Computers, Materials & Continua
DOI:10.32604/cmc.2021.016610
Article

Tech Science Press

Usability Evaluation Through Fuzzy AHP-TOPSIS Approach: Security Requirement Perspective

Yoosef B. Abushark[1], **Asif Irshad Khan**[1,*], **Fawaz Jaber Alsolami**[1], **Abdulmohsen Almalawi**[1], **Md Mottahir Alam**[2], **Alka Agrawal**[3], **Rajeev Kumar**[3,4] **and Raees Ahmad Khan**[3]

[1]Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[2]Department of Electrical and Computer Engineering, Faculty of Engineering, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[3]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, 226025, India
[4]Department of Computer Application, Shri Ramswaroop Memorial University, Barabanki, 225003, India
[*]Corresponding Author: Asif Irshad Khan. Email: aikhan@kau.edu.sa

Received: 06 January 2021; Accepted: 06 February 2021

Abstract: Most of the security strategies today are primarily designed to provide security protection, rather than to solve one of the basic security issues related to adequate software product architecture. Several models, frameworks and methodologies have been introduced by the researchers for a secure and sustainable software development life cycle. Therefore it is important to assess the usability of the popular security requirements engineering (SRE) approaches. A significant factor in the management and handling of successful security requirements is the assessment of security requirements engineering method performance. This assessment will allow changes to the engineering process of security requirements. The consistency of security requirements depends heavily on the usability of security requirements engineering. Several SRE approaches are available for use and each approach takes into account several factors of usability but does not cover every element of usability. There seems to be no realistic implementation of such models because the concept of usability is not specific. This paper aims at specifying the different taxonomy of usability and design hierarchical usability model. The taxonomy takes into account the common quality assessment parameters that combine variables, attributes, and characteristics identified in different approaches used for security requirements engineering. The multiple-criteria decision-making (MCDM) model used in this paper for usability evaluation is called the fuzzy AHP-TOPSIS model which can conveniently be incorporated into the current approach of software engineering. Five significant usability criteria are identified and used to evaluate the six different alternatives. Such strategies are graded as per their expected values of usability.

Keywords: Security requirements engineering; cyber-security; usability; fuzzy logic; MCDM

1 Introduction

It is evident that the digital age is now a much more threatening place. Electronic devices are progressively connected, making it easier for adversaries to attack virtually everyone in the world, often with quite minimal harm. Even basic software that shows or changes local files needs to be safe since users can access or modify high-risk documents that are received via e-mail. Sadly, many software engineers never learnt to write stable apps. With the increase of cybercrime, application security has becoming a major challenge for system managers and cyber users worldwide [1,2]. For an application development organization, security is critical to implement during software development process [3,4]. They must not only secure and build the software they construct, but must also maintain the data protection that any individuals creates and enters. The software users input may be unbelievably personal details based on the programme.

All the relevant details that people will definitely like privately are things like emails, identities or even bank account numbers. Therefore security is crucial to ensure the information is safe, the connection between the company and its customers clearly evolves and improves. If user knows that his data is safe, he would certainly retain their dealings with a software development firm. Software should be compatible from the outset of engineering and design and provide a unified security infrastructure that takes security concepts into consideration. Designers, architects, and experts have acute expectations and possible threats to record. For any step of the software development cycle, risk assessment is a basic requirement. And most significantly, it's a must to secure the application from any modern fraudulent code intervention after software has been transferred, maintained and up-dated from time to time. The entire process of creation is skewed. Individuals may care about completely inconsequential pieces of software which are installed early in the project and then run through valuable aspects close to the end.

Activities such as quality control, normally near the final step, are streamlined and minimized [5]. Globally Security Spending explores technical, manufacturing, company and regional security opportunities. According to a revised IDC estimate, worldwide hardware, software and services spending in 2019 is expected to hit 106.6 billion dollars, up 10.7% from 2018. In 2023 this volume would hit a compound annual growth rate (CAGR) of 151.2 billion dollars (9.4 percent) over the forecast timeline 2019–2023. ICT expenditure remains largely stagnant in 2020 as a result of the COVID-19 pandemic after years of rise. The global market will be propelled back to the rise of over 2× GDP as emerging innovations start to take into account a bigger market share, even though conventional ICT expenses are expected to follow GDP rise over the next decade. IOT has already been developing and would increase over 5–10 years to cover more than 25 per cent of ICT investment, and would be powered by technological innovations like robotics, artificial intelligence [4]. Fig. 1 shows the IDC forecast report on ICT spending worldwide 2018 to 2023.

In order to manage security issues it is important to put together enterprise, growth and security groups to identify the main intolerances and business implications induced by risk of security vulnerabilities. Since SDLC is an intake forwarding method and flaws implemented in this step will be distributed in the next implementation phase, it is essential to investigate potential risks at very initial stages. The majority of security bugs found in software and systems were triggered by deficiencies in the methodology for software development process. In order to address this issue, elements of security quality management along the software development life cycle would be described, in general the best practices for security requirement elicitation.

There are numerous security requirements engineering approaches with some advantages and disadvantages developed by different authors. It is a big challenge for the new security practitioners to select the most effective and well-organized security requirements engineering method in the software development process. In this research we implement a MCDM model based methodology to select the most effective SRE approach. Over the past couple of decades, software engineering standards have evolved to deliver high quality software applications. As per the International Standard Organization [6–8] there've been various quality parameters such as efficiency, effectiveness, reliability, usability, etc. The overall quality aspects are Functionality, Reliability, Usability, Efficiency, Maintainability and Portability. Amongst all these quality parameters, usability is an important performance factors for applications those necessities to be examined during project management. The word usability is extracted from user-friendly terms. Numerous software engineering practitioners describe usability in their own words [9–12].

