Computers, Materials & Continua
DOI:10.32604/cmc.2020.013854
Article

Managing Security-Risks for Improving Security-Durability of Institutional Web-Applications: Design Perspective

Abdulaziz Attaallah[1], Abdullah Algarni[1] and Raees Ahmad Khan[2,*]

[1]Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia
[2]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, Uttar Pradesh, India
*Corresponding Author: Raees Ahmad Khan. Email: khanraees@yahoo.com
Received: 24 August 2020; Accepted: 06 October 2020

Abstract: The advanced technological need, exacerbated by the flexible time constraints, leads to several more design level unexplored vulnerabilities. Security is an extremely vital component in software development; we must take charge of security and therefore analysis of software security risk assumes utmost significance. In order to handle the cyber-security risk of the web application and protect individuals, information and properties effectively, one must consider what needs to be secured, what are the perceived threats and the protection of assets. Security preparation plans, implements, tracks, updates and consistently develops safety risk management activities. Risk management must be interpreted as the major component for tackling security efficiently. In particular, during application development, security is considered as an add-on but not the main issue. It is important for the researchers to stress on the consideration of protection right from the earlier developmental stages of the software. This approach will help in designing software which can itself combat threats and does not depend on external security programs. Therefore, it is essential to evaluate the impact of security risks during software design. In this paper the researchers have used the hybrid Fuzzy AHP-TOPSIS method to evaluate the risks for improving security durability of different Institutional Web Applications. In addition, the e-component of security risk is measured on software durability, and vice versa. The paper's findings will prove to be valuable for enhancing the security durability of different web applications.

Keywords: Web applications; durability; cyber-security; risk; fuzzy logic; decision-making approach

1 Introduction

Software development team experiences multiple challenges to improve the usable security of the application. Software companies are often searching for a feasible software protection mechanism. Scientists and developers in this circumstance adjust their plans so that protection of the device can be handled. Risk is a challenge that can disrupt well-defined strategies and have specific aims [1–3]. Risk management process is used not only to minimize the risk but also to increase efficiency through safeguarding the software product. The risk management security strategy is a theoretical structure that

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

tracks the progress of the risk mitigation security programme. Risk management process, control and management for security are interconnected processes that are incorporated into the design of protection for the safe production of software. The technology of risk management assists the whole software development process in the risk reduction activities [4,5].

The optimal risk management protection mechanism is similar to many other concepts with different features. A major study was performed in the field of risk management for security [6,7]. Software security risk management and compliance are essential to handling a variety of safety risks. All systems must be changed in order to produce better performance. The entire software product life cycle is used to define and reduce threats for managing risk strategic. Risk management and control systems have different emphasis in line with the policy and supervision included in the security evaluation, for example, it is not the consequences of criteria like costs and plans, but they are essential components of safety risk management.

In the past, this viewpoint has not been taken into consideration, but the idea of integrated protection is important to be used today. Risk identification and security management systems are a better and more streamlined security performance assessment methodology. Integrated risk assessment uses policies as well as methodologies for realistic protection. Risk management of web applications has become an important task. It computer security is crucial about everything from primary education to intrinsic engineering towards the 21st century [8,9]. Because of the apparent increase and the users reliance on software growth, software applications must be extremely safe everywhere [10].

Over the years we have been making attempts to expand the security of applications to increase transparency and to evaluate how and by what degree our improvements in technology and systems make our applications safer. 'Design compromise' has been found in most situations to be one of the most serious security risks. To minimize "time-to-market," engineers prefer to hasten the design process, which ensures that protection is not built into a product but squeezed from outside. This means that the protection must be taken into account during early stage of software development. According to McGraw [11], risk management system, touch points and expertise are three pillars of application security. Therefore, risk management is one of the main issues to focus upon, if one wishes to improve security. If a threat compromises vulnerability, the risk can be described as the possibility for failure or harm. Development team normally relies on knowledge and experience for risk management without appropriate frameworks for risk management.

Quantification of the security risk factors with previous approaches is very challenging. Sodiya et al. have suggested that appropriate measurement, which itself is a very complicated process, is necessary to determine the real security of any software [12]. The comprehensive fuzzy modeling needed for safety risk evaluation has been divided into two important forms by Shamala et al. [13]: Conventional and Conceptual models based on the study of fuzzy sets. In the context of durable application development, there are few types of security risk assessment. Developers usually discuss several decision-making issues. The design of software development is influenced by enforced complexities which rely mainly on the thinking process of the individual during production about security risk management. Saleh et al. designed a security risk assessment method [14].

The researchers have measured the safety hazards of machines by using fuzzy numbers. For instance, in security risk management [15], Ming-Chang Lee has used sets. The hierarchical analysis interpretation system of safety risk was used by Shedden and others to build a software qualitative safety risk assessment [16] model. Some researchers have used the term of fuzzy inference to characterize the process of uncertainty and analytical hierarchy for structural building and thus rating the various risk factors involved in the software development process [14–16]. Some other researchers have also investigated about the protection strategies including the hierarchical characterization and acceptance.

Nevertheless, authors of the present study work have not found any research that focuses on evaluating the impact of security risk for improving security durability of web applications with the help of Fuzzy based Decision-Making Process. That is why our research, in general, evaluated the impact of several security risks factors by using the Fuzzy-TOPSIS method.

The rest of this study is organized as follows: In Section 2, the paper describes the identification and assessment of software security risks at design phase. Section 3 discusses the hybrid fuzzy AHP-TOPSIS methodology and the impact of security risk analysis for web application has been evaluated. Finally, discussion and conclusions are chronicled in Section 4.

2 Identification and Assessment of Software Security Risks at Design Phase

Since the risk management in itself requires professional expertise, the design manager is not necessarily the right person to conduct risk assessment. Thorough review of risk depends heavily on a knowledge of economic impacts including knowledge of legislation and regulation and the software-supported business model. Software designers and developers construct some hypotheses about their systems and the threats they pose and, at a reasonable level, risk and protection experts help in testing the hypotheses of best practices.

Successful techniques of risk analysis have distinct benefits and drawbacks, but most of them have similar good concepts and limitations when they are implemented in advanced software design. This is the capacity to apply classic risk concepts to application design and then to establish specific mitigation criteria that distinguishes a significant risk evaluation from a merely average software evaluation. In the software development process, a high-level strategy to adaptive risk analysis would be thoroughly incorporated [4]. Software security risk management has become a critical task. Towards moving the twenty-first century, software security has become essential for everything from basic education to inherent engineering. As risks are everywhere, so software applications need to be highly secure because of enormous investment and dependency of the users on software development [11]. The following Fig. 1 shows the security risk management process for a software development project.

