International Journal of Computational Intelligence Systems
Vol. **12(2)**, 2019, *pp.* 627–642
DOI: https://doi.org/10.2991/ijcis.d.190513.001; ISSN: 1875-6891; eISSN: 1875-6883
https://www.atlantis-press.com/journals/ijcis/

Measuring Security Durability of Software through Fuzzy-Based Decision-Making Process

Rajeev Kumar[1,*], Mohammad Zarour[2], Mamdouh Alenezi[2], Alka Agrawal[1], Raees Ahmad Khan[1]

[1]*Department of Information Technology, BBA University, Lucknow, UP, India*
[2]*College of Computer & Information Sciences, Prince Sultan University, KSA*

ARTICLE INFO

Article History
Received 27 Oct 2018
Accepted 11 May 2019

Keywords
Software security
Software durability
Security durability
Fuzzy logic
Simple average method
Rating evaluation

ABSTRACT

It is critical to develop secure software with long-term performance and capability to withstand and forestall the growing competition in the software development industry. To enhance the potential of Confidentiality, Integrity, and Availability (CIA), a mechanism is required to built in and secure the durability at the time of software development. Security of a software product is durable if the software works efficiently for user's satisfaction up to the expected duration. Despite the fact that focusing on security which is durable enough considerably reduces maintenance cost, the work done on addressing security as well as durability issues simultaneously during software development remains minimal. To achieve durable security, there is a need to fill the gap between security and durability through identifying and establishing a relationship between security and durability attributes. This article extends the concept of the life span of security services and assesses as well as prioritizes security durability attributes by taking a real-time case study. While building durable security, security experts often face complicated decision problems. Hence, multi-criteria decision-making techniques have been used to solve the issues of measuring conflicting tangible/intangible criteria. In addition, the fuzzy simple average method is used for finding out the rating of security durability attributes. The work has been demonstrated by taking a case study. The results of the study would be useful for security developers to assure the importance of attributes for improving the duration of security.

1. INTRODUCTION

The development environment of software in the early 21st century has created new challenges for all, including developers [1]. On one hand, exponential increase in fatal security attacks on software have imposed the need for building security right from its conception while on the other, a huge investment on software has posed the demand for a durable software to justify Return on Investment (RoI). Hence, software security as well as software durability both has become the propelling factors to drive software development [2]. Unfortunately, development organizations spend a considerable amount of money and effort on resolving security issues during the early stage of secure software development [3] without paying any attention to the longevity, that is, durability of the security offered. Software security with restrictive durability is likely to fail in a highly competitive market; therefore, software development organizations should invest significant resources in realizing the tenet of durable security. Durable security can be defined as the longevity of the security of software.

In security perspective, software development includes security attributes, security strategy, security design, security testing, and security management. Earlier practices have shown that the security of software is not as high as it could be. The reason behind this is that in addition to the increasing demand for secure software, developers are facing new challenges to fulfill the customers' requirements while developing the software [4]. In addition, organizations impose development constraints due to cost, time-to-market requirements, productivity impact, customer satisfaction concerns, and so on. The result is improperly developed secure software with low durable security [5].

Further, NASA has presented a report on expenses on software maintenance. This report describes that software maintenance has invariably increased [4]. For reducing these expenses, there is a need to develop software having security with durability. In addition, a report has found that 60% of time and cost are being consumed on security maintenance [5]. These multiple reports on software maintenance focus on a single issue of nondurable software. According to another report, the service life of working software affects durability during the former stage of software development [2]. The report iterates that durability depends on the dependability and trustworthiness of developed software and also discusses the differences between durability, consistency, and survivability of software.

Maintenance cost is closely related to software durability. Low durability of software increases its maintenance cost. It has also been found that if it is possible to assess the working life of the secure software, the cost and time incurred for maintenance can be lessened [6]. During software development, identification of security

*Corresponding author. Email: rs0414@gmail.com

durability attributes may optimize the maintenance issues and thus decrease time and cost incurred on it [7,8]. Owing to this fact, durability has received a lot of attention in recent years [2]. Moreover, security and durability both are drawing research interests but not simultaneously. During the course of review, no literature has been found addressing security as well as durability issues in software at the same time during software development.