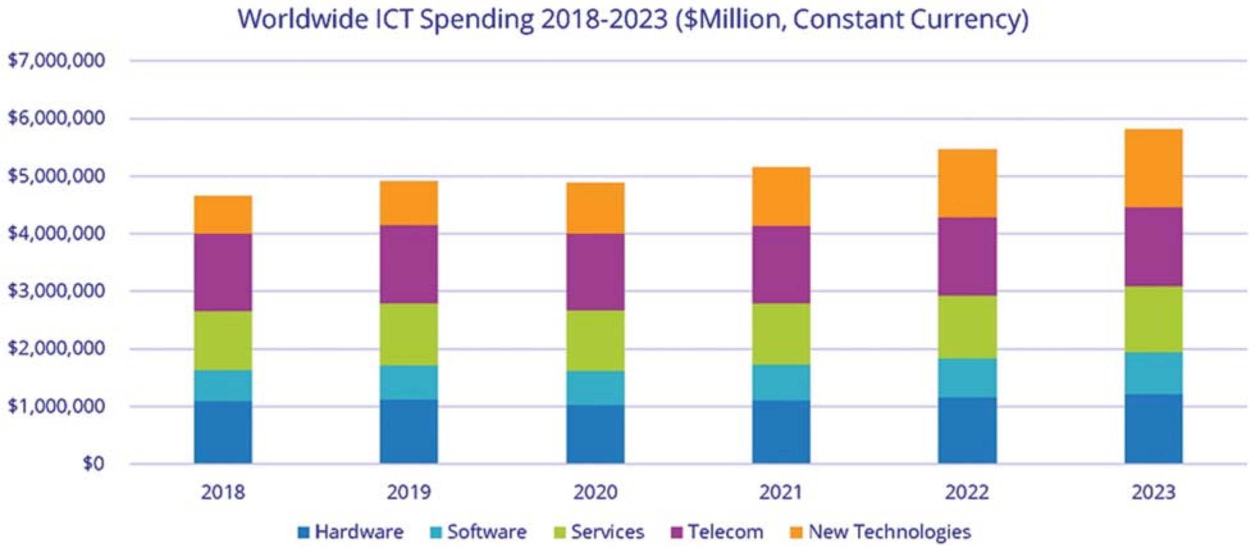

Figure 1: Global ICT spending forecast 2020–2023

The assortment of an effective security requirements engineering method is a multi-criteria decision-making (MCDM) issue [13–15] where several usability criteria are identified in the decision-making procedure. In addition, in the evaluation practice, the issue of security requirements engineering method selection consists of some dependency characteristics, such as subjectivity, vagueness, complexity and ambiguity. This research therefore uses a model focused on AHP [16–18], fuzzy sets [19–22] and TOPSIS [23–26] to rank the effective SRE approach. On the one side, the "AHP" can be used to evaluate the weights of and criterion, and the "fuzzy sets" are used to resolve the vagueness involved with linguistic terms and triangular fuzzy numbers (TFNs). On the other side, "TOPSIS" is proposed to obtain a priority ranking for security requirements engineering approaches [27–30]. Using the hybrid AHP and fuzzy TOPSIS techniques, the statistical capacity of the proposed approach is simple and can be easily configured into an excel sheet. In addition, the integrated strategy has some clear reasoning that is easy to grasp and reflects a human decision. One of the essential reasons for using the fuzzy TOPSIS approach is that it removes the issue of rank reversal, whereas the separate AHP and fuzzy AHP methods do not eliminate the issue of rank reversal.

The rest of this article is arranged as follows. The different security requirements engineering approaches is presented in Section 2. In Section 3, the requisite usability assessment criteria that are needed to select effective SRE approach are added. Section 4 describes the brief implementation of the proposed hybrid model. Section 5 defines a numerical specification focused on the application of the proposed MCDM model. It also addresses the findings and their confirmation. The conclusion is ultimately stated in the Section 6.

2 Security Requirements Engineering

Security specifications are technically called non-functional specifications, typically defined as software qualities, which can be transformed to suitable functional requirements. The outcome application will possibly not be tested before deployment for strength or weakness. If the security requirements are non-functional to functional requirements, these represent component of the entire requirements review process and, if problems are unavoidable, they need not be adequately defined and addressed. Simplification SRE approaches is important because it is more likely that a streamlined approach is implemented than a complicated method. It also emphasizes the significance of technical training in the SRE field for developers and design engineers. Some popular security requirements engineering approaches steps are present below in Tab. 1.

Table 1: Step of different security requirements engineering approaches

SQUARE [22]	SREF [23]	STORE [24]	MOSRE [25]	SREP [26]	MSRA [27]
• Agree on definitions • Identify security goals • Develop artifacts • Perform risk assessment • Select elicitation technique • Elicit security requirements • Categorize requirements • Prioritize requirements • Requirements inspection	• Identify business (Functional) requirements • Identify security goals • Identify security requirements • Construct satisfaction arguments	• Identify system goals • Identify and prioritize stakeholders • Agreed upon goals • Asset identification • Security attack analysis • Threat identification and categorization • Risk evaluation and prioritization • Security requirements elicitation • Security requirements validation • Security requirements specification document	• Inception • Elicitation • Elaboration • Negotiation and validation • Specification	• Agree on definitions • Identify vulnerable and/or critical assets • Identify security objectives and dependencies • Identify threats and develop artifacts • Risk assessment • Elicit security requirements • Categorize and prioritize requirements • Requirements inspection • Repository improvement	• Identify stakeholder • Identify episodes • Elaborate security goals • Identify facts and assumption • Refine stakeholder views on episodes • Reconcile security goals • Reconcile security and functional requirements

3 The Proposed Hierarchical Usability Model

The degree to which software is conveniently and comfortably accessible to various types of clients can be described as Usability. Numerous authors have investigated usability in different ways [10–14] however; any description did not encompass all areas of software usability. We discussed in this study that the usability depends on five variables, namely Efficiency, Effectiveness, Learnability, Satisfaction, and Productivity.