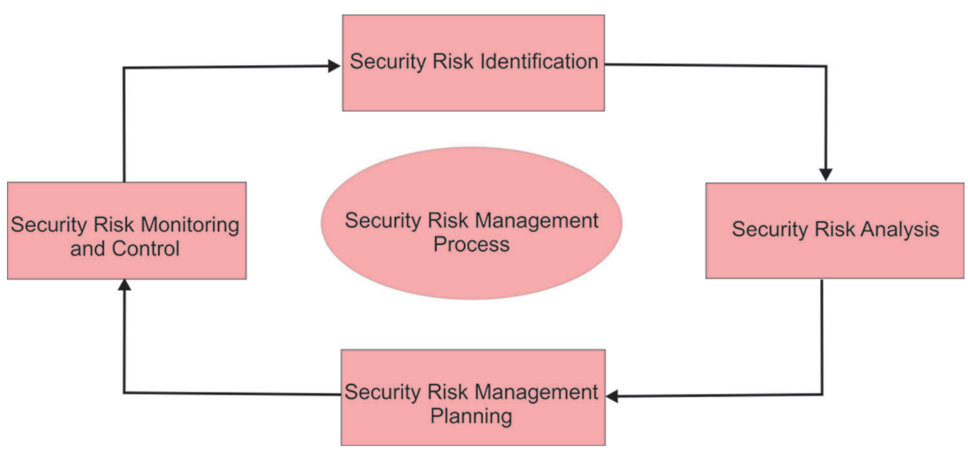

Figure 1: Security risk management process

The essence of the security threats in question should be well known to designers of software development process as they have been shown to have a significant effect on time and production costs. Recognition of security threats and their causes during development may also help developers take initial measures and necessary actions to resolve those threats. It has been found that software computing evaluation of security risks can significantly improve durable software security. The security risk elements software design was first described in this paper. In addition, the hybrid fuzzy AHP-TOPSIS technique is used to measure the impact of these security risks.

2.1 Identification of Design-Level Software Security Risks

Today most service providers are based on technology around the world. It implementation in almost every sector has increased significantly. This makes it important for security issues to be overcome as security breaches can have devastating effects on human lives. Gary McGraw pointed out earlier that protection cannot be poured on any software following its production, but must be evaluated in the development phases [17–19]. It would help develop apps that can actively defend against attack vectors, while relying on some security software application (say, antivirus) to safeguard itself from attacks [20,21]. The key explanation for the excessive breach of security is that loopholes are found in the final product. The early identification and resolution of these inconsistencies can lead to the reduction of these challenges. In general, the design process attempts to prevent errors from being implemented [22,23]. Therefore, the security vulnerabilities that arise during the design stage of the life cycle of software development have to be resolved in order to decrease the incidence of security breaches. In the initial step, recognizing the safety threats that can be addressed would help "install" protection into the program.

The concept of tackling safety problems during the early phases in the software development life cycle is now stressed upon by most researchers. Effective identification and removal of safety threats can help to fix the prevailing security concerns in the production of apps. Devanbu et al. [24] have emphasized on the consideration of security issues at every phase of development life cycle. The authors have also outlined the idea of refining the requirement and design processes so as to shift the focus on initial developmental levels. Baker et al. have dragged the focus towards the lack of valid methodology to quantify the effectiveness of the security measures. According to the authors, it is not the scarcity of security methodologies that hinders the development of secure software, but the absence of proper quantification tools [25,26].

Mehta [27] has highlighted the idea of integrating security in the development process. The author has also stated that the only thing that can help in development of secure software is modifying the development life cycle. Sandeep Gupta [28] has insisted on the application of risk management strategies in the early stages of software development. The author has also proclaimed that late risk management indirectly poses greater threats to secure software development. Steps such as identification of threats, vulnerabilities and determining the appropriate risk mitigation strategies at the design phase have also been proposed by the researcher.

2.2 Need for Design Level Security Risk Identification

Security is widely known to be a combination of two parts, viz., effective risk management and application of proper countermeasures [29,30]. Risk assessment is widely accepted as an integral part of risk management process. The risk assessment process is a complex procedure which consists of the following sub-steps: Identification of various risks; Assessment of the vulnerabilities; Establishment of threats and their countermeasures; Preparation of corrective action plan; and, Review and monitoring. As the first step itself is the identification of the risks, therefore, it becomes a prerequisite to pin them down. Also, the basic aim of risk assessment is to provide apt security levels of a system by ranking the risk on the basis of severity of its impact.

Therefore, recognizing various security threats during the software design phase helps to prevent potential lags which could pose a threat to the security of the system. When the design itself has been intended to measure security risk, it will help minimize the cost and time spent on implementation of security for software. It was found, relative to the design level, that the identification and correction of bugs after production was 100 times crucial [31–33]. Therefore, the security risks associated with software development should be discussed at an early stage.

2.3 Major Security Risks at Design Phase

The researchers have selected the critical risks based on the related security factor. Addressing security factors such as confidentiality, access control, authentication, integrity, etc. has become a pre-requisite for secure software development. Especially today, when each and every individual is primarily concerned about the security of his data, it becomes the prime responsibility of the software developers to effectively address them. Therefore, in this proposed work, the authors have filtered the security risks that may penetrate into the software at design phase from Common Weaknesses Enumeration (CWE) list. The CWE is a community that facilitates the secure software development by providing a list of all possible weaknesses that may occur in any software. It serves as a security tool by providing a standard for identification and mitigation of various software weaknesses. The major design-level security risks, as identified by the researchers have been shown in Tab. 1 and Fig. 2 shows the relation of the security risks with the security factors along with risk-definition.

Table 1: Security risks and related security factor

S. No.	Security Risk at Design Phase	Definition	Related Security Factor
1.	Access to Critical Private Variable via Public Method [34] (ACPVPM)	The software defines a public method for reading or changing a private variable [35].	Access Control; Integrity
2.	Password in Configuration File [34] (PCF)	A secret password is retained in the settings tab, so that any intruder is vulnerable to misuse [36].	Authentication; Access Control
3.	Critical Variable Declared Public [34] (CVDP)	When the security policy allows it to be personal, every sensitive variable/field is made public [37].	Confidentiality; Integrity
4.	Unverified Password Change [34] (UPC)	Once you create a fresh user password, there is no authentication procedure [22].	Authentication; Access Control
5.	Race Condition within a Thread [34] (RCT)	When some resource is being used concurrently, the resources could be used when the operation state is null and therefore undefined [23].	Integrity
6.	Untrusted Search Path [34] (USP)	For essential resources which may lead to resources which are not explicitly managed by the program, an externally defined search path may be used [24].	Confidentiality; Integrity; Availability; Access control
7.	Download of Code Without Integrity Check [34] (DCIC)	The executable program code can be retrieved without inspecting the origins and validity of the program from any distant location [35].	Integrity; Confidentiality
8.	Concurrent Execution using Shared Resource with Improper Synchronization (‘Race Condition’) [34] (RC)	The software includes a sequence of code which may overlap with other code, and the sequence of code requires immediate, exclusive access to the common resource; however, a time period exists where the share resource may be changed with another similarity code sequence [36].	Integrity; Confidentiality
9.	External Initialization of Trusted Variables or Data Stores [34] (EITV)	The software uses inputs which can be altered by dubious actors to preprocess critical inner variables or database servers [37].	Integrity
10.	Improperly Controlled Modification of Dynamically-Determined Object Attributes [34] (ICMD)	When the object contains just internal features, its unintended alteration can lead to weakness [37].	Integrity

3 Methodology and Results

3.1 Hybrid Fuzzy AHP-TOPSIS

Fuzzy AHP (Analytical Hierarchy Process) is a stronger method for assessing difficult decision-making problems by evaluating a common graded target rate for any complex question. With the aid of Fuzzy-AHP,

