^+} \tag{22}$$

where, $i = 1, 2, 3 \ldots .m$

The above-described step-by-step procedure will be followed to assess the security of software in the security tactics perspective by using a symmetrical method of fuzzy-ANP-TOPSIS with a different number of alternatives. The next section performs a case study and gives the numerical analysis to achieve security tactics for software.

3. Data Analysis and Results

Estimation of the security strength of a software system quantitatively is complex as well as a challenging issue because security assessment is rationally a qualitative measure. During the software development process, the priority of quality attributes plays a very essential role to develop secure as well as usable software products. As a case study, this work contributes an approach for security assessment of university's software by using fuzzy ANP-TOPSIS. For the determination of security assessment in security tactics perspective, three criteria at Level-1 namely Detect attacks, Resist attacks, and React and recover from attacks are represented as F1, F2, and F3, respectively.

With respect to software security assessment in security tactics perspective at level 2: the attributes of detect attacks are detect intrusion, detect denial of services, verify message integrity, detect message delay, and verify repudiation and are represented as F11, F12, F13, F14, F15, respectively. The attributes of resist attacks are identification, authentication, and authorization, encryption, and limit access and are represented as F21, F22, F23, F24, F25, respectively. The attributes of react and recover from attacks are revoke access, lock computer, inform actors, maintain audit trail, and availability and are represented as F31, F32, F33,F34, and F35, respectively, in the tables given below. Software security assessment using fuzzy-ANP-TOPSIS has been examined by applying these Equations (1)–(20) as follows:

With the help of standard Saaty scale shown in Table 1 and by applying Equations (1)–(9), authors of this paper converted the linguistic-terms into numeric values and then aggregated triangular fuzzy number values. Equations (3)–(6) were applied to convert crisp numerical values into fuzzy TFN numbers. Then the pair-wise comparison matrixes of the level-1 criteria is calculated and shown in Table 2. Thereafter, with the help of Equations (10) and (11), the consistency index and the random index has been calculated. The random index of a pair-wise comparison matrix is less than 0.1. This implies that our pair-wise matrix is consistent. In addition, Equations (7)–(9) are used for intermediately operations such as addition, multiplication, and reciprocal of fuzzy numbers, respectively.

Table 2. Fuzzy pair-wise comparison matrix for level 1.

	F1	F2	F3
(F1)	1.00000, 1.00000, 1.00000	1.72010, 1.41000, 1.14300	2.31100, 1.74500, 1.27500
(F2)	0.88100, 0.70100, 0.60200	1.00000, 1.00000, 1.00000	1.68000, 1.37100, 1.02140
(F3)	0.80200, 0.60400, 0.40300	0.98100, 0.73410, 0.59000	1.00000, 1.00000, 1.00000

These intermediate operations are not shown in this study because it will increase the page limit of this study. In Table 3, local weights and normalized values of level-1 attributes are shown. By applying the same operations and Equations (1)–(9) that are used for level-1 attributes, local pair-wise comparison matrixes for sub-attributes of detect attacks, resist attacks, and react and recover from attacks at level-2 have been calculated and shown in Tables 2–5, respectively. Using Equations (12)–(14), the defuzzification of pair-wise comparison matrixes has been done with the help of the alpha-cut method and then normalized values and defuzzified local weights of these sub-attributes are shown in Tables 6–9, respectively.

Table 3. Fuzzy pair-wise comparison matrix for level 2.

	F11	**F12**	**F13**	**F14**	**F15**
F11	1.00000, 1.00000, 1.00000	1.40000, 1.82000, 2.26000	2.46000, 3.09000, 3.76000	2.75000, 3.38000, 3.98000	2.83000, 3.87000, 4.90000
F12	0.44000, 0.55000, 0.72000	1.00000, 1.00000, 1.00000	1.71000, 1.89000, 2.08000	2.46000, 3.5000, 4.52000	1.87000, 2.31000, 2.81000
F13	0.27000, 0.32000, 0.41000	0.48000, 0.53000, 0.58000	1.00000, 1.00000, 1.00000	2.81000, 3.27000, 3.78000	2.23000, 2.88000, 3.57000
F14	0.25000, 0.30000, 0.36000	0.22000, 0.29000, 0.41000	0.26000, 0.31000, 0.36000	1.00000, 1.00000, 1.00000	0.21000, 0.25000, 0.31000
F15	0.20000, 0.26000, 0.35000	0.36000, 0.43000, 0.54000	0.28000, 0.35000, 0.45000	3.25000, 4.04000, 4.81000	1.00000, 1.00000, 1.00000

Table 4. Fuzzy pair-wise comparison matrix for level 2.

	F21	**F22**	**F23**	**F24**	**F25**
F21	1.00000, 1.00000, 1.00000	0.52000, 0.65000, 0.85000	1.4000, 1.7900, 2.22000	1.32000, 1.68000, 2.04000	1.19000, 1.45000, 1.78000
F22	1.1800, 1.5300, 1.9200	1.00000, 1.00000, 1.00000	1.64000, 1.92000, 2.20000	2.42000, 3.06000, 3.70000	0.84000, 1.04000, 1.33000
F23	0.45000, 0.56000, 0.71000	0.45000, 0.52000, 0.61000	1.00000, 1.00000, 1.00000	1.52000, 1.94000, 2.48000	1.25000, 1.49000, 1.78000
F24	0.49000, 0.60000, 0.76000	0.27000, 0.33000, 0.41000	0.40000, 0.52000, 0.66000	1.00000, 1.00000, 1.00000	1.71000, 2.07000, 2.51000
F25	0.56000, 0.69000, 0.84000	0.75000, 0.96000, 1.20000	0.56000, 0.67000, 0.80000	0.59000, 0.48000, 0.59000	1.00000, 1.00000, 1.00000