This study indicated the integral taxonomy of all principles, variables and characteristics that influence the usability of software systems, as numerous researchers have observed. This taxonomy is represented in Tab. 2. The model is hierarchical in design and takes into account several requirements, which rely on usability. Evaluating usability based on the Tab. 2 and Fig. 2 model may be considered as a challenge with multi-criteria decision-making (MCDM) due to its dynamic structure with its tangible and intangible behavior.

Table 2: Taxonomy of proposed model

Factor	Sub-factor	Description
Efficiency (ST1)	User effort (ST11) Time-effective (ST12)	Once participants have understood about the interface, how easily can they execute the given task?
Effectiveness (ST2)	Operability (ST21) Scalability (ST22) Extensibility (ST23)	When users switch to the prototype after a time of not utilizing it, how quickly can they recover their skills?
Learnability (ST3)	User interface (ST31) Training (ST32) System structure (ST33)	How simple is it for individuals to complete basic tasks the very first time they experience a SRE approach?
Satisfaction (ST4)	Convenience (ST41) Likeability (ST42)	How good is it to utilize the SRE approach?
Productivity (ST5)	Useful output (ST51) Cost-effective (ST52)	How easy for the software designers to implement SRE in the software development firms?

4 Hybrid Fuzzy AHP-TOPSIS Approach

4.1 Fuzzy AHP

Analytical hierarchy process [15] is a mathematical technique to assist discovering solutions to real problems which can be formulated on hierarchical structures by levels of various objectives, factors, and alternatives. Taking into consideration various factors for accomplishing a feasible alternative is the greatest reason for its popularity. The strategy is effective in prioritizing multiple alternatives on the basis of several factors. However, there are some restrictions to this technique. The first restriction is that AHP is designed to handle crisp values and figures. Second, decisions and similarities are decided to make on an inconsistent scale that is difficult to assess. The third barrier of AHP is its lack of unpredictability. Ambiguity is generally linked with various comparative analyses in the AHP method, and therefore there are no strategies for dealing with ambiguity in this procedure. As a possible consequence, the forth barrier is that evaluations are not accurate [14–16].