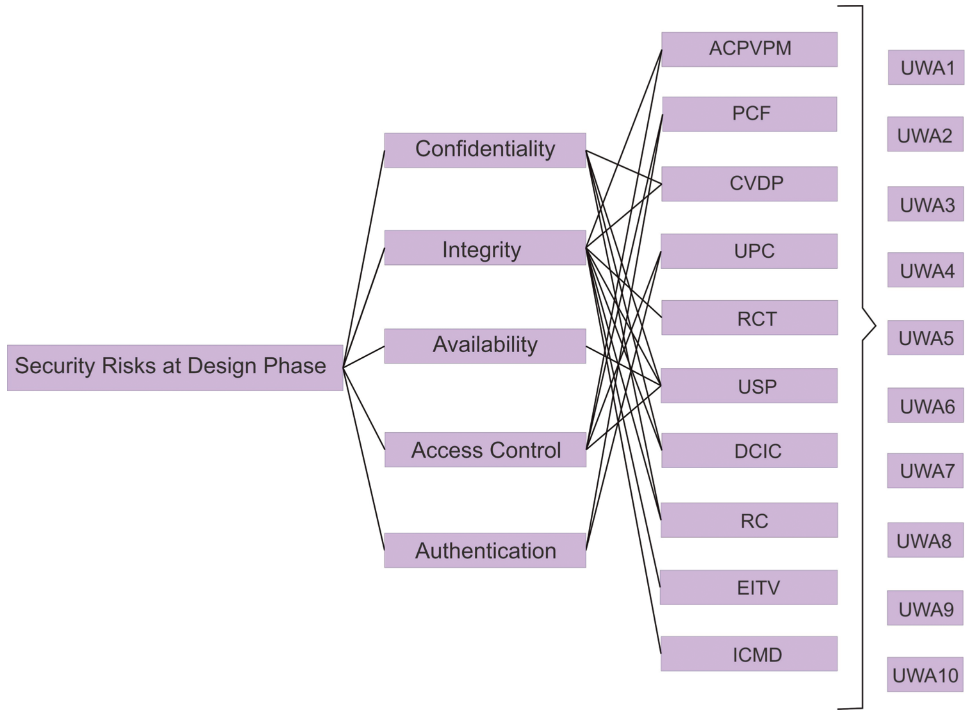

Figure 2: Software security risk attributes in a security-durability design perspective

the problem is separated into a structure such as a tree. AHP is also used as a decision-making tool to measure rank statistics for different alternatives using a variety of hierarchical parameters [3]. To optimize the efficacy of Fuzzy AHP method for a more feasible perspective, the Fuzzy AHP focuses on the Fuzzy Numerical interval of triangular Fuzzy Numbers. These numbers are introduced to decide the weights of interpretative components. Saaty was the first to propose the AHP process [4]. AHP process utilizes only the matrix of the pair-wise analysis to tackle the inaccuracy in challenges of decision labeling in multi-criteria [6]. The model suggested here allows the use of the triangular fuzzy figures to define the linguistic parameters and to incorporate with AHP fuzzy procedures. Because of the inaccuracy and ambiguity, Zadeh developed the fuzzy based set theory to cope with uncertainty [5]. Fig. 2 shows the hierarchy layout for the MCDM problem. This tree layout can be designed by collating the viewpoints and responses of the domain specialists and experts through questionnaires or brainstorming. The next stage is to develop the Triangular Fuzzy Number (TFN) from the Hierarchy of the Tree. A pair-wise assessment of each category of defined goals plays a key role with the aid of one criterion's effect on other criterion.

The Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) considers a multi-criteria decision-making issue of m alternatives like a geometric structure with m points in the n-dimensional space of component. For TOPSIS, the approach used in this research paper is based on the assumption that, for higher and lower ideal solutions, a specified alternative has the shortest and the farthest range from the positive-ideal solution as well as the negative-ideal solution simultaneously [8–15]. Professionals find difficulty in assigning a particular output ranking to an alternative with reference to factor, as shown by Kaur et al. [37]. In compatibility with the actual-world fuzzy setting, this approach applies fuzzy numbers to reflect the relative value of the factor rather than specific numbers. Furthermore, the Fuzzy AHP-TOPSIS approach is especially appropriate for finding solutions of group decision-making in fuzzy settings. Fig. 3 shows the overall weight acquisition process and the feasibility estimation of Fuzzy AHP-TOPSIS methods.