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

	F31	**F32**	**F33**	**F34**	**F35**
F31	1.00000, 1.00000, 1.00000	0.60000, 0.76000, 0.91000	0.87000, 1.09000, 1.30000	0.69000, 0.95000, 1.32000	0.64000, 0.79000, 1.02000
F32	1.10000, 1.32000, 1.66000	1.00000, 1.00000, 1.00000	0.72000, 0.87000, 1.07000	1.30000, 1.56000, 1.86000	0.93000, 1.17000, 1.44000
F33	0.77000, 0.92000, 1.15000	0.93000, 1.14000, 1.39000	1.00000, 1.00000, 1.00000	1.02000, 1.35000, 1.72000	0.71000, 0.91000, 1.13000
F34	0.76000, 1.05000, 1.46000	0.54000, 0.64000, 0.77000	0.58000, 0.74000, 0.98000	1.00000, 1.00000, 1.00000	0.70000, 0.85000, 1.03000
F35	0.98000, 1.27000, 1.57000	0.70000, 0.85000, 1.07000	0.88000, 1.10000, 1.40000	0.97000, 1.17000, 1.43000	1.00000, 1.00000, 1.00000

Table 6. Normalized local weights of level 1 attributes.

	Normalizing Value	Local Weights
(F1)	0.30000, 0.44000, 0.63000	0.43560
(F2)	0.22500, 0.32000, 0.43500	0.31850
(F3)	0.17500, 0.23640, 0.33680	0.23590

Table 7. Normalized local weights of level 2 attributes.

	Normalizing Value	Local Weights
F11	0.12000, 0.19000, 0.31000	0.19600
F12	0.10000, 0.16000, 0.25000	0.16300
F13	0.08000, 0.13000, 0.21000	0.13400
F14	0.04000, 0.07000, 0.11000	0.06600
F15	0.05000, 0.07000, 0.11000	0.07500

Table 8. Normalized local weights of level 2 attributes.

	Normalizing Value	Local Weights
F21	0.13000, 0.21000, 0.33000	0.22700
F22	0.04000, 0.07000, 0.11000	0.29400
F23	0.06000, 0.09000, 0.14000	0.19100
F24	0.05000, 0.06000, 0.13000	0.15600
F25	0.15000, 0.18000, 0.23000	0.13200

Table 9. Normalized local weights of level 2 attributes.

	Normalizing Value	Local Weights
F21	0.23000, 0.23000, 0.33000	0.139000
F22	0.14000, 0.17000, 0.21000	0.135000
F23	0.16000, 0.19000, 0.24000	0.103000
F24	0.15000, 0.16000, 0.23000	0.112000
F25	0.25000, 0.28000, 0.33000	0.139000

The priorities derived from the different pair-wise comparisons are used to get an unweighted super-matrix. After the weighted super-matrix is calculated, the limit super-matrix is calculated. With the help of local weights, weighted super-matrix, and limit super-matrix, global weights and ranks of the attributes through the hierarchy are estimated, as shown in Table 10.

Table 10. Global weights through the hierarchy.

Second Level Attributes	Global Weights	Percentage	Ranks
F11	0.05785	5.78	11
F12	0.07178	7.17	8
F13	0.06556	6.55	9
F14	0.09387	9.38	2
F15	0.09489	9.48	1
F21	0.03902	3.90	14
F22	0.01369	1.36	15
F23	0.08779	8.77	5
F24	0.04189	4.18	12
F25	0.05954	5.95	10
F31	0.03954	3.95	13
F32	0.08988	8.98	4
F33	0.07478	7.47	7
F34	0.07899	7.89	6
F35	0.09093	9.09	3

Global weights of factors obtained by fuzzy-ANP are given to fuzzy-TOPSIS method as inputs to generate rank for each alternative. The performance using fuzzy-ANP-TOPSIS has been tested by applying these Equations (15)–(20) as follows:

With the help of the Equations (16)–(20) defined in the methodology sub-section, we took the inputs on the technical data of ten software projects (BBA University's software projects) as shown in Table 11. For that, the Equation (16) has been used and normalized decision-matrix for 15 criteria and 10 alternatives have been constructed. Then each cell value (known as normalized performance value) of normalized decision-matrix is multiplied by weights of each criterion and a fuzzy weighted normalized decision-matrix has been obtained with the help of equation 16 and is shown in Table 12. Next, by applying Equation (17), the fuzzy positive-ideal solution (PIS) and fuzzy negative-ideal solution (NIS) have been determined. Then by applying Equations (18) and (19), the distance of each option value from the PIS and NIS is estimated and is represented in Table 13 under the column named D+I and D-I. Finally, by applying Equation (20), the performance value of each criterion has been calculated. The ranking of alternatives is obtained on the basis of the calculated performance score which has also been enlisted in Table 13.

The determined performance of ten institutional alternatives is as: US-1, US-6, US-7, US-9, US-2, US-10, US-5, US-4, US-8, and US-3. As per the assessment of this study, US-1 provides the best security mechanism in security tactics perspective among the 10 competitive alternatives.

3.1. Sensitivity Analysis

Sensitivity analysis is performed by changing the variables to examine the validity of results [36]. In this research work, the sensitivity analysis has been performed on resulted weights (variables). In this work, 15 factors are taken at last (2nd) level so the sensitivities are examined through 15 experiments. In each experiment, the satisfaction degree (CC-i) is calculated by making changes in weights of each factor while other factor's weight remains constant through the fuzzy-ANP-TOPSIS approach. Calculated results are shown in Table 14 and Figure 4.