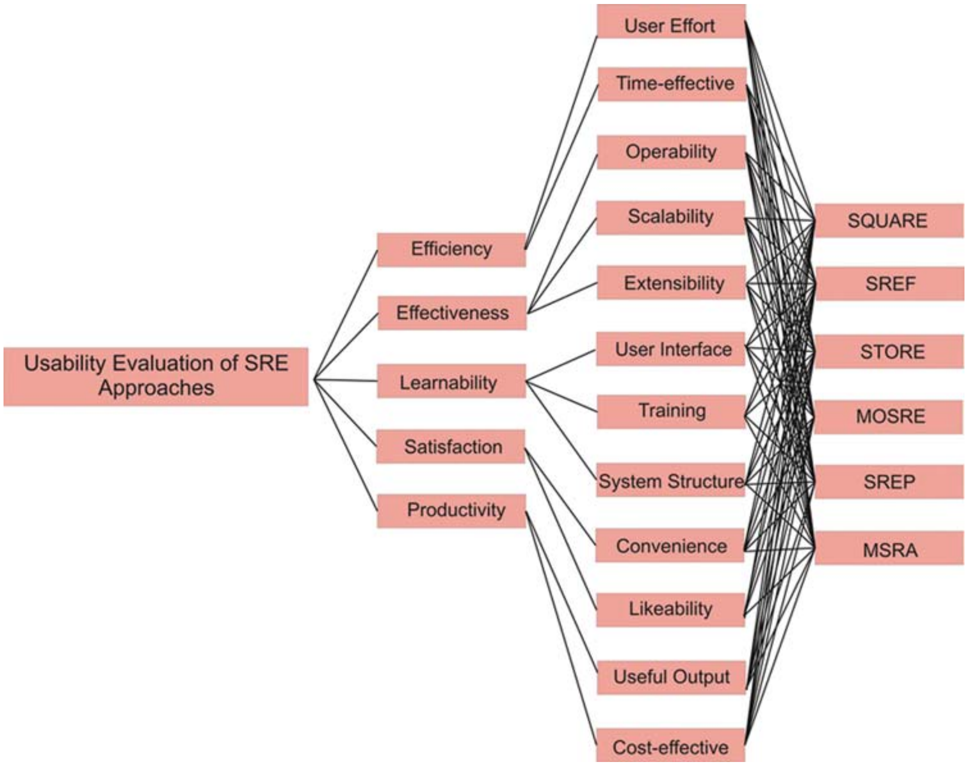

Figure 2: Detailed taxonomy of the hierarchical proposed model

At the end of the evaluation, the findings can be severely impacted by the mentality, predilection and judgment of the experts. In responding, the concepts of fuzzy set model are used in the AHP technique to enhance the evaluation process findings. The combined effect of fuzzy set concept and MCDM techniques in real-world situations case studies has enhanced the research with the relevant structures. This evaluation is accompanied by the [17] research methodology for the fuzzy AHP procedure. In the first place, efficiency points are described and expressed by linguistic words. Linguistic words indicate the exact importance of correlations. Second, the factors can be contrasted. For this reason, a pair-wise comparative analysis of components at the very same stage of the hierarchy is made to show the relative significance of the factors. The fuzzy correlation matrixes utilize triangular fuzzy numbers (TFNs) to show the significance of the factors at each level of the proposed hierarchy. The efficiency ratings are contrasted in the first stage. Linguistic terms are used to show the relative importance of every pair of factors in the same hierarchical structure. After that, in the second phase, fuzzy comparative matrixes are created. TFNs are used to show the relative resilience of each set of factors within the same hierarchical structure. A TFN could be interpreted as (l, mi, u) [18,19]. Domain Experts assigned points as per the scale provided in Tab. 3 to the variables that influence the scores in a numerical manner.

Table 3: TFN scale

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

4.2 *Fuzzy-TOPSIS*

The fuzzy TOPSIS approach is a powerful and efficient MCDM approach. There are many representations in the literary works of Fuzzy TOPSIS. The general concept is that two standards must be met for the chosen alternative. First, this should be the closest point from the ideal solution; as well as second, this should be the farthest width from the target solution. The conventional TOPSIS approach uses crisp values for comparative analysis [20]. As mentioned earlier, the crisp numbers do not comprise an expert judgment. For this reason, research teams use linguistic expressions to replace numerical output in the conventional TOPSIS approach. The fuzzy logic is used to create and evaluate linguistic representations. The fuzzy TOPSIS approach is a combination of TOPSIS with fuzzy logic, formed to deal with ambiguous decision-making complications. 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 [21–30]. Furthermore, the Fuzzy AHP-TOPSIS approach is especially appropriate for finding solutions of group decision-making in fuzzy settings. The overall weight acquisition process and the feasibility estimation performed by Fuzzy AHP-TOPSIS methods. The following Fig. 3 establishes the sequential process of the Fuzzy AHP-TOPSIS methodology.

Next, we assess the weight of the assessment element. The present study introduces Fuzzy AHP to the resolve of problem of fuzzy priority weights. In addition, authors are creating a fuzzy based decision matrix and choosing suitable semantic terms as alternatives to the parameters using Tab. 4.

5 Statistical Data Analysis

This segment delivers a comprehensive explanation of the empirical outcomes, their clarification. Tab. 5 shows the collective pairwise comparison matrix at first level. Tabs. 6–10 demonstrate the aggregated pair-wise assessment matrix at second level for Efficiency, Effectiveness, Learnability, Satisfaction and Productivity respectively. Tab. 11 presents the summary of the results. Tab. 12 presents the subjective cognition consequences of assessors in linguistic terms. Tab. 13 shows the normalized fuzzy-decision matrix. Tab. 14 presents the weighted normalized fuzzy-decision matrix. And finally Tab. 15 presents the closeness coefficients to the aspired level between the different Alternatives. Fig. 4 present the graphical representation of the outcome.

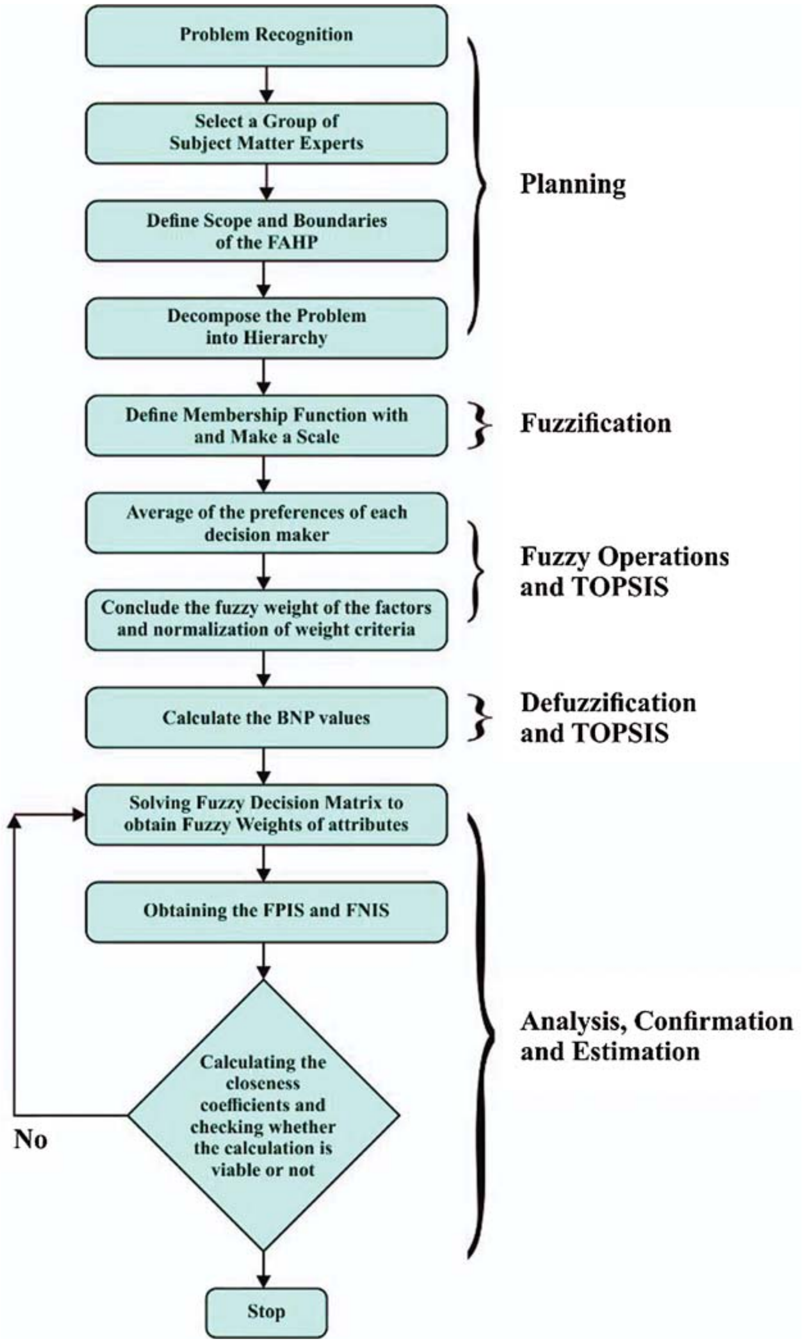
Problem Recognition
Select a Group of Subject Matter Experts
Define Scope and Boundaries of the FAHP
Decompose the Problem into Hierarchy
Planning
Define Membership Function with and Make a Scale
Fuzzification
Average of the preferences of each decision maker
Conclude the fuzzy weight of the factors and normalization of weight criteria
Fuzzy Operations and TOPSIS
Calculate the BNP values
Defuzzification and TOPSIS
Solving Fuzzy Decision Matrix to obtain Fuzzy Weights of attributes
Obtaining the FPIS and FNIS
Calculating the closeness coefficients and checking whether the calculation is viable or not
No
Analysis, Confirmation and Estimation
Stop