Software security with inhibitive durability is most likely to fail in a market where demands for optimum returns from investments in software development are becoming increasingly competitive. Hence, it becomes imperative for the developers to pivot their attention on ensuring the durability of security of the software that they develop. The authors have defined security durability as ***the time period during which the software performs securely***. To develop cost-effective security durability, there is need to investigate the connection between durability, its characteristics, and security [9]. Further, an assessment of security durability is important to help industries know how far their software goes securely. Developing a secure and durable software application is a complex concern and security durability attributes must be considered as important tools of longer security during the use of software [10,11]. To assess and improve security durability, there is a need to fill the gap between security and durability through their attributes.

For resolving the issues discussed above and for focusing on the software durable security to enhance the working life of the software, our contribution prioritizes security and durability attributes. Security durability may be improved by measuring the importance of attributes. And, hence the paper is evaluating the importance of security durability attributes. The prioritization of security durability attributes will help in focusing on most important factors which contribute in increasing security durability of the software. The problem of quantifying security durability attributes is multiple decision-making problem. Hence, for quantifying the security durability attributes, Multiple Criteria Decision-Making (MCDM) technique is a significant problem-solving methodology. MCDM can be used in areas including software, system, and many more [12–15]. MCDM allows decision-makers to select alternatives among different and conflicting criteria when experts are uncertain about their choices [16–19]. The contentions in decisions of experts' motivated the authors to use fuzzy multi-criteria methodology as fuzzy systems help in evaluating vague and imprecise data in linguistic forms. Here the simple fuzzy logic (Type 2) has been used because fuzzy logic describes systems in terms of combination of numeric and linguistic both [13,20].

The ratings of these attributes have been measured with the help of fuzzy sets [21]. Also, this article is using the fuzzy Simple Average Method (SAM) for rating of the security durability attributes to deal with fuzziness or uncertainty. Entrance Examination Software of BBA University (BBAU Software) has been taken as the case study. The data has been collected in form of a rating questionnaire (The Appendix A is shows the numeric data received from the experts). Rating is divided into a scale of five linguistic values, which are further fuzzified to use it for Fuzzy SAM methodology. Security design of this software is both very crucial and integral. The data collates sensitive information of online entrance exam and also demands more maintenance time and cost [22]. Security developers are trying to minimize the security maintenance cost and time by integrating longer security [23]. In addition, the paper also provides an extended methodology to evaluate the ratings at multiple levels. These ratings help in developing guidelines to ensure security durability.

The remaining paper is organized as follows: A literature survey is in Section 2. Section 3 discusses security durability. The procedure to measure security durability is described in Section 4. Section 5 shows the sensitivity analysis. Validation through the SAM is presented in Section 6. Finally, discussion and conclusions are put forth in Sections 7 and 8.

2. LITERATURE REVIEW

Over the years practitioners are trying to find out the causes of security failures [10]. After going through literature survey it has been found that security and durability attributes play a key role in deciding the longevity of software security. CIA is the set of attributes forming three pillars of security that play a key role in enhancing security [6]. It has also been observed that several factors including dependability, trustworthiness, and human trust have been ignored which also play a key role for longer security during the software development process. Further, security- and durability-related literature are discussed as follows: In 2019, H. Assal and S. Chiasson have presented a survey report and discussed the security strategies for prediction of life span for security services [24]. Development companies are trying to develop secure and durable services as per the users' needs and market values. But continuous updating of security is compelling the users to lose trust over software companies.

In 2019, T. D. Oyetoyan *et al.*, discussed the suitability of security services [25]. They compared the life of security services to improve the user's satisfaction among different software applications. Authors established the relationship between the user's requirements and design properties with respect to complexity and size. In 2016, E. V. Bartlett *et al.* have discussed the relationship between durability and reliability with respect to user experience design [11]. Reliability and durability both are important for the longer service life of software with user's satisfaction. In 2015, Kluwer W. gave a mechanism for security assurance program [26]. The study tried to fill the gap between security and durability through the security assurance program. Unfortunately, there is not a single work of assessment of security durability.