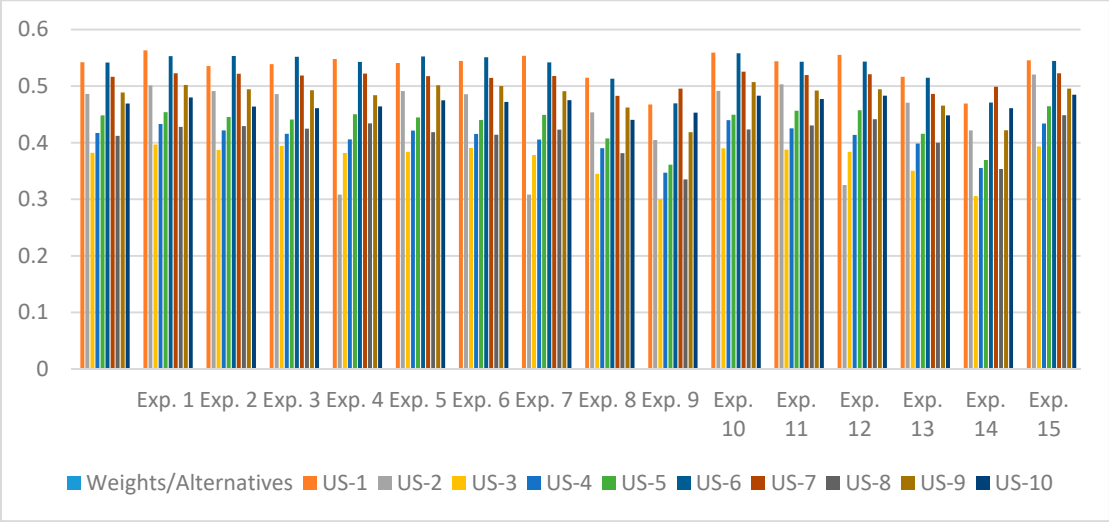

Figure 4. Graphical representation of the sensitivity analysis.

Table 11. Subjective cognition results of evaluators in linguistic terms.

	US-1	**US-2**	**US-3**	**US-4**	**US-5**	**US-6**	**US-7**	**US-8**	**US-9**	**US-10**
	3.20000,	3.70000,	1.80000,	5.40000,	2.90000,	3.60000,	3.70000,	1.80000,	5.40000,	2.90000,
F11	4.60000,	5.30000,	2.80000,	6.70000,	4.50000,	5.40000,	5.30000,	2.80000,	6.70000,	4.50000,
	6.00000	6.80000	4.30000	7.70000	6.10000	7.10000	6.80000	4.30000	7.70000	6.10000
	4.00000,	2.20000,	3.20000,	3.70000,	4.90000,	2.60000,	2.20000,	3.20000,	3.70000,	4.90000,
F12	5.60000,	3.60000,	4.80000,	5.20000,	6.50000,	3.90000,	3.60000,	4.80000,	5.20000,	6.50000,
	7.10000	5.30000	6.30000	6.70000	7.80000	5.40000	5.30000	6.30000	6.70000	7.80000
	7.40000,	4.10000,	2.50000,	3.90000,	5.00000,	3.50000,	4.10000,	2.50000,	3.90000,	5.00000,
F13	8.90000,	5.40000,	3.90000,	5.70000,	6.60000,	5.00000,	5.40000,	3.90000,	5.70000,	6.60000,
	9.60000	6.60000	5.50000	7.40000	7.80000	6.60000	6.60000	5.50000	7.40000	7.80000
	2.80000,	4.10000,	5.20000,	2.80000,	4.10000,	5.10000,	4.10000,	5.20000,	2.80000,	4.10000,
F14	3.90000,	5.60000,	6.70000,	3.70000,	5.60000,	6.10000,	5.60000,	6.70000,	3.70000,	5.60000,
	5.10000	7.00000	7.90000	4.90000	7.00000	6.90000	7.00000	7.90000	4.90000	7.00000
	3.90000,	2.80000,	2.90000,	1.90000,	3.50000,	5.30000,	2.80000,	2.90000,	1.90000,	3.50000,
F15	5.50000,	4.10000,	4.40000,	2.90000,	5.10000,	6.80000,	4.10000,	4.40000,	2.90000,	5.10000,
	6.90000	5.60000	60000	4.30000	6.60000	8.00000	5.60000	60000	4.30000	6.60000
	2.90000,	3.40000,	4.90000,	2.50000,	4.80000,	2.40000,	3.40000,	4.90000,	2.50000,	4.80000,
F21	4.40000,	4.80000,	6.10000,	4.00000,	6.20000,	4.10000,	4.80000,	6.10000,	4.00000,	6.20000,
	5.90000	6.30000	7.10000	5.70000	7.40000	5.90000	6.30000	7.10000	5.70000	7.40000
	4.20000,	3.20000,	3.50000,	4.30000,	2.70000,	3.00000,	3.20000,	3.50000,	4.30000,	2.70000,
F22	5.70000,	4.50000,	4.60000,	6.10000,	4.20000,	4.40000,	4.50000,	4.60000,	6.10000,	4.20000,
	7.20000	6.00000	5.80000	7.70000	5.90000	6.00000	6.00000	5.80000	7.70000	5.90000