Figure 3: Functional diagram of fuzzy AHP-TOPSIS method

With growing usage of the Internet, there is an elevated incidence of malicious software such as viruses impacting a business communications system. The software virus is a component of computer programs that is introduced into another programme and is inactive until it is activated by an unaware person. This cause can be as easy as accessing a file or uploading a document from the internet. With the complication and speed of the software development lifecycle, software engineering is under tremendous pressure to produce market specifications without paying enough attention to the security vulnerabilities that the application might have experienced. With these kinds of security issues, the company would have a problem providing the consistency and availability of the company needed by its clients. However some software firms use security requirements engineering approach during software development process, but even the most advanced SRE approach cannot keep up with the ever-increasing number of malware and malicious programmes out there. This research presents the usability evaluation of different security requirements engineering approaches. Fig. 4 presents the graphical representation of the findings obtained in this study. The finding demonstrates the satisfaction degree of several alternatives is estimated as 0.47548754, 0.38645784, 0.65467548, 0.44575487, 0.46457984 and 0.38496457 for ST1, ST2, ST3, ST4, ST5 and ST6 respectively. The outcome show the ST3 which is STORE methodology has highest usability priority for the assortment of effective and efficient security requirements engineering method.

Table 4: Linguistic scales for the rating

Linguistic variable	Corresponding triangular fuzzy number
Very poor (VP)	(0, 1, 3)
Poor (P)	(1, 3, 5)
Fair (F)	(3, 5, 7)
Good (G)	(5, 7, 9)
Very good (VG)	(7, 9, 10)

Table 5: Combined pairwise comparison matrix at level 1

	ST1	ST2	ST3	ST4	ST5	Weights
ST1	1.00000	2.55440	1.70170	2.42740	0.59930	0.24130
ST2	0.39150	1.00000	0.79640	0.97690	0.20730	0.09530
ST3	0.58760	1.25560	1.00000	1.05630	0.25320	0.12240
ST4	0.41200	1.02360	0.94670	1.00000	0.23570	0.10340
ST5	1.66860	4.82390	3.94950	4.24270	1.00000	0.44160
C.R. = 0.002500						

Table 6: Aggregated pair-wise comparison matrix at level 2 for efficiency

	ST11	ST12	Weights
ST11	1.00000	0.41110	0.29130
ST12	2.43250	1.00000	0.70870
C.R. = 0.000000			

Table 7: Aggregated pair-wise comparison matrix at level 2 for effectiveness

	ST21	ST22	ST23	Weights
ST21	1.00000	0.57340	0.70860	0.24160
ST22	1.74400	1.00000	0.89450	0.37850
ST23	1.41120	1.11790	1.00000	0.37990
C.R. = 0.005800				

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

	ST31	ST32	ST33	Weights
ST31	1.00000	0.59790	0.28390	0.16900
ST32	1.67250	1.00000	0.89050	0.34850
ST33	3.52240	1.12300	1.00000	0.48250
C.R. = 0.022700				

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

	ST41	ST42	Weights
ST41	1.00000	0.82430	0.45184
ST42	1.21320	1.00000	0.54816
C.R. = 0.000000			

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

	ST51	ST52	Weights
ST51	1.00000	0.74470	0.42684
ST52	1.34280	1.00000	0.57316
C.R. = 0.000000			

Table 11: Summary of the results

Main	Local weights	Sub	Local weights	Overall weights	Ranks
ST1	0.24130	S11	0.29130	0.07029069	4
		S12	0.70870	0.17100931	3
ST2	0.09530	S21	0.24160	0.02302448	11
		S22	0.37850	0.03607105	10
		S23	0.37990	0.03620447	9
ST3	0.12240	S31	0.16900	0.02068560	12
		S32	0.34850	0.04265640	8
		S33	0.48250	0.05905800	5
ST4	0.10340	S41	0.45184	0.04672026	7
		S42	0.54816	0.05667974	6
ST5	0.44160	S51	0.42684	0.18849254	2
		S52	0.57316	0.25310746	1