In 2015, Kelty C. *et al.* have described the role of software in computer prices and how durable software affects the cost of the computers [2]. They have suggested that the design process of software still needs to be improved for better user experience. For the same idea, in 1992, Parker D. B. has said that long security life span is needed to improve user's satisfaction related to protecting user's data [27]. He has also discussed that due to high-security maintenance cost and time, practitioners are focusing on security design during software development. In 1994, Ruth Thomas proposed the concept of durable software [28]. He discussed about the need and importance of durable and low-cost educational software. He has given a concept to optimize the maintenance for cost-effectiveness. According to his research, developers should focus on the secure and durable design to achieve longer software services.

Practitioners must be involved to develop a durable security design of software [29]. Measuring the importance of security durability

attributes through rating evaluation is one of the best approaches to develop longer security services. MCDM is the best technique to solve the uncertainty problem while selecting among attributes to enhance the security durability of software [30,31]. Fuzzy in hybridization with a multi-criteria approach and weighted average approach has been used several times in the literature. Some of the pertinent work related to rating evaluation of different case studies is discussed as follows: In 2018, Abbas Mardani *et al.*, reviewed the fuzzy aggregation methods from 1986 to 2017 [32]. Authors evaluated the importance of fuzzy aggregation methods during evaluation of rating. In this review, the authors have covered the literature of three decades and proposed a meta-analysis method called PRISMA.

In 2015, S. K. Dubey *et al.* proposed a methodology for quantifying the usability rating of software using a fuzzy multi-criteria weighted average approach [33]. A case study of MS Word 2003 has been taken to validate the feasibility of this approach. Rating of attributes is evaluated in this paper to calculate the final usability of MS Word 2003. In 2007, L. Lin *et al.* assessed the rating of usability of MS PowerPoint 2007 using fuzzy multi-criteria approach [34]. The model described the five factors given in the ISO 9126-1 namely, attractiveness, operability, understandability, learnability, and usability compliance and a detailed sub-factors structure on which these factors depend. In 2001, Yu-Ru Syau *et al.* described the credit rating in linguistic terms, which were vague and difficult to put into precise numerical values [22]. They focused on fuzzy set theory and handled this vagueness of data. The case study used here was focused on software related to commercial banks.

In 2000, S. Ammar *et al.* applied fuzzy set theory in performance evaluation of three different applications that was evaluating state governments, client satisfaction, and evaluating state funding agencies [31]. The three applications described in this paper rely on survey data but are different in nature. Over the years, there has been lot of work done related to durability as well as MCDM techniques for evaluating the ratings of attributes. But, no work has been seen relating to security durability assessment. After the thorough literature review, it has been concluded that the rating of security durability is instrumental in determining the longer security (long life span of security) of working software. Hence, this article will determine the rating of security durability through extended fuzzy SAM technique in the next sections.

3. SECURITY DURABILITY

Security of user's information is at risk, as the increasing use of software makes it important to use software in every field. Nowadays, it is easy to build and use the software but to maintain its security is not an easy task because organizations are facing numerous issues related to security services of software. Amongst them is the nodal issue of software security durability. Software security durability ensures the long life of secure services to the user. This introduces an urgent need to address security issues as security failure may lead to disastrous effects on human lives. Complex operations, rising cost, resource constraint, and a future of strategic uncertainty demand that software must deliver higher security with reducing cost. This will help in building software that will actually be able to defend itself from attacks despite being dependent upon any application security software for its protection against threats. The basic cause of the maximum of the security breaches is the absence of security services when it is most needed. Software developers are trying their best to achieve higher security durability of software. But, security of software is still not at its best. In addition, organizations are demanding optimal maintenance of security during working life of software services.

Further, software durability can be defined as the predicted service life span of software. As time passes, the use of software, the need for updating security increases because new security threats are generated day by day [2,5]. If these threats get active then security will fail and as a result, the software will crash. Authors have identified and classified the security durability attributes in their previous work [6,7]. There are numerous attributes of security durability including dependability, trustworthiness, and human trust that are to be used for improvement of security durability which is shown in Figure 1.