	3.20000,	3.70000,	1.80000,	5.40000,	2.90000,	3.60000,	3.70000,	1.80000,	5.40000,	2.90000,
F23	4.60000,	5.30000,	2.80000,	6.70000,	4.50000,	5.40000,	5.30000,	2.80000,	6.70000,	4.50000,
	6.00000	6.80000	4.30000	7.70000	6.10000	7.10000	6.80000	4.30000	7.70000	6.10000
	4.00000,	2.20000,	3.20000,	3.70000,	4.90000,	2.60000,	2.20000,	3.20000,	3.70000,	4.90000,
F24	5.60000,	3.60000,	4.80000,	5.20000,	6.50000,	3.90000,	3.60000,	4.80000,	5.20000,	6.50000,
	7.10000	5.30000	6.30000	6.70000	7.80000	5.40000	5.30000	6.30000	6.70000	7.80000
	7.40000,	4.10000,	2.50000,	3.90000,	5.00000,	3.50000,	4.10000,	2.50000,	3.90000,	5.00000,
F25	8.90000,	5.40000,	3.90000,	5.70000,	6.60000,	5.00000,	5.40000,	3.90000,	5.70000,	6.60000,
	9.60000	6.60000	5.50000	7.40000	7.80000	6.60000	6.60000	5.50000	7.40000	7.80000
	2.80000,	4.10000,	5.20000,	2.80000,	4.10000,	5.10000,	4.10000,	5.20000,	2.80000,	4.10000,
F31	3.90000,	5.60000,	6.70000,	3.70000,	5.60000,	6.10000,	5.60000,	6.70000,	3.70000,	5.60000,
	5.10000	7.00000	7.90000	4.90000	7.00000	6.90000	7.00000	7.90000	4.90000	7.00000
	3.90000,	2.80000,	2.90000,	1.90000,	3.50000,	5.30000,	2.80000,	2.90000,	1.90000,	3.50000,
F32	5.50000,	4.10000,	4.40000,	2.90000,	5.10000,	6.80000,	4.10000,	4.40000,	2.90000,	5.10000,
	6.90000	5.60000	60000	4.30000	6.60000	8.00000	5.60000	60000	4.30000	6.60000
	2.90000,	3.40000,	4.90000,	2.50000,	4.80000,	2.40000,	3.40000,	4.90000,	2.50000,	4.80000,
F33	4.40000,	4.80000,	6.10000,	4.00000,	6.20000,	4.10000,	4.80000,	6.10000,	4.00000,	6.20000,
	5.90000	6.30000	7.10000	5.70000	7.40000	5.90000	6.30000	7.10000	5.70000	7.40000
	4.20000,	3.20000,	3.50000,	4.30000,	2.70000,	3.00000,	3.20000,	3.50000,	4.30000,	2.70000,
F34	5.70000,	4.50000,	4.60000,	6.10000,	4.20000,	4.40000,	4.50000,	4.60000,	6.10000,	4.20000,
	7.20000	6.00000	5.80000	7.70000	5.90000	6.00000	6.00000	5.80000	7.70000	5.90000
	2.80000,	4.10000,	5.20000,	2.80000,	4.10000,	5.10000,	4.10000,	5.20000,	2.80000,	4.10000,
F35	3.90000,	5.60000,	6.70000,	3.70000,	5.60000,	6.10000,	5.60000,	6.70000,	3.70000,	5.60000,
	5.10000	7.00000	7.90000	4.90000	7.00000	6.90000	7.00000	7.90000	4.90000	7.00000