Table 12: Subjective cognition results of evaluators in linguistic terms

	SRE1	SRE2	SRE3	SRE4	SRE5	SRE6
ST11	0.7300, 2.2700, 4.2700	4.8200, 6.8200, 8.2700	1.0000, 2.6400, 4.6400	1.4500, 3.3600, 5.3006	5.0000, 7.0000, 8.4500	2.8200, 4.8200, 6.7300
ST12	0.7300, 2.2700, 4.2700	4.8200, 6.8200, 8.2700	1.0000, 2.6400, 4.6400	4.4500, 6.4500, 8.1800	5.0000, 7.0000, 8.4500	2.8200, 4.8200, 6.7300
ST21	0.8200, 2.4500, 4.4500	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
ST22	4.1800, 6.0900, 7.6400	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
ST23	4.4500, 6.4500, 8.1800	3.0900, 5.0000, 6.8200	2.9100, 4.8200, 6.7300	2.8200, 4.8200, 6.7300	4.4500, 6.4500, 8.1800	3.5500, 5.5500, 7.3600
ST31	1.2000, 3.0000, 5.0000	2.9100, 4.8200, 6.7300	2.8200, 4.8200, 6.7300	5.3600, 7.3600, 8.7300	3.5500, 5.5500, 7.3600	3.0900, 5.0000, 6.8200
ST32	1.0000, 2.6400, 4.6400	2.5500, 4.4500, 6.4500	1.2000, 3.0000, 5.0000	3.5500, 5.5500, 7.3600	4.4500, 6.4500, 8.1800	2.4500, 4.4500, 6.4500
ST33	0.7300, 2.2700, 4.2700	4.8200, 6.8200, 8.2700	1.0000, 2.6400, 4.6400	4.4500, 6.4500, 8.1800	5.0000, 7.0000, 8.4500	2.8200, 4.8200, 6.7300
ST41	0.8200, 2.4500, 4.4500	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
ST42	4.1800, 6.0900, 7.6400	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
ST51	4.4500, 6.4500, 8.1800	3.0900, 5.0000, 6.8200	2.9100, 4.8200, 6.7300	2.8200, 4.8200, 6.7300	4.4500, 6.4500, 8.1800	3.5500, 5.5500, 7.3600
ST52	6.2700, 8.2700, 9.4500	3.1800, 5.1800, 7.0000	1.6400, 3.3600, 5.3600	1.4500, 3.3600, 5.3600	6.2700, 8.2700, 9.4500	3.9100, 5.9100, 7.5500

Table 13: The normalized fuzzy-decision matrix

	SRE1	SRE2	SRE3	SRE4	SRE5	SRE6
ST11	0.4200, 0.6900, 0.9900	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.5400, 0.7500, 0.9300	0.4600, 0.6700, 0.8600	0.1800, 0.4500, 0.7400
ST12	0.2000, 0.4700, 0.7700	0.4600, 0.6700, 0.8600	0.3900, 0.5900, 0.7900	0.4200, 0.6400, 0.8300	0.5000, 0.7100, 0.8900	0.4600, 0.6700, 0.8600
ST21	0.5900, 0.8000, 0.9700	0.5400, 0.7500, 0.9200	0.4600, 0.6700, 0.8600	0.3800, 0.6000, 0.8000	0.4600, 0.6700, 0.8600	0.3500, 0.5800, 0.8100
ST22	0.4600, 0.6700, 0.8600	0.3900, 0.5900, 0.7900	0.5000, 0.7100, 0.8900	0.5200, 0.7400, 0.9400	0.5000, 0.7100, 0.8900	0.4600, 0.6700, 0.8600
ST23	0.5400, 0.7500, 0.9200	0.5200, 0.7400, 0.9400	0.4600, 0.6700, 0.8600	0.3800, 0.6000, 0.8000	0.5400, 0.7500, 0.9200	0.5000, 0.7100, 0.8900
ST31	0.3900, 0.5900, 0.7900	0.4600, 0.6700, 0.8600	0.3800, 0.6000, 0.8000	0.3500, 0.5800, 0.8100	0.4600, 0.6700, 0.8600	0.5000, 0.7100, 0.8900
ST32	0.4600, 0.6700, 0.8600	0.5400, 0.7500, 0.9200	0.5200, 0.7400, 0.9200	0.4600, 0.6700, 0.8600	0.5000, 0.7100, 0.8900	0.4600, 0.6700, 0.8600
ST33	0.4600, 0.6700, 0.8600	0.3900, 0.5900, 0.7900	0.4200, 0.6400, 0.8300	0.5000, 0.7100, 0.8900	0.4600, 0.6700, 0.8600	0.3500, 0.5800, 0.8100
ST41	0.5400, 0.7500, 0.9200	0.4600, 0.6700, 0.8600	0.3800, 0.6000, 0.8000	0.4600, 0.6700, 0.8600	0.3500, 0.5800, 0.8100	0.4600, 0.6700, 0.8600
ST42	0.3900, 0.5900, 0.7900	0.5000, 0.7100, 0.8900	0.5200, 0.7400, 0.9400	0.5000, 0.7100, 0.8900	0.4600, 0.6700, 0.8600	0.5000, 0.7100, 0.8900
ST51	0.5200, 0.7400, 0.9400	0.4600, 0.6700, 0.8600	0.3800, 0.6000, 0.8000	0.5400, 0.7500, 0.9200	0.5000, 0.7100, 0.8900	0.2000, 0.4700, 0.7700
ST52	0.4200, 0.6900, 0.9900	0.5000, 0.7100, 0.8900	0.5200, 0.7400, 0.9400	0.5400, 0.7500, 0.9200	0.5200, 0.7400, 0.9200	0.1800, 0.4500, 0.7400