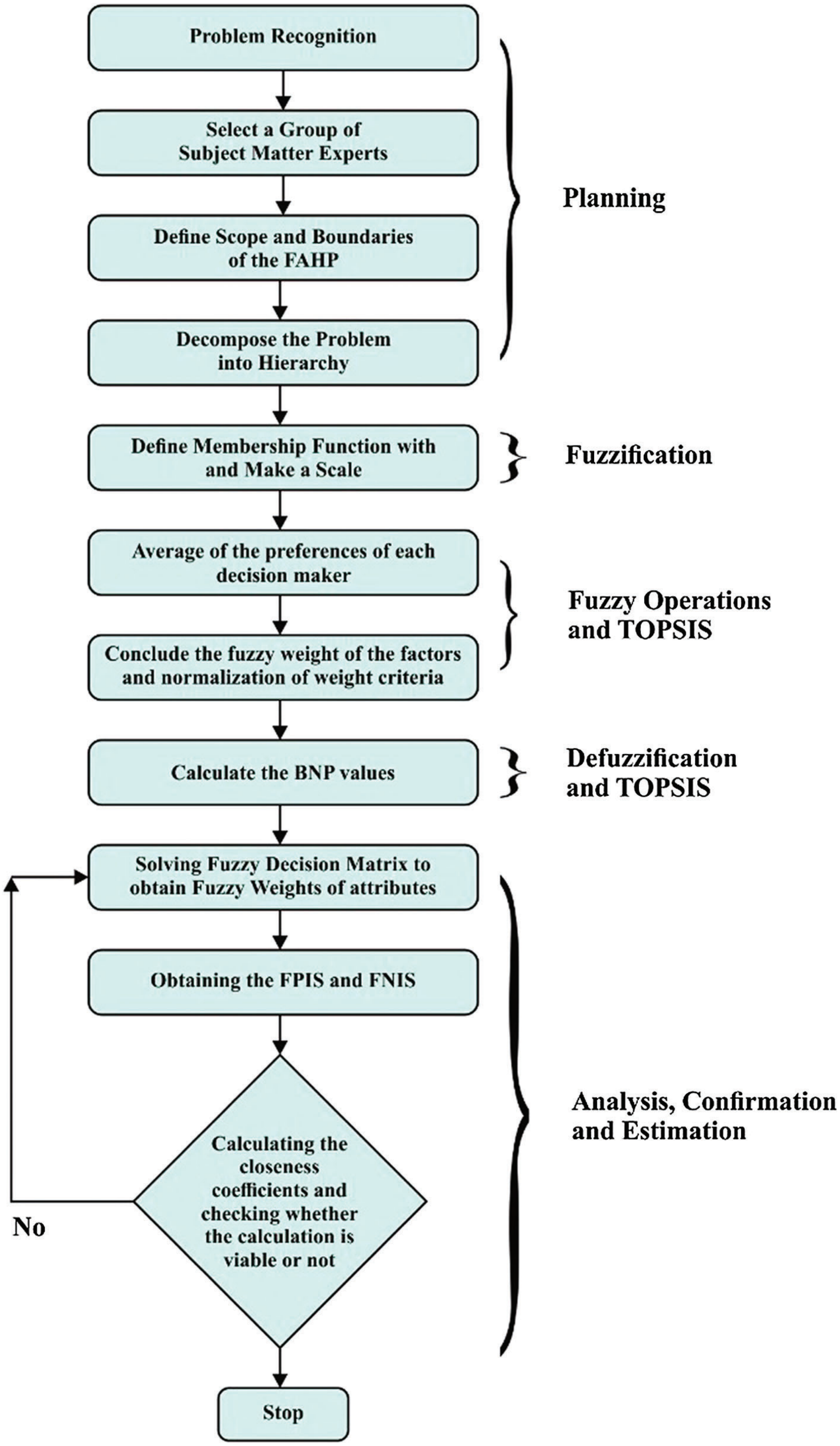

Figure 3: Flow chart of fuzzy AHP-TOPSIS method

3.2 Results

This sub-section discusses different statistical findings of integrated fuzzy AHP-TOPSIS model implementation. Security experts usually do a behavior-based research of risks to analyze about previously identified examples of security risk or family of risk. To achieve this, it is important to identify and characterize questionable behaviors from large sets of signs of implementation. IT security experts and academicians face a complicated task of assessing the impact of risk analysis techniques numerically in current cyber-attack setting. To accomplish the objective, in our research paper, we have used an emphatically established and validated decision-making strategy, the integrated fuzzy AHP-TOPSIS. This technique is conversant for prioritizing the malware analysis techniques based on their impact evaluation in current cyber security setting. For eliciting a more convincing outcome, we took suggestions from 80 IT security experts who come from different software industries and educational backgrounds. The information outsourced from these specialists was collected for our empirical investigations. The different factors for security risk evaluation at design phase, i.e., *Confidentiality, Integrity, Availability, Access Control* and *Authentication* are represented by *T1, T2, T3, T4* and *T5*, respectively. Systematic approach of fuzzy-AHP TOPSIS is used according to Fig. 4 to determine the impact of the mentioned security risks for different institutional web applications represented by *UWA1, UWA2….UWA10*.

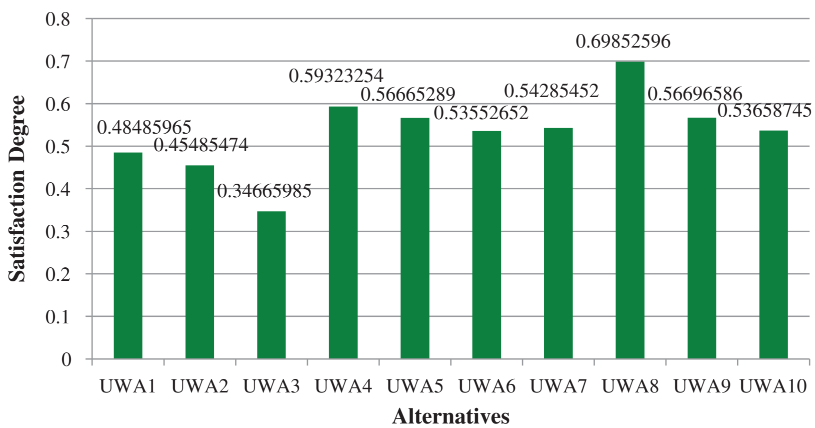

Figure 4: Graphical representation of closeness coefficients to the aspired level among the different alternatives

This was done to determine the variables and calculate the findings. Similarly, the pair-wise comparative matrix of the attributes at level 1 is developed as shown in Tab. 2. Likewise, the composite pair-wise comparative matrix for the level 2 hierarchies has been collated in Tabs. 3–11. Tab. 12 shows the summary of the results. In Tabs. 13 and 14, subjective cognition results of evaluators in linguistic terms, the normalized fuzzy-decision matrix and weighted normalized fuzzy-decision matrix respectively. To be more comprehensive, an integration to measure the weights of the factor of each point is performed. Furthermore, Tab. 15 and Fig. 4 demonstrate the Closeness coefficients to the aspired level among the different alternatives with the help of the hierarchy.

Finally the global weights of factors obtained by fuzzy-AHP are given to fuzzy-TOPSIS method as inputs to generate rank for each alternative. The performance using fuzzy-AHP-TOPSIS has been tested. The determined performance of ten institutional alternatives is as: UWA8, UWA4, UWA9, UWA5, UWA7, UWA10, UWA6, UWA1, UWA2 and UWA3. As per the assessment of this study, UWA8 provides the best security mechanism in security durability perspective among the 10 competitive alternatives.

Table 2: Fuzzy-aggregated pair-wise comparison matrix at level 1

Level 1	T1	T2	T3	T4	T5
T1	1.00000, 1.00000, 1.00000	1.87220, 2.57100, 3.20350	1.46400, 1.68420, 1.97430	1.44610, 2.43850, 3.38650	0.46770, 0.57240, 0.78450
T2	–	1.00000, 1.00000, 1.00000	0.60830, 0.77540, 1.02650	0.77080, 0.95040, 1.23610	0.16300, 0.19530, 0.24970
T3	–	–	1.00000, 1.00000, 1.00000	0.76940, 1.05020, 1.35530	0.20860, 0.24620, 0.31170
T4	–	–	–	1.00000, 1.00000, 1.00000	0.19506, 0.22830, 0.29030
T5	–	–	–	–	1.00000, 1.00000, 1.00000

Table 3: Fuzzy aggregated pair-wise comparison matrix at level 2 for confidentiality

	T11	T12	T13
T11	1.00000, 1.00000, 1.00000	0.69500, 0.95002, 1.34507	1.10486, 1.43805, 1.69062
T12	–	1.00000, 1.00000, 1.00000	1.19028, 1.58206, 2.14970
T13	–	–	1.00000, 1.00000, 1.00000

Table 4: Fuzzy aggregated pair-wise comparison matrix at level 2 for integrity

	T21	T22	T23	T24	T25	T26	T27	T28
T21	1.00000, 1.00000, 1.00000	1.0000, 1.51057, 1.93301	0.48906, 0.63072, 1.00000	0.41052, 0.57430, 1.00000	0.22105, 0.28701, 0.41520	0.31460, 0.46100, 0.87050	0.65750, 1.16530, 1.68830	0.24440, 0.32380, 0.48010
T22	–	1.00000, 1.00000, 1.00000	0.57043, 0.66507, 0.80202	0.30309, 0.39306, 0.56601	0.26790, 0.35201, 0.51706	0.16630, 0.19609, 0.25301	0.39300, 0.57403, 1.05604	0.16920, 0.20706, 0.27509
T23	–	–	1.00000, 1.00000, 1.00000	1.00000, 1.31905, 1.55108	0.30009, 0.43502, 0.80207	0.80207, 0.87005, 1.00000	1.26109, 1.82500, 2.43034	0.17208, 0.20901, 0.26408
T24	–	–	–	1.00000, 1.00000, 1.00000	0.53860, 0.91430, 1.58360	0.60830, 1.05920, 1.68290	0.75030, 1.34650, 1.96110	0.67900, 0.74809, 0.87050
T25	–	–	–	–	1.00000, 1.00000, 1.00000	0.41520, 0.63720, 1.17910	0.94650, 1.10950, 1.24570	0.25000, 0.33000, 0.50000
T26	–	–	–	–	–	1.00000, 1.00000, 1.00000	1.88801, 2.55080, 3.16970	0.80270, 1.03520, 1.31600
T27	–	–	–	–	–	–	1.00000, 1.00000, 1.00000	0.21360, 0.25750, 0.31950
T28	–	–	–	–	–	–	–	1.00000, 1.00000, 1.00000

Table 5: Fuzzy aggregated pair-wise comparison matrix at level 2 for access control