Table 12. The weighted normalized fuzzy-decision matrix.

	US-1	US-2	US-3	US-4	US-5	US-6	US-7	US-8	US-9	US-10
	0.0250000,	0.0330000,	0.0120000,	0.0180000,	0.0110000,	0.0350000,	0.0040000,	0.0120000,	0.0180000,	0.0110000,
F11	0.0360000,	0.0470000,	0.0180000,	0.0220000,	0.0160000,	0.0530000,	0.0060000,	0.0180000,	0.0220000,	0.0160000,
	0.0460000	0.060000	0.0280000	0.0250000	0.0220000	0.070000	0.010000	0.0280000	0.0250000	0.0220000
	0.0310000,	0.0190000,	0.0210000,	0.0120000,	0.0180000,	0.0260000,	0.0120000,	0.0210000,	0.0120000,	0.0180000,
F12	0.0430000,	0.0320000,	0.0310000,	0.0170000,	0.0240000,	0.0380000,	0.0170000,	0.0310000,	0.0170000,	0.0240000,
	0.0550000	0.0470000	0.0410000	0.0220000	0.0280000	0.0530000	0.0220000	0.0410000	0.0220000	0.0280000
	0.0570000,	0.0360000,	0.0160000,	0.0130000,	0.0180000,	0.0340000,	0.0170000,	0.0160000,	0.0130000,	0.0180000,
F13	0.0690000,	0.0480000,	0.0250000,	0.0190000,	0.0240000,	0.0490000,	0.0220000,	0.0250000,	0.0190000,	0.0240000,
	0.0740000	0.0580000	0.0350000	0.0240000	0.0280000	0.0650000	0.0250000	0.0350000	0.0240000	0.0280000
	0.0220000,	0.0360000,	0.0330000,	0.0090000,	0.0150000,	0.050000,	0.0090000,	0.0330000,	0.0090000,	0.0150000,
F14	0.030000,	0.0490000,	0.0430000,	0.0120000,	0.020000,	0.060000,	0.0130000,	0.0430000,	0.0120000,	0.020000,
	0.0390000	0.0620000	0.0510000	0.0160000	0.0250000	0.0680000	0.0180000	0.0510000	0.0160000	0.0250000
	0.030000,	0.0250000,	0.0190000,	0.0060000,	0.0130000,	0.0520000,	0.0130000,	0.0190000,	0.0060000,	0.0130000,
F15	0.0430000,	0.0360000,	0.0280000,	0.0090000,	0.0190000,	0.0670000,	0.0170000,	0.0280000,	0.0090000,	0.0190000,
	0.0530000	0.0490000	0.0390000	0.0140000	0.0240000	0.0790000	0.0210000	0.0390000	0.0140000	0.0240000
	0.0220000,	0.030000,	0.0320000,	0.0080000,	0.0170000,	0.0240000,	0.0070000,	0.0320000,	0.0080000,	0.0170000,
F21	0.0340000,	0.0420000,	0.0390000,	0.0130000,	0.0230000,	0.040000,	0.0110000,	0.0390000,	0.0130000,	0.0230000,
	0.0460000	0.0560000	0.0460000	0.0190000	0.0270000	0.0580000	0.0160000	0.0460000	0.0190000	0.0270000
	0.0320000,	0.0280000,	0.0230000,	0.0140000,	0.010000,	0.030000,	0.0050000,	0.0230000,	0.0140000,	0.010000,
F22	0.0440000,	0.040000,	0.030000,	0.020000,	0.0150000,	0.0430000,	0.0090000,	0.030000,	0.020000,	0.0150000,
	0.0560000	0.0530000	0.0370000	0.0250000	0.0210000	0.0590000	0.0140000	0.0370000	0.0250000	0.0210000
	0.0310000,	0.0190000,	0.0210000,	0.0120000,	0.0180000,	0.0260000,	0.0120000,	0.0210000,	0.0120000,	0.0180000,
F23	0.0430000,	0.0320000,	0.0310000,	0.0170000,	0.0240000,	0.0380000,	0.0170000,	0.0310000,	0.0170000,	0.0240000,
	0.0550000	0.0470000	0.0410000	0.0220000	0.0280000	0.0530000	0.0220000	0.0410000	0.0220000	0.0280000
	0.0570000,	0.0360000,	0.0160000,	0.0130000,	0.0180000,	0.0340000,	0.0170000,	0.0160000,	0.0130000,	0.0180000,
F24	0.0690000,	0.0480000,	0.0250000,	0.0190000,	0.0240000,	0.0490000,	0.0220000,	0.0250000,	0.0190000,	0.0240000,
	0.0740000	0.0580000	0.0350000	0.0240000	0.0280000	0.0650000	0.0250000	0.0350000	0.0240000	0.0280000
	0.0220000,	0.0360000,	0.0330000,	0.0090000,	0.0150000,	0.050000,	0.0090000,	0.0330000,	0.0090000,	0.0150000,
F25	0.030000,	0.0490000,	0.0430000,	0.0120000,	0.020000,	0.060000,	0.0130000,	0.0430000,	0.0120000,	0.020000,
	0.0390000	0.0620000	0.0510000	0.0160000	0.0250000	0.0680000	0.0180000	0.0510000	0.0160000	0.0250000
	0.030000,	0.0250000,	0.0190000,	0.0060000,	0.0130000,	0.0520000,	0.0130000,	0.0190000,	0.0060000,	0.0130000,
F31	0.0430000,	0.0360000,	0.0280000,	0.0090000,	0.0190000,	0.0670000,	0.0170000,	0.0280000,	0.0090000,	0.0190000,
	0.0530000	0.0490000	0.0390000	0.0140000	0.0240000	0.0790000	0.0210000	0.0390000	0.0140000	0.0240000
	0.0220000,	0.030000,	0.0320000,	0.0080000,	0.0170000,	0.0240000,	0.0070000,	0.0320000,	0.0080000,	0.0170000,
F32	0.0340000,	0.0420000,	0.0390000,	0.0130000,	0.0230000,	0.040000,	0.0110000,	0.0390000,	0.0130000,	0.0230000,
	0.0460000	0.0560000	0.0460000	0.0190000	0.0270000	0.0580000	0.0160000	0.0460000	0.0190000	0.0270000
	0.0320000,	0.0280000,	0.0230000,	0.0140000,	0.010000,	0.030000,	0.0050000,	0.0230000,	0.0140000,	0.010000,
F33	0.0440000,	0.040000,	0.030000,	0.020000,	0.0150000,	0.0430000,	0.0090000,	0.030000,	0.020000,	0.0150000,
	0.0560000	0.0530000	0.0370000	0.0250000	0.0210000	0.0590000	0.0140000	0.0370000	0.0250000	0.0210000
	0.0220000,	0.0360000,	0.0330000,	0.0090000,	0.0150000,	0.050000,	0.0090000,	0.0330000,	0.0090000,	0.0150000,
F34	0.030000,	0.0490000,	0.0430000,	0.0120000,	0.020000,	0.060000,	0.0130000,	0.0430000,	0.0120000,	0.020000,
	0.0390000	0.0620000	0.0510000	0.0160000	0.0250000	0.0680000	0.0180000	0.0510000	0.0160000	0.0250000
	0.030000,	0.0250000,	0.0190000,	0.0060000,	0.0130000,	0.0520000,	0.0130000,	0.0190000,	0.0060000,	0.0130000,
F35	0.0430000,	0.0360000,	0.0280000,	0.0090000,	0.0190000,	0.0670000,	0.0170000,	0.0280000,	0.0090000,	0.0190000,
	0.0530000	0.0490000	0.0390000	0.0140000	0.0240000	0.0790000	0.0210000	0.0390000	0.0140000	0.0240000

Table 13. Closeness coefficients to the aspired level among the different alternatives.

Alternatives		D+i	D-i	Performance Score (Pi)	Rank
Alternative 1	US-1	0.24812	0.13114	0.54213	1
Alternative 2	US-2	0.23512	0.14911	0.48617	5
Alternative 3	US-3	0.22822	0.14189	0.38212	10
Alternative 4	US-4	0.21511	0.15414	0.41717	8
Alternative 5	US-5	0.20410	0.16614	0.44818	7
Alternative 6	US-6	0.16902	0.19913	0.54158	2
Alternative 7	US-7	0.17908	0.19013	0.51643	3
Alternative 8	US-8	0.21707	0.15212	0.41217	9
Alternative 9	US-9	0.18905	0.18151	0.48877	4
Alternative 10	US-10	0.17015	0.19914	0.46913	6

Table 14. Sensitivity analysis.