Table 14: The weighted normalized fuzzy-decision matrix

	SRE1	SRE2	SRE3	SRE4	SRE5	SRE6
ST11	0.00200, 0.00700, 0.02400	0.00200, 0.00800, 0.02700	0.00200, 0.00800, 0.02500	0.00200, 0.00800, 0.02500	0.00200, 0.00700, 0.02700	0.00200, 0.00700, 0.02500
ST12	0.00200, 0.00700, 0.02400	0.00100, 0.00500, 0.01800	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02400	0.00200, 0.00700, 0.02400
ST21	0.00200, 0.00800, 0.02500	0.00100, 0.00600, 0.01900	0.00200, 0.00700, 0.02400	0.00200, 0.00600, 0.02000	0.00100, 0.00500, 0.01900	0.00200, 0.00700, 0.02400
ST22	0.00200, 0.00700, 0.02200	0.00200, 0.00800, 0.02700	0.00200, 0.00700, 0.02400	0.00200, 0.00800, 0.02500	0.00200, 0.00700, 0.02700	0.00200, 0.00800, 0.02500
ST23	0.00200, 0.00600, 0.02000	0.00100, 0.00500, 0.01800	0.00200, 0.00800, 0.02500	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02400	0.00200, 0.00700, 0.02200
ST31	0.00200, 0.00800, 0.02500	0.00100, 0.00500, 0.01800	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02400	0.00200, 0.00600, 0.02000
ST32	0.00200, 0.00700, 0.02500	0.00500, 0.01600, 0.04900	0.00200, 0.00600, 0.02000	0.00200, 0.00800, 0.02500	0.00200, 0.00800, 0.02500	0.00200, 0.00800, 0.02500
ST33	0.00100, 0.00500, 0.01800	0.00200, 0.00900, 0.03800	0.00200, 0.00800, 0.02500	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02500
ST41	0.00100, 0.00500, 0.01800	0.00100, 0.00500, 0.01800	0.00200, 0.00700, 0.02500	0.00200, 0.00600, 0.02000	0.00200, 0.00600, 0.02000	0.00100, 0.00500, 0.01800
ST42	0.00100, 0.00500, 0.01800	0.00100, 0.00500, 0.01800	0.00100, 0.00500, 0.01800	0.00200, 0.00800, 0.02500	0.00200, 0.00800, 0.02500	0.00200, 0.00700, 0.02700
ST51	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
ST52	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

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

Alternatives	d + i	d − i	Gap degree (CC + i)	Satisfaction degree (CC − i)
SRE1	0.4554274	0.0557645	0.56645784	0.47548754
SRE2	0.0467548	0.05546754	0.61346574	0.38645784
SRE3	0.0645124	0.03754677	0.36794574	0.65467548
SRE4	0.0546754	0.04649754	0.58455124	0.44575487
SRE5	0.0113454	0.02346517	0.56457944	0.46457984
SRE6	0.04675487	0.04454612	0.62346457	0.38496457

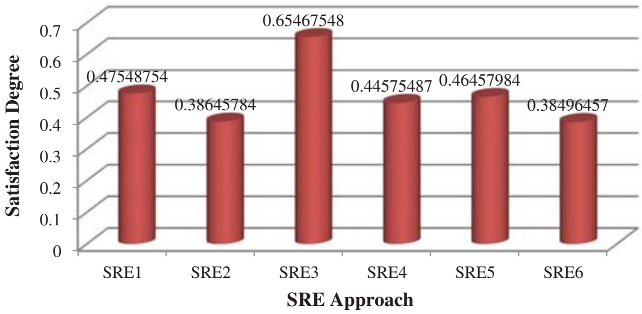

Figure 4: Graphical representation of the outcome

6 Conclusion

We contrasted and addressed different categories of security requirements engineering (SRE) approaches and procedures. Our viewpoint of assessment and analysis uses some of the usability principles set out in previous works contained in the research. One purpose of such parameters is to evaluate the ability of the process that can provide an environment for its system to develop job in a timely, efficient and productive manner while experiencing practice. Another goal is to explore which SRE approaches can be used to analyses the degree of security of the software against attacks. Our research then demonstrates and prioritizes the SRE approaches founded on the security expert's viewpoint. We conclude that STORE methodology is the very consistent and usable SRE approaches with a threat-driven approach since it uses an effective and well-organized way of eliciting security requirements in the software development procedure. The findings of this research would assist and provide future directions to the security requirements engineers and security experts. This study helps them in selecting the most effective security requirements engineering approach.

Acknowledgement: This research work was funded by Institutional Fund Projects under Grant No. (IFPHI-269-611-2020). Therefore, authors gratefully acknowledge technical and financial support from the Ministry of Education and King Abdulaziz University, DSR, Jeddah, Saudi Arabia.

Funding Statement: Funding for this study is received from the Ministry of Education and Deanship of Scientific Research at King Abdulaziz University, Kingdom of Saudi Arabia under Grant No. IFPHI-269-611-2020.

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

References

[1] J. Zadeh and D. DeVolder, "Software development and related security issues," in *Proc. of the 2007 IEEE Southeast Conf.*, Beijing, China, Richmond, VA, USA, pp. 746–748, 2007.

[2] M. T. J. Ansari and D. Pandey, "Risks, security, and privacy for HIV/AIDS data: Big data perspective," *Big Data Analytics in HIV/AIDS Research*, vol. 5, no. 6, pp. 117–139, 2018.