	T41	T42	T43	T44
T41	1.00000, 1.00000, 1.00000	1.07810, 1.59900, 2.11300	0.82006, 1.11108, 1.61500	0.56700, 0.71302, 0.87309
T42	–	1.00000, 1.00000, 1.00000	0.32300, 0.44800, 0.60501	0.25804, 0.31702, 0.41608
T43	–	–	1.00000, 1.00000, 1.00000	0.66601, 1.05604, 1.54207
T44	–	–	–	1.00000, 1.00000, 1.00000

Table 6: Fuzzy aggregated pair-wise comparison matrix at level 2 for authentication

	T51	T52
T51	1.00000, 1.00000, 1.00000	0.66601, 1.05064, 1.54270
T52	–	1.00000, 1.00000, 1.00000

Table 7: Combined pairwise comparison matrix at level 1

	T1	T2	T3	T4	T5	Weights
T1	1.00000	2.55404	1.70170	2.42740	0.59093	0.24000
T2	0.39150	1.00000	0.79640	0.97069	0.20703	0.09500
T3	0.58760	1.25560	1.00000	1.05630	0.25320	0.12000
T4	0.41200	1.02360	0.94670	1.00000	0.23570	0.10300
T5	1.66860	4.82390	3.94950	4.24270	1.00000	0.44200
C.R. = 0.002500						

Table 8: Aggregated pair-wise comparison matrix at level 2 for confidentiality

	T11	T12	T13	Weights
T11	1.00000	0.98530	1.35708	0.36110
T12	1.01490	1.00000	1.62609	0.38730
T13	0.73650	0.61470	1.00000	0.25160
C.R. = 0.002600				

Table 9: Aggregated pair-wise comparison matrix at level 2 for integrity

	T21	T22	T23	T24	T25	T26	T27	T28	Weights
T21	1.00000	1.49120	0.69100	0.64100	0.30027	0.52068	1.16901	0.34300	0.07330
T22	0.67006	1.00000	0.67700	0.41043	0.37204	0.20330	0.64905	0.21501	0.04970
T23	1.44700	1.47701	1.00000	1.29770	0.49350	0.85020	1.83640	0.21400	0.10310
T24	1.56000	2.41370	0.77006	1.00000	0.96360	1.10240	1.35110	0.73190	0.12710
T25	3.30360	2.68530	2.02630	1.03780	1.00000	0.71720	1.10280	0.43500	0.14140
T26	1.89802	4.91880	1.17370	0.90710	1.39430	1.00000	2.38520	1.04730	0.17290
T27	0.85504	1.53970	0.54450	0.74010	0.90679	0.41920	1.00000	0.26210	0.07600
T28	2.91540	4.64900	4.67290	1.36631	2.29890	0.95484	3.81530	1.00000	0.25650
C.R. = 0.03330									

Table 10: Aggregated pair-wise comparison matrix at level 2 for availability

	T31	T32	T33	T34	Weights
T31	1.00000	1.59730	1.16480	0.71680	0.25430
T32	0.6261	1.00000	0.45610	0.32740	0.13000
T33	0.85850		1.00000	1.0804	0.28290
T34	1.39510	3.05440	0.92560	1.00000	0.33260
CR = 0.018700					

Table 11: Aggregated pair-wise comparison matrix at level 2 for access control

	T41	T42	Weights
T41	1.00000	1.08040	0.51930
T42	0.92560	1.00000	0.48070
CR = 0.00000			

Table 12: Summary of the results

Characteristics of Level 1	Local Weights of Level 1	Characteristics of Level 2	Local Weights of Level 2	Global Weights of Level 2
T1	0.24000	T11	0.36110	0.086664
		T12	0.38730	0.092952
		T13	0.25160	0.060384
T2	0.09500	T21	0.07330	0.006964
		T22	0.04970	0.004722
		T23	0.10310	0.009795
		T24	0.12710	0.012075
		T25	0.14140	0.013433
		T26	0.17290	0.016426
		T27	0.07600	0.007220
		T28	0.25650	0.024368
T3	0.12000	T31	–	0.120000
T4	0.10300	T41	0.25430	0.026193
		T42	0.13000	0.013390
		T43	0.28290	0.029139
		T44	0.33260	0.034258
T5	0.44200	T51	0.51930	0.229531
		T52	0.48070	0.212470

Table 13: Subjective cognition results of evaluators in linguistic terms

	UWA1	UWA2	UWA3	UWA4	UWA5	UWA6	UWA7	UWA8	UWA9	UWA10
T11	5.7300, 7.7300, 9.0900	5.3600, 7.3006, 8.7300	5.5500, 7.5500, 8.9100	1.6400, 3.5500, 5.5500	2.8200, 4.8200, 6.6400	5.0000, 7.0000, 8.4500	5.7300, 7.7300, 9.0000	4.2700, 6.2700, 7.9100	1.6400, 3.5500, 5.5500	2.8200, 4.8200, 6.6400
T12	5.0000, 7.0000, 8.4500	5.7300, 7.7300, 9.0000	4.2700, 6.2700, 7.9100	1.1800, 3.0000, 5.0000	2.8200, 4.8200, 6.7300	5.1800, 7.1800, 8.6400	5.3600, 7.3600, 8.7300	5.3600, 7.3600, 8.7300	1.4500, 3.3600, 5.3006	2.8200, 4.8200, 6.7300
T13	4.2700, 6.2700, 8.0900	3.7300, 5.5500, 7.2700	4.4500, 6.4500, 8.1800	1.6400, 3.5500, 5.5500	2.0900, 3.9100, 5.8200	5.7300, 7.7300, 9.0900	5.3600, 7.3006, 8.7300	5.5500, 7.5500, 8.9100	1.6400, 3.5500, 5.5500	2.0900, 3.9100, 5.8200
T21	5.1800, 7.1800, 8.9100	4.8200, 6.8200, 8.5500	4.6400, 6.6400, 8.5500	0.8200, 2.6400, 4.6400	2.8200, 4.8200, 6.6400	5.0000, 7.0000, 8.4500	5.7300, 7.7300, 9.0000	4.2700, 6.2700, 7.9100	1.1800, 3.0000, 5.0000	2.8200, 4.8200, 6.6400
T22	5.7300, 7.7300, 9.3600	5.5500, 7.5005, 9.2700	5.7300, 7.7300, 9.2700	1.6400, 3.5500, 5.5500	2.8200, 4.8200, 6.7300	4.2700, 6.2700, 8.0900	3.7300, 5.5500, 7.2700	4.4500, 6.4500, 8.1800	1.6400, 3.5500, 5.5500	3.0900, 5.0000, 6.8200

Table 13 (continued).