Experiments	Weights/ Alternatives		US-1	US-2	US-3	US-4	US-5	US-6	US-7	US-8	US-9	US-10
	Original Weights		0.54213	0.48617	0.38212	0.41717	0.44818	0.54158	0.51643	0.41217	0.48877	0.46913
Exp. 1	F11	Satisfaction Degree (CC-i)	0.56323	0.50127	0.39672	0.43297	0.45408	0.55298	0.52263	0.42807	0.50207	0.48002
Exp. 2	F12		0.53533	0.49137	0.38732	0.42177	0.44548	0.55338	0.52183	0.42947	0.49437	0.46393
Exp. 3	F13		0.53893	0.48587	0.39432	0.41577	0.44098	0.55188	0.51883	0.42497	0.49287	0.46093
Exp. 4	F14		0.54793	0.30837	0.38172	0.40587	0.45018	0.54288	0.52213	0.43417	0.48387	0.46423
Exp. 5	F15		0.54093	0.49127	0.38372	0.42147	0.44458	0.55248	0.51763	0.41857	0.50157	0.47503
Exp. 6	F21		0.54453	0.48577	0.39072	0.41547	0.44008	0.55098	0.51463	0.41407	0.50007	0.47203
Exp. 7	F22		0.55353	0.30827	0.37812	0.40557	0.44928	0.54198	0.51793	0.42327	0.49107	0.47533
Exp. 8	F23		0.51473	0.45367	0.34492	0.39027	0.40768	0.51318	0.48293	0.38167	0.46227	0.44033
Exp. 9	F24		0.46743	0.40467	0.30012	0.34697	0.36128	0.46948	0.49563	0.33527	0.41857	0.45303
Exp. 10	F25		0.55923	0.49157	0.38992	0.43987	0.44948	0.55818	0.52563	0.42347	0.50727	0.48303
Exp. 11	F31		0.54383	0.50327	0.38772	0.42547	0.45638	0.54308	0.51963	0.43037	0.49217	0.47703
Exp. 12	F32		0.55523	0.32537	0.38372	0.41387	0.45748	0.54348	0.52113	0.44147	0.49447	0.48323
Exp. 13	F33		0.51643	0.47077	0.35052	0.39857	0.41588	0.51468	0.48613	0.39987	0.46567	0.44823
Exp. 14	F34		0.46913	0.42177	0.30572	0.35527	0.36948	0.47098	0.49883	0.35347	0.42197	0.46093
Exp. 15	F35		0.54553	0.52037	0.39332	0.43377	0.46458	0.54458	0.52283	0.44857	0.49557	0.48493

In Table 14, the original weights of this work are shown in the first row. According to the original results, Alternative one (US-1) has a high satisfaction degree (CC-i). From F11-F15, F21-F25, and F31-F35 fifteen experiments are completed. Obtained results show that the alternative-1 (US-1) still has high-satisfaction degree (CC-i) in 15 experiments. The least weight of alternative is US-3 in thirteen experiments and US-2 in two experiments. The variations of results with each other show that the ratings of the alternatives are sensitive to the weights. The graphical representation of the 15 experiments with respect to original weights and 10 alternatives is shown in Figure 4.

3.2. Comparison of the Results

Applying different methods on the same data shows variations in results. Researches use different symmetrical techniques to check the accuracy of results attained through projected symmetrical techniques [35,36]. In this study, the authors have used a fuzzy ANP-TOPSIS approach to examine the accuracy of the results obtained. In fuzzy ANP-TOPSIS, the process of data gathering and evaluation of that data is the same as that of the classical ANP-TOPSIS. However, for the fuzzy-ANP-TOPSIS, the fuzzification and defuzzification are required. Hence, for fuzzy ANP-TOPSIS, data is taken in its original numeric form and later converted into fuzzy numbers. The variations in the results of fuzzy and classical ANP-TOPSIS are shown in Table 15.

Table 15. Comparison of the results of classical and fuzzy-Analytic Network Process (ANP)- Symmetrical technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) methods.

Methods/Alternatives	US-1	US-2	US-3	US-4	US-5	US-6	US-7	US-8	US-9	US-10
Fuzzy-ANP-TOPSIS	0.54213	0.48617	0.38212	0.41717	0.44818	0.54158	0.51643	0.41217	0.48877	0.46913
Classical-ANP-TOPSIS	0.53653	0.48627	0.38572	0.41747	0.44908	0.54248	0.52063	0.42307	0.48157	0.45803

There are various real-life problems where we cannot decide that the solution to the problem is either completely true or completely false. If we do so it will provide imprecise and inefficient results. Fuzzy-logic considers all uncertainties of a problem and considers 0 and 1 as two extreme cases of truth and represents some other cases in between these two boundary values to address and handle ambiguous information in decision-making problems. Integrating fuzzy logic with ANP and TOPSIS makes this symmetrical technique more powerful. Moreover, this approach provides accurate results in dealing with similar problems [37]. In comparison, the classical ANP-TOPSIS does not address such ambiguities. Further, as evident from the results, fuzzy-ANP and classical-ANP strategies have extraordinary procedures.

The outcomes are unique, yet fundamentally the same. This empirical work has taken the Pearson's Correlation Method [37] for assessing the correlation between outcomes. The correlation coefficient shows the impact of the relationship between two values. The scale lies between −1 and +1 [37]. The value near to −1 shows the lower bonding between values, and the value near to *+1* shows the tighter bonding between values. The Pearson correlation between the results of fuzzy-ANP and classical-ANP is 0.89176, which shows the strong correlation between the results achieved. As given in Table 15, the results with different approaches with the same dataset have been obtained, and these results show that the correlation between the results of fuzzy-ANP and classical-ANP is highly correlated.

The results of our study also show that the covered factors and their contribution to efficient security mechanisms in security tactics perspective are remarkable. Mamdouh Alenezi et al. recently published an article in which they assessed the security of software in a tactics perspective [38]. This article contained Fuzzy AHP-TOPSIS only. Due to network structure rather than tree structure, ANP methodology is better than the AHP methodology [37,38]. Therefore, in the current paper, the authors have taken design tactics as a contributor in the first level of the network, which improvises the results in the end. With the help of fuzzy-ANP-TOPSIS method, there is not a symmetric method for assessing software security in the design tactics perspective. Additionally, for testing the results, Mamdouh Alenezi et al. took eight alternatives only, whereas this paper has opted for ten alternatives to validate the results.

4. Discussion

Extensive use of computers, smartphones, electronic gadgets and other electromechanical devices has rapidly increased the demand for software throughout the world. A report on smartphone users (2019) shows that 3.3 billion people use smartphones in the whole world [31,35]. This figure was 1.31 billion in 2013 [32]. The number of active internet users has reached 4.33 billion as of July 2019, which is 56% of the total population of the world [33]. Meanwhile, in other sectors like business, health, education and government departments, the use of intelligent information systems has also shown rapid growth. Unfortunately, on the other side, the magnitude of attacks against software vulnerability and data breaches has also increased rapidly.