[3] D. D. Clark, E. W. Borbert and S. Gerhart, "Computers at risk: Safe computing in the information age," *Final Report of the System Security Study Committee*, vol. 5, no. 1, pp. 1574–1587, 1990.

[4] IDC Corporate, USA, "Global ICT Spending-Forecast 2020–2023," 2020. [Online]. Available: https://www.idc.com/promo/global-ict-spending/forecast.

[5] W. Iso, "9241-11-ergonomic requirements for office work with visual display terminals," *International Organization for Standardization*, vol. 45, no. 9, pp. 154–168, 1998.

[6] D. Gupta, A. K. Ahlawat and K. Sagar, "Usability prediction & ranking of SDLC models using fuzzy hierarchical usability model," *Open Engineering*, vol. 7, no. 1, pp. 161–168, 2017.

[7] M. T. J. Ansari, F. A. Alzahrani, D. Pandey and A. Agrawal, "A fuzzy TOPSIS based analysis toward selection of effective security requirements engineering approach for trustworthy healthcare software development," *BMC Medical Informatics and Decision Making*, vol. 20, no. 1, pp. 1–13, 2020.

[8] T. L. Satty, "The analytic hierarchy process," *Analytic Hierarchy Process Journal*, vol. 5, no. 6, pp. 187–194, 1980.

[9] L. A. Zadeh, "Fuzzy sets," *Information and Control*, vol. 8, no. 3, pp. 338–353, 1965.

[10] C. L. Hwang, Y. J. Lai and T. Y. Liu, "A new approach for multiple objective decision making," *Computers & Operations Research*, vol. 20, no. 8, pp. 889–899, 1993.

[11] J. Preece, Y. Rogers, H. Sharp, D. Benyon, S. Holland *et al., Human-Computer Interaction*. Edinburgh Gate Harlow, United Kingdom: Addison-Wesley Longman Ltd., 1994. [Online]. Available: https://dl.acm.org/doi/10.5555/561701.

[12] A. Dix, A. J. Dix, J. Finlay, G. D. Abowd and R. Beale, "Human-computer interaction," *Pearson Education*, vol. 45, no. 6, pp. 1574–1581, 2003.

[13] J. A. McCall, "Factors in software quality," *US Rome Air Development Center Reports*, vol. 20, no. 1, pp. 1–13, 1977.

[14] R. Paradis and B. Tran, "Balancing security/safety and sustainability objectives," *National Institute of Building Sciences*, vol. 7, no. 1, pp. 161–168, 2010.

[15] T. L. Saaty, "How to make a decision: The analytic hierarchy process," *European Journal of Operational Research*, vol. 48, no. 1, pp. 9–26, 1990.

[16] K. A. Dawood, K. Y. Sharif, A. A. Zaidan, A. A. Ghani, H. B. Zulzalil *et al.,* "Mapping and analysis of open source software (OSS) usability for sustainable OSS product," *IEEE Access*, vol. 7, no. 5, pp. 65913–65933, 2019.

[17] Z. Ayağ, "A fuzzy AHP-based simulation approach to concept evaluation in a NPD environment," *IIE Transactions*, vol. 37, no. 9, pp. 827–842, 2005.

[18] J. F. Chen, H. N. Hsieh and Q. H. Do, "Evaluating teaching performance based on fuzzy AHP and comprehensive evaluation approach," *Applied Soft Computing*, vol. 28, no. 5, pp. 100–108, 2015.

[19] A. Agrawal, M. Zarour, M. Alenezi, R. Kumar and R. A. Khan, "Security durability assessment through fuzzy analytic hierarchy process," *PeerJ Computer Science*, vol. 5, no. 8, pp. 1–44, 2019.

[20] Y. C. Chou, H. Y. Yen, V. T. Dang and C. C. Sun, "Assessing the human resource in science and technology for Asian countries: Application of fuzzy AHP and fuzzy TOPSIS," *Symmetry*, vol. 11, no. 2, pp. 251–271, 2019.

[21] W. B. Gray and R. J. Shadbegian, "The environmental performance of polluting plants: A spatial analysis," *Journal of Regional Science*, vol. 47, no. 1, pp. 63–84, 2007.

[22] N. R. Mead and T. Stehney, "Security quality requirements engineering (SQUARE) methodology," *ACM SIGSOFT Software Engineering Notes*, vol. 30, no. 4, pp. 1–7, 2005.

[23] C. Haley, R. Laney, J. Moffett and B. Nuseibeh, "Security requirements engineering: A framework for representation and analysis," *IEEE Transactions on Software Engineering*, vol. 34, no. 1, pp. 133–153, 2008.

[24] 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*, vol. 45, no. 9, pp. 154–161, 2018.

[25] P. Salini and S. Kanmani, "Implementation of MOSRE framework for a web application-a case study," *International Journal on Web Service Computing*, vol. 3, no. 3, pp. 95–106, 2012.

[26] D. Mellado, E. F. Medina and M. Piattini, "Applying a security requirements engineering process," in *Proc. of the European Symp. on Research in Computer Security*, Berlin, Heidelberg, pp. 192–206, 2006.

[27] S. F. Gürses and T. Santen, "Contextualizing security goals: A method for multilateral security requirements elicitation," *Sicherheit–Schutz und Zuverlässigkeit*, vol. 5, no. 8, pp. 1–44, 2006.

[28] 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. 1–15, 2017.

[29] M. Zarour, M. T. J. Ansari, M. Alenezi, A. K. Sarkar, M. Faizan *et al.,* "Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records," *IEEE Access*, vol. 8, no. 8, pp. 157959–157973, 2020.

[30] 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. 493–512, 2020.