	UWA1	UWA2	UWA3	UWA4	UWA5	UWA6	UWA7	UWA8	UWA9	UWA10
T23	5.7300, 7.7300, 9.2700	4.2700, 6.2700, 8.1800	4.0900, 6.0900, 8.0900	1.1800, 3.0000, 5.0000	2.0900, 3.9100, 5.8200	4.0900, 6.0900, 7.9100	2.3600, 4.2700, 6.2700	2.4500, 4.2700, 6.2700	1.3600, 3.3600, 5.3600	2.4500, 4.4500, 6.4500
T24	5.1800, 7.1800, 9.0000	4.2700, 6.2700, 8.0900	3.7300, 5.5500, 7.2700	2.8200, 4.8200, 6.7300	3.0900, 5.0000, 6.8200	5.1800, 7.1800, 8.9100	4.8200, 6.8200, 8.5500	4.6400, 6.6400, 8.5500	0.8200, 2.6400, 4.6400	2.3600, 4.2700, 6.1800
T25	2.5500, 4.4500, 6.4500	1.2000, 3.0000, 5.0000	1.3600, 3.3600, 5.3600	4.4500, 6.4500, 8.1800	2.4500, 4.4500, 6.4500	5.7300, 7.7300, 9.3600	5.5500, 7.5005, 9.2700	5.7300, 7.7300, 9.2700	1.6400, 3.5500, 5.5500	3.1800, 5.1800, 7.1800
T26	2.5500, 4.4500, 6.4500	1.0900, 2.8200, 4.8200	0.8200, 2.6400, 4.6400	4.4500, 6.4500, 8.2700	2.3600, 4.2700, 6.1800	5.7300, 7.7300, 9.2700	4.2700, 6.2700, 8.1800	4.0900, 6.0900, 8.0900	1.1800, 3.0000, 5.0000	2.8200, 4.8200, 6.8200
T27	3.5500, 5.5500, 7.2700	1.8200, 3.7300, 5.7300	1.6400, 3.5500, 5.5500	5.7300, 7.7300, 9.2700	3.1800, 5.1800, 7.1800	5.1800, 7.1800, 9.0000	4.2700, 6.2700, 8.0900	3.7300, 5.5500, 7.2700	2.8200, 4.8200, 6.7300	3.5500, 5.5500, 7.3600
T28	2.0900, 4.0900, 6.0900	1.7300, 3.5500, 5.5500	1.1800, 3.0000, 5.0000	5.1800, 7.1800, 8.8200	2.8200, 4.8200, 6.8200	6.2700, 8.2700, 9.4500	5.7300, 7.7300, 9.0000	5.3600, 7.3600, 8.7300	1.4500, 3.3600, 5.3600	3.9100, 5.9100, 7.5500
T31	4.0900, 6.0900, 7.7300	0.7300, 2.2700, 4.2700	1.6400, 3.5500, 5.5500	5.3600, 7.3600, 8.7300	2.0900, 3.9100, 5.8200	5.7300, 7.7300, 9.0900	5.3600, 7.3006, 8.7300	5.5500, 7.5500, 8.9100	1.6400, 3.5500, 5.5500	2.0900, 3.9100, 5.8200
T41	3.5500, 5.5500, 7.2700	0.8200, 2.4500, 4.4500	1.1800, 3.0000, 5.0000	4.1800, 6.0900, 7.6400	2.8200, 4.8200, 6.6400	5.0000, 7.0000, 8.4500	5.7300, 7.7300, 9.0000	4.2700, 6.2700, 7.9100	1.1800, 3.0000, 5.0000	2.8200, 4.8200, 6.6400
T42	4.8200, 6.8200, 8.2700	1.0000, 2.6400, 4.6400	0.7300, 2.4500, 4.4500	5.0000, 7.0000, 8.4500	2.8200, 4.8200, 6.7300	4.2700, 6.2700, 8.0900	3.7300, 5.5500, 7.2700	4.4500, 6.4500, 8.1800	1.6400, 3.5500, 5.5500	3.0900, 5.0000, 6.8200
T43	2.9100, 4.8200, 6.7300	2.8200, 4.8200, 6.7300	1.6400, 3.5500, 5.5500	3.5500, 5.5500, 7.3600	3.0900, 5.0000, 6.8200	5.1800, 7.1800, 8.9100	4.8200, 6.8200, 8.5500	4.6400, 6.6400, 8.5500	0.8200, 2.6400, 4.6400	2.3600, 4.2700, 6.1800
T44	2.5500, 4.4500, 6.4500	1.2000, 3.0000, 5.0000	1.3600, 3.3600, 5.3600	4.4500, 6.4500, 8.1800	2.4500, 4.4500, 6.4500	5.7300, 7.7300, 9.3600	5.5500, 7.5005, 9.2700	5.7300, 7.7300, 9.2700	1.6400, 3.5500, 5.5500	3.1800, 5.1800, 7.1800
T51	2.5500, 4.4500, 6.4500	1.0900, 2.8200, 4.8200	0.8200, 2.6400, 4.6400	4.4500, 6.4500, 8.2700	2.3600, 4.2700, 6.1800	5.7300, 7.7300, 9.2700	4.2700, 6.2700, 8.1800	4.0900, 6.0900, 8.0900	1.1800, 3.0000, 5.0000	2.8200, 4.8200, 6.8200
T52	3.5500, 5.5500, 7.2700	1.8200, 3.7300, 5.7300	1.6400, 3.5500, 5.5500	5.7300, 7.7300, 9.2700	3.1800, 5.1800, 7.1800	5.1800, 7.1800, 9.0000	4.2700, 6.2700, 8.0900	3.7300, 5.5500, 7.2700	2.8200, 4.8200, 6.7300	3.5500, 5.5500, 7.3600