Moreover, reliance on informal and traditional procedures to address software security issues has further increased software vulnerabilities. Thus, providing software products to customers with ideal security mechanisms poses to be a daunting task for the present-day developers. The main goal of this study is to assess the security of software in security tactics perspective that will help the developers in prioritizing and selecting the security attributes to make secure software systems. In this league, the present study used an integrated fuzzy-ANP TOPSIS method of MCDM to estimate the software security in security tactics perspective.

Furthermore, the effectivity of the proposed symmetrical technique is convincingly established through a case study undertaken to evaluate 10 software of Babasaheb Bhimrao Ambedkar University. Unlike the fuzzy-AHP, fuzzy-ANP represents interactions and dependencies among attributes as well as alternatives with feedback [23–25]. Due to this it closely depicts the real-life problems and provides better results [23–27] and fuzzy logic addresses and handles the uncertain and imprecise information in decision problems very well [22]. Moreover, TOPSIS performs very well in ranking alternatives and choosing the best alternative among the available alternatives [28–30]. Therefore, a hybrid fuzzy-ANP-TOPSIS method is applied to get better results as compared to the other MCMD symmetrical techniques.

Finally, University's software-1 (US-1) has been found best among 10 competitive alternatives because it provides the best security mechanism in the security tactics perspective with a 0.54213 performance score. Alternative US-1 is followed by US-6, US-7, US-9, US-2, US-10, US-5, US-4, US-8, and US-3 with performance scores 0.54158, 0.51643, 0.48877, 0.48617, 0.46913, 0.44818, 0.41717, 0.41217, and 0.38212, respectively. Overall findings (pros and limitations) of our research work are:

4.1. Pros

Assessment of software security in the security-tactics perspective is a way to evaluate the security attribute of a software system and provide guidelines for designers and developers.

Practitioners can take help from this study to prioritize and select attributes for software development to build secure systems.

Software security is a serious issue for both developers and stakeholders but still gets ignored. This study will provide sufficient understanding to practitioners to adopt security tactics instead of informal and traditional approaches while developing software systems to make them more secure.

4.2. Limitations

Our assessment can be sufficient for practitioners but not final because software security is a complex as well as dynamic task. Every day new challenges have been raised and faced by both developers and users.

Hybrid fuzzy-ANP-TOSIS is a suitable and significant approach for software security assessment but there may be better MCDM symmetrical techniques for MCMD problems.

5. Conclusions

This study employs a hybrid fuzzy-ANP-TOPSIS approach to assess the security of University's software in the perspective of security tactics. The hybrid fuzzy-ANP-TOPSIS approach provides an efficient way to evaluate any MCDM problem like software security assessment with different factors and alternatives. Software security factors are determined, their weights are calculated, alternative ranking is determined and overall software security is estimated. It has been concluded that alternative (US-1) provides the best reliable and durable security mechanism among all 10 competitive alternatives. Evaluation of software security of the university's software in security tactics perspective will provide guidelines and support practitioners to develop high-quality software products that will provide durable and reliable security mechanisms against all internal as well as external threats and attacks.

Author Contributions: A.A., A.H.S., A.B., H.A., W.A. and M.B. contributed to the motivation, the interpretation of the method effects and the results. A.B. and R.K. proposed minor suggestions. A.H.S. and R.K. provided the concept, prepared the draft versions, performing the evaluation and extracting the conclusions. R.A.K. supervised the study. All authors have read and approved the final manuscript.

Funding: Deanship of Scientific Research at Umm Al-Qura University, Kingdom of Saudi Arabia.

Acknowledgments: The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by grant code: 18-COM-1-01-0001.

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

References

1. Elisa, N. Usability, accessibility and web security assessment of e-government websites in Tanzania. *Int. J. Comput. Appl.* **2017**, *164*, 42–48. [CrossRef]
2. McGraw, G. *Software Security: Building Security*; Addison Wesley Professional: Boston, MA, USA, 2006.
3. Sasse, M.A.; Flechais, I. Usable Security Why Do We Need It? How Do We Get It? 2005. Available online: https://www.researchgate.net/publication/316236669 (accessed on 15 November 2019).
4. Research and Markets. Software Industry. 2016. Available online: https://www.researchandmarkets.com/resear/w2nrwg (accessed on 16 November 2019).
5. Cyber Security Facts and Stats—CybintSolutions. Available online: https://www.cybintsolutions.com/cyber-Security-facts-stats (accessed on 18 November 2019).
6. IBM. Cost of Data Breach Report. 2019. Available online: https://www.ibm.com/security/data-breach (accessed on 20 November 2019).