Table 14: The weighted normalized fuzzy-decision matrix

	UWA1	UWA2	UWA3	UWA4	UWA5	UWA6	UWA7	UWA8	UWA9	UWA10
T11	0.00300, 0.01100, 0.03600	0.00200, 0.00900, 0.03000	0.00200, 0.00900, 0.03000	0.00200, 0.01000, 0.03500	0.00100, 0.00500, 0.01800	0.00100, 0.00400, 0.01700	0.00200, 0.00600, 0.02000	0.00100, 0.00500, 0.01900	0.00100, 0.00500, 0.01800	0.00100, 0.00400, 0.01700
T12	0.00400, 0.01400, 0.04400	0.00300, 0.01200, 0.04100	0.00300, 0.01200, 0.04100	0.00500, 0.01600, 0.04800	0.00200, 0.00700, 0.02500	0.00000, 0.00400, 0.01700	0.00200, 0.00800, 0.02500	0.00200, 0.00700, 0.02700	0.00200, 0.00700, 0.02500	0.00000, 0.00400, 0.01700
T13	0.00400, 0.01400, 0.04400	0.00300, 0.01200, 0.04200	0.00300, 0.01200, 0.04200	0.00200, 0.01000, 0.03700	0.00100, 0.00500, 0.01800	0.00000, 0.00200, 0.00900	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02400	0.00100, 0.00500, 0.01800	0.00000, 0.00200, 0.00900
T21	0.00100, 0.00600, 0.01900	0.00200, 0.00600, 0.02000	0.00200, 0.00600, 0.02000	0.00100, 0.00500, 0.01900	0.00100, 0.00500, 0.01800	0.00100, 0.00400, 0.01700	0.00200, 0.00600, 0.02000	0.00100, 0.00500, 0.01900	0.00100, 0.00500, 0.01800	0.00100, 0.00400, 0.01700
T22	0.00100, 0.00500, 0.01800	0.00000, 0.00200, 0.00900	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02400	0.00200, 0.00700, 0.02500	0.00000, 0.00400, 0.01700	0.00200, 0.00800, 0.02500	0.00200, 0.00700, 0.02700	0.00200, 0.00700, 0.02500	0.00000, 0.00400, 0.01700
T23	0.00400, 0.01400, 0.04400	0.00300, 0.01200, 0.04100	0.00300, 0.01200, 0.04100	0.00500, 0.01600, 0.04800	0.00100, 0.00500, 0.01800	0.00000, 0.00200, 0.00900	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02400	0.00100, 0.00500, 0.01800	0.00000, 0.00200, 0.00900
T24	0.00400, 0.01400, 0.04400	0.00300, 0.01200, 0.04200	0.00300, 0.01200, 0.04200	0.00200, 0.01000, 0.03700	0.00100, 0.00500, 0.01800	0.00000, 0.00200, 0.00900	0.00200, 0.00900, 0.03000	0.00200, 0.01000, 0.03500	0.00300, 0.01100, 0.03600	0.00200, 0.00900, 0.03400
T25	0.00100, 0.00600, 0.01900	0.00200, 0.00600, 0.02000	0.00200, 0.00600, 0.02000	0.00100, 0.00500, 0.01900	0.00300, 0.01100, 0.03600	0.00400, 0.01400, 0.04400	0.00300, 0.01200, 0.04100	0.00300, 0.01200, 0.04100	0.00500, 0.01600, 0.04800	0.00500, 0.01600, 0.04900
T26	0.00200, 0.00800, 0.02700	0.00200, 0.00800, 0.02500	0.00200, 0.00800, 0.02500	0.00200, 0.00700, 0.02700	0.00100, 0.00500, 0.01800	0.00400, 0.01400, 0.04400	0.00300, 0.01200, 0.04200	0.00300, 0.01200, 0.04200	0.00200, 0.01000, 0.03700	0.00200, 0.00900, 0.03800
T27	0.00100, 0.00500, 0.01800	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02400	0.00300, 0.01100, 0.03600	0.00100, 0.00600, 0.01900	0.00200, 0.00600, 0.02000	0.00200, 0.00600, 0.02000	0.00100, 0.00500, 0.01900	0.00100, 0.00500, 0.01800
T28	0.00500, 0.01600, 0.04900	0.00300, 0.01300, 0.04500	0.00300, 0.01200, 0.04100	0.00500, 0.01600, 0.04800	0.00500, 0.01600, 0.04900	0.00100, 0.00500, 0.01800	0.00000, 0.00200, 0.00900	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02400	0.00100, 0.00500, 0.01800
T31	0.00000, 0.00200, 0.00900	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02400	0.00100, 0.00500, 0.01800	0.00000, 0.00200, 0.00900	0.00400, 0.01400, 0.04400	0.00300, 0.01200, 0.04200	0.00300, 0.01200, 0.04200	0.00200, 0.01000, 0.03700	0.00100, 0.00500, 0.01800
T41	0.00100, 0.00400, 0.01700	0.00200, 0.00600, 0.02000	0.00100, 0.00500, 0.01900	0.00100, 0.00500, 0.01800	0.00100, 0.00400, 0.01700	0.00100, 0.00600, 0.01900	0.00200, 0.00600, 0.02000	0.00200, 0.00600, 0.02000	0.00100, 0.00500, 0.01900	0.00100, 0.00500, 0.01800
T42	0.00000, 0.00400, 0.01700	0.00200, 0.00800, 0.02500	0.00200, 0.00700, 0.02700	0.00200, 0.00700, 0.02500	0.00000, 0.00400, 0.01700	0.00100, 0.00500, 0.01800	0.00000, 0.00200, 0.00900	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02400	0.00200, 0.00700, 0.02500
T43	0.00000, 0.00200, 0.00900	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02400	0.00100, 0.00500, 0.01800	0.00000, 0.00200, 0.00900	0.00400, 0.01400, 0.04400	0.00300, 0.01200, 0.04100	0.00300, 0.01200, 0.04100	0.00500, 0.01600, 0.04800	0.00100, 0.00500, 0.01800

Table 14 (continued).

	UWA1	UWA2	UWA3	UWA4	UWA5	UWA6	UWA7	UWA8	UWA9	UWA10
T44	0.00000, 0.00200, 0.00900	0.00200, 0.00900, 0.03000	0.00200, 0.01000, 0.03500	0.00300, 0.01100, 0.03600	0.00200, 0.00900, 0.03400	0.00400, 0.01400, 0.04400	0.00300, 0.01200, 0.04200	0.00300, 0.01200, 0.04200	0.00200, 0.01000, 0.03700	0.00100, 0.00500, 0.01800
T51	0.00400, 0.01400, 0.04400	0.00300, 0.01200, 0.04100	0.00300, 0.01200, 0.04100	0.00500, 0.01600, 0.04800	0.00500, 0.01600, 0.04900	0.00100, 0.00500, 0.01800	0.00000, 0.00200, 0.00900	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02400	0.00100, 0.00500, 0.01800
T52	0.00400, 0.01400, 0.04400	0.00300, 0.01200, 0.04200	0.00300, 0.01200, 0.04200	0.00200, 0.01000, 0.03700	0.00200, 0.00900, 0.03800	0.00400, 0.01400, 0.04400	0.00300, 0.01200, 0.04200	0.00300, 0.01200, 0.04200	0.00200, 0.01000, 0.03700	0.00100, 0.00500, 0.01800

Table 15: Closeness coefficients to the aspired level among the different alternatives

Alternatives (A)	di+	di−	Gap Degree of CCi+	Satisfaction Degree
UWA1	1.2495427	1.3331256	0.51654874	0.48485965
UWA2	0.6994547	0.8458648	0.54765985	0.45485474
UWA3	0.7877546	1.4845648	0.65435265	0.34665985
UWA4	2.1654572	1.4845648	0.40765952	0.59323254
UWA5	2.0054512	1.5363265	0.43452645	0.56665289
UWA6	0.4487545	0.3975488	0.46552158	0.53552652
UWA7	1.0054646	1.5368897	0.48874574	0.54285452
UWA8	0.4324645	0.3768998	0.42385958	0.69852596
UWA9	2.5254512	1.5368852	0.43455847	0.56696586
UWA10	0.4548745	0.4051254	0.46596589	0.53658745

4 Conclusion

If security problems are addressed in their evolving stages, it will help to reduce security infringements significantly. Priority should be given to the constructive approach to developing safe apps. When any lapses are found at the early stage it is supposed to result in more effective and stable applications. The use of object oriented technology continues to increase naturally in today's world, where almost everything is done digitally. It is difficult to ignore the security factor at the same time. Therefore it can be very good for safe software creation in future if these threats of security are related to object-focused properties of design.

In order to accurately interdependence, the researchers can also quantify the relation between these risks and object-oriented design properties. An accurate, effective and reliable program can be used to establish exact mutual reliability. In this study, the Alternative (UWA8) has been determined to provide most effective and durable security framework among all 10 competing choices. With the assessment of information protection in security strategies for the university web application provides guidance and assists practitioners for designing high-quality software products that offer reliable and trustworthy frameworks for protection against both internal and outside threats and attacks.

Acknowledgement: This Project was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, under grant No. G-323-611-1441. The authors, therefore, gratefully acknowledge DSR technical and financial support.

Funding Statement: Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, Kingdom of Saudi Arabia, under grant No. G-323-611-1441.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. T. J. Ansari, D. Pandey and M. Alenezi, "STORE: Security threat oriented requirements engineering methodology," *Journal of King Saud University-Computer and Information Sciences*, pp. 1–17, 2018.

[2] R. Kumar, S. A. Khan and R. A. Khan, "Fuzzy analytic hierarchy process for software durability: Security risks perspective," *Advances in Intelligent Systems and Computing*, vol. 508, pp. 469–478, 2017.

[3] S. A. Khan, M. Alenezi, A. Agrawal, R. Kumar and R. A. Khan, "Evaluating performance of software durability through an integrated fuzzy-based symmetrical method of ANP and TOPSIS," *Symmetry*, vol. 12, no. 4, pp. 1–15, 2020.

[4] A. Agrawal, M. Zarour, M. Alenezi, R. Kumar and R. A. Khan, "Security durability assessment through fuzzy analytic hierarchy process," *PeerJ Computer Science* vol. 8, pp. 1–43, 2019.

[5] R. Kumar, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal *et al.,* "A knowledge based integrated system of hesitant fuzzy set, AHP and TOPSIS for evaluating security-durability of web applications," *IEEE Access*, vol. 8, no. 2, pp. 48870–48885, 2020.

[6] M. T. J. Ansari and D. Pandey, "An integration of threat modeling with attack pattern and misuse case for effective security requirement elicitation," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 3, pp. 24–29, 2018.

[7] R. Kumar, M. Zarour, M. Alenezi, A. Agrawal and R. A. Khan, "Measuring security-durability through fuzzy based decision-making process," *International Journal of Computational Intelligence Systems*, vol. 12, no. 2, pp. 627–642, 2019.

[8] M. T. J. Ansari, D. Pandey and N. A. Khan, "Comparative literature analysis on security requirements engineering," *International Journal of Engineering Sciences and Research Technology*, vol. 8, no. 12, pp. 113–124, 2019.

[9] R. Kumar, S. A. Khan, A. Agrawal and R. A. Khan, "Measuring the security attributes through fuzzy analytic hierarchy process: Durability perspective," *ICIC Express Letters–An International Journal of Research and Surveys*, vol. 12, no. 6, pp. 615–620, 2018.

[10] R. Kumar, S. A. Khan and R. A. Khan, "Durability challenges in software engineering," *CrossTalk–The Journal of Defense Software Engineering*, vol. 32, no. 8, pp. 29–31, 2016.

[11] G. McGraw, "Software security," *IEEE Security & Privacy Magazine*, vol. 2, no. 2, pp. 80–83, 2004.

[12] A. S. Sodiya, S. A. Onashoga and O. B. Ajayĩ, "Towards building secure software systems," *Issues in Informing Science and Information Technology*, vol. 3, no. 12, pp. 35–42, 2006.

[13] P. Shamala, R. Ahmad and M. Yusoff, "A conceptual framework of info structure for information security risk assessment (ISRA)," *Journal of Information Security and Applications*, vol. 18, no. 1, pp. 45–52, 2013.

[14] Z. I. Saleh, H. Refai and A. Mashhour, "Proposed framework for security risk assessment," *Journal of Information Security*, vol. 2, no. 2, pp. 85–90, 2011.

[15] M. C. Lee, "Information security risk analysis methods and research trends: AHP and fuzzy comprehensive method," *International Journal of Computer Science and Information Technology*, vol. 6, no. 1, pp. 29–35, 2014.

[16] P. Shedden, R. Scheepers, W. Smith and A. Ahmad, "Incorporating a knowledge perspective into security risk assessments," *ICIC Express Letters-An International Journal of Research and Surveys*, vol. 12, no. 14, pp. 4567–4573, 2011.

[17] P. Kocher, R. Lee, G. McGraw and A. Raghunathan, "Security as a new dimension in embedded system design," *Proceedings of the 41st Annual Design Automation Conference IEEE*, vol. 25, pp. 753–760, 2004.

[18] K. Sahu, R. Shree and R. Kumar, "Risk management perspective in SDLC," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, no. 3, pp. 1247–1251, 2014.

[19] R. Kumar, S. A. Khan and R. A. Khan, "Revisiting software security: durability perspective," *International Journal of Hybrid Information Technology*, vol. 8, no. 2, pp. 311–322, 2015.

[20] K. Sahu and R. K. Srivastava, "Soft computing approach for prediction of software reliability," *ICIC Express Letters*, vol. 12, no. 12, pp. 1213–1222, 2018.

[21] R. Kumar, S. A. Khan and R. A. Khan, "Software security durability," *International Journal of Computer Science and Technology*, vol. 5, no. 2, pp. 23–26, 2014.

[22] K. Sahu and Rajshree, "Stability: Abstract roadmap of security," *American International Journal of Research in Science, Engineering and Mathematics*, vol. 2, no. 9, pp. 183–186, 2015.

[23] A. Agrawal, M. Alenezi, R. Kumar and R. A. Khan, "Measuring the sustainable-security of web applications through a fuzzy-based integrated approach of AHP and TOPSIS," *IEEE Access*, vol. 7, pp. 153936–153951, 2019.

[24] P. T. Devanbu and S. Stubblebine, "Software engineering for security: A roadmap," *Proceedings of the Conference on the Future of Software Engineering, IEEE*, vol. 254, pp. 227–239, 2000.

[25] R. Kumar, S. A. Khan and R. A. Khan, "Durable security in software development: Needs and importance," *CSI Communication*, vol. 39, no. 7, pp. 34–36, 2015.

[26] K. Sahu and R. K. Srivastava, "Needs and importance of reliability prediction: An industrial perspective," *Information Sciences Letters*, vol. 9, no. 1, pp. 33–37, 2020.

[27] D. M. Mehta, "Effective software security management," *Technical Report*, OWASP, 2007. [online]. Available: https://www.owasp.org/images/2/28/Effective_Software_Security_Management.pdf, last visit Aug 20, 2020.

[28] J. Kaur, A. Agrawal and R. A. Khan, "Major software security risks at design phase," *ICIC Express Letters–An International Journal of Research and Surveys*, vol. 12, no. 14, pp. 4578–4584, 2018.

[29] K. Sahu and R. Shree, "Software security: A risk taxonomy," *International Journal of Computer Science and Engineering Technology*, vol. 7, no. 3, pp. 36–41, 2015.

[30] A. H. Seh, M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal *et al.,* "Healthcare data breaches: Insights and implications," *Healthcare*, vol. 8, no. 133, pp. 1–18, 2020.

[31] K. Sahu and R. Shree, "Helpful and defending actions in software risk management: A security viewpoint," *Integrated Journal of British*, vol. 4, pp. 1–7, 2015.

[32] M. Alenezi, R. Kumar, A. Agrawal and R. A. Khan, "Usable-security attribute evaluation using fuzzy analytic hierarchy process," *ICIC Express Letters–An International Journal of Research and Surveys*, vol. 13, no. 6, pp. 453–460, 2019.

[33] K. Sahu and R. K. Srivastava, "Revisiting software reliability," *Data Management, Analytics and Innovation (Advances in Intelligent Systems and Computing)*. Springer, vol. 808, pp. 221–235, 2019.

[34] Weaknesses introduced during design, Common Weakness Enumeration, 2008. [online]. Available: https://cwe.mitre.org/data/definitions/701.html.

[35] CWE-767: Access to critical private variable via public method, Common Weakness Enumeration, 2009. [online]. Available: https://cwe.mitre.org/data/definitions/767.html.

[36] CWE-915: Improperly controlled modification of dynamically-determined object attributes, Common Weakness Enumeration, 2013. Available: https://cwe.mitre.org/data/definitions/915.html, last visit Aug 20, 2020.

[37] J. Kaur, A. I. Khan, Y. B. Abushark, M. M. Alam, S. A. Khan *et al.,* "Security risk assessment of healthcare web application through adaptive neuro-fuzzy inference system: A design perspective," *Risk Management and Healthcare Policy,* Dove Press, vol. 13, no. 5, pp. 355–371, 2020.