7. Ryoo, J.; Malone, B.; Laplante, P.A.; Anand, P. The Use of Security Tactics in Open Source Software Projects. *IEEE Trans. Reliab.* **2015**, *65*, 1195–1204. [CrossRef]
8. Pedraza-Garcia, G.; Astudillo, H.; Correal, D. A methodological approach to apply security tactics in software architecture design. In Proceedings of the 2014 IEEE Colombian Conference on Communications and Computing (COLCOM), Bogota, Colombia, 4–6 June 2014; pp. 1–8.
9. Osses, F.; Márquez, G.; Villegas, M.M.; Orellana, C.; Visconti, M.; Astudillo, H. Security tactics selection poker (TaSPeR) a card game to select security tactics to satisfy security requirements. In Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings, Madrid, Spain, 7 September 2018; pp. 1–7.
10. Pressman, R.S. *Software Engineering: A practitioner's Approach*; Palgrave Macmillan: London, UK, 2005; Available online: http://seu1.org/files/level4/IT-242/Software%20Engineering%20_%207th%20Edition.pdf (accessed on 18 November 2019).
11. Ross, T.J. *Fuzzy Logic with Engineering Applications*; John Wiley & Sons, Ltd.: Hoboken, NJ, USA, 2010.
12. Zhao, J.J.; Zhao, S.Y. Opportunities and threats: A security assessment of state e-government websites. *Gov. Inf. Q.* **2010**, *27*, 49–56. [CrossRef]
13. Ravasan, A.Z.; Zare, M.A. *A Framework for Assessing Website Quality: An Application in the Iranian free Economic Zones Websites*; IGI Global: Hershey, PA, USA, 2018; Chapter-13; pp. 248–272. [CrossRef]
14. Jha, S.K.; Mishra, R.K. Predicting and Accessing Security Features into Component-Based Software Development: A Critical Survey. In *Advances in Intelligent Systems and Computing, Proceedings of the Software Engineering*; Springer: Singapore, 2018; Volume 731, pp. 287–294.
15. Márquez, G.; Astudillo, H. Identifying availability tactics to support security architectural design of microservice-based systems. In Proceedings of the 13th European Conference on Software Architecture, Paris, France, 9–13 September 2019; Volume 2, pp. 123–129. Available online: https://dl.acm.org/doi/10.1145/3344948.3344996 (accessed on 18 November 2019).
16. Park, K.C.; Shin, J.W.; Lee, B.G. Analysis of Authentication Methods for Smartphone Banking Service using ANP. *KSII Trans. Internet Inf. Syst.* **2014**, *8*, 2087–2103. [CrossRef]
17. Roy, B.; Misra, S.K. An Integrated Fuzzy ANP and TOPSIS Methodology for Software Selection under MCDM Perspective. *Int. J. Innov. Res. Comput. Commun. Eng.* **2018**, *6*, 492–501.
18. Bai, W.; Kim, D.; Namara, M.; Qian, Y.; Kelley, P.G.; Mazurek, M.L. Balancing security and usability in encrypted email. *IEEE Internet Comput.* **2017**, *21*, 30–38. [CrossRef]
19. Ryoo, J.; Laplante, P.; Kazman, R. A methodology for mining security tactics from security patterns. In Proceedings of the 2010 43rd Hawaii International Conference on System Sciences, Honolulu, HI, USA, 5–8 January 2010; pp. 1–5.
20. Rekik, R.; Kallel, I.; Alimi, A.M. Ranking criteria based on fuzzy ANP for assessing E-commerce web sites. In Proceedings of the 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Budapest, Hungary, 9–12 October 2016; pp. 003469–003474.
21. Research Methodology. Available online: https://researchmethodology.net/research-methodology/ (accessed on 31 November 2019).
22. Solangi, Y.A.; Tan, Q.; Mirjat, N.H.; Valasai, G.D.; Khan, M.W.A.; Ikram, M. An integrated Delphi-AHP and fuzzy TOPSIS approach toward ranking and selection of renewable energy resources in Pakistan. *Processes* **2019**, *7*, 118. [CrossRef]
23. Saaty, T.L. The Analytic Network Process. *Iran. J. Oper. Res.* **2008**, *1*, 1–27.
24. Saaty, T.L. The Analytic Hierarchy Process Mcgraw Hill, New York. *Agric. Econ. Rev.* **1980**, *70*. Available online: https://www.scirp.org/(S(lz5mqp453edsnp55rrgjct55))/reference/ReferencesPapers.aspx?ReferenceID=1895817 (accessed on 31 November 2019).
25. Yuksel, I.; Dagdeviren, M. Using the analytic network process (ANP) in a SWOT analysis–A case study for a textile firm. *Inf. Sci.* **2007**, *177*, 3364–3382. [CrossRef]
26. Kuo, R.J.; Hsu, C.W.; Chen, Y.L. Integration of fuzzy ANP and fuzzy TOPSIS for evaluating carbon performance of suppliers. *Int. J. Environ. Sci. Technol.* **2015**, *12*, 3863–3876. [CrossRef]
27. Lee, J.W.; Kim, S.H. Using analytic network process and goal programming for interdependent information system project selection. *Comput. Oper. Res.* **2000**, *27*, 367–382. [CrossRef]
28. Mohaghar, A.; Fathi, M.R.; Faghih, A.; Turkayesh, M.M. An integrated approach of Fuzzy ANP and Fuzzy TOPSIS for R&D project selection: A case study. *Aust. J. Basic Appl. Sci.* **2012**, *6*, 66–75.

29. Lai, Y.J.; Liu, T.Y.; Hwang, C.L. TOPSIS for MODM. *Eur. J. Oper. Res.* **1994**, *76*, 486–500. [CrossRef]
30. 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]
31. Statista. Smartphone Users Worldwide. 2019. Available online: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ (accessed on 25 November 2019).
32. DazeInfo. Worldwide Active Smartphone Users. 2019. Available online: https://dazeinfo.com/2014/12/18/worldwide-Smartphone-users (accessed on 26 November 2019).
33. Statista. Worldwide Digital Population. 2019. Available online: https://www.statista.com/statistics/617136/digital-population-worldwide/ (accessed on 26 November 2019).
34. Bass, L.; Clements, P.; Kazman, R. *Software Architecture in Practice*; Addison Wesley Professional: Boston, MA, USA, 2003.
35. Bankmycell. How Many Phones Are in the World? 2019. Available online: https://www.bankmycell.com/blog/how-many-phones-are-in-the-world (accessed on 28 November 2019).
36. Kumar, R.; Zarour, M.; Alenezi, M.; Agrawal, A.; Khan, R.A. Measuring security durability of software through fuzzy-based decision-making process. *Int. J. Comput. Intell. Syst.* **2019**, *12*, 627–642. [CrossRef]
37. Khan, S.A.; Alenezi, M.; Agrawal, A.; Kumar, R.; Khan, R.A. Evaluating Performance of Software Durability through an Integrated Fuzzy-Based Symmetrical Method of ANP and TOPSIS. *Symmetry* **2020**, *12*, 493. [CrossRef]
38. Alenezi, M.; Agrawal, A.; Kumar, R.; Khan, R.A. Evaluating Performance of Web Application Security Through a Fuzzy Based Hybrid Multi-Criteria Decision-Making Approach: Design Tactics Perspective. *IEEE Access* **2020**, *8*, 25543–25556. [CrossRef]