For the purpose of assessment, attributes of durable security at level 1 are denoted as C1, C2, and C3 in Figure 1. Each of them is described in the following section.

3.1. Dependability

A computer is called secure if the user can depend on it and its software to work as expected [3,4]. This definition is controversial as it implies that security exists in the user's expectations of computer and software behavior. It is useful, however, in underlining the importance of dependability in computer security. Security durability is affected as well by dependability and its other co-attributes [7]. Dependability refers to the ability to deliver service that can justifiably be trusted [35]. While according to dependability definition, it is inferred that user's expectation of secure software service life span is important. Hence, in these terms, dependable or secure software helps to build durability of security stronger. There are many attributes of dependability but only a few are affected by security durability which is shown in Figure 2.

Figure 2 shows the attributes of dependability which are affecting the life span of security services. The definition stresses the need for justification of trust. Hence, it is directly related to security attributes such as confidentiality, authentication, and reliability [7]. The alternate, quantitative definition that provides the criteria for deciding if the service is dependable is its ability to avoid service failures (including security service failures) that are more frequent and more severe than is acceptable to the user(s) [11]. The quantitative definition formulates that dependability is also related to availability and maintainability. For the purpose of assessment, attributes of durable security with respect to dependability at level 2 and level 3 are denoted as C11 ⋯ ⋯ C15 and C111 ⋯ ⋯ ⋯ ⋯ .C115, and so on, which are shown in Figure 2.

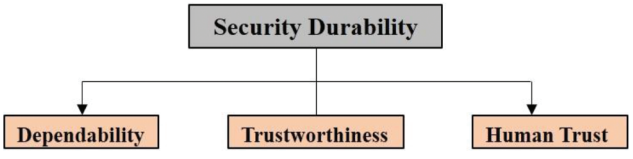

Figure 1 | Main attributes of security durability.

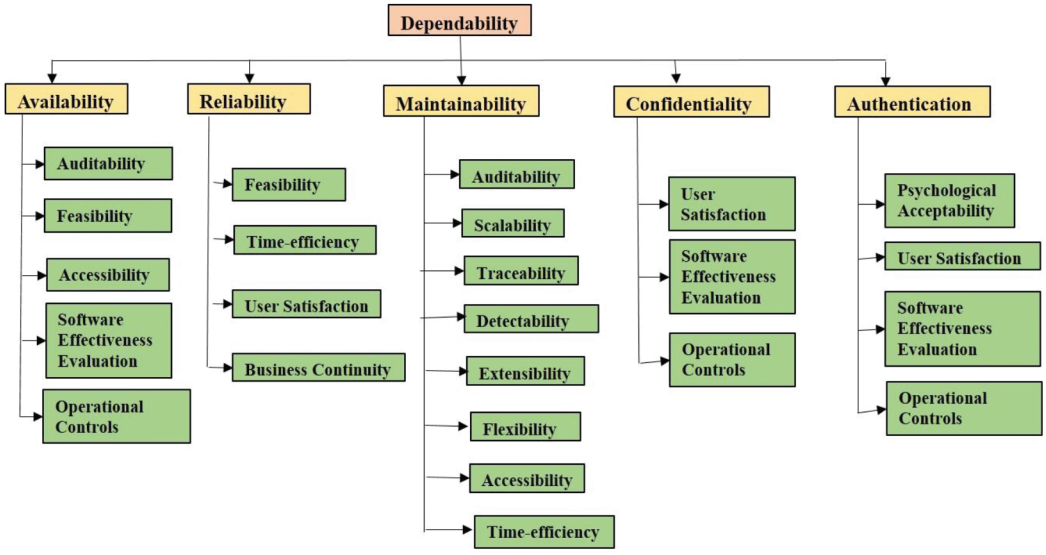

Figure 2 | Attributes of dependability affecting security durability.

3.2. Trustworthiness

The software possesses trustworthiness if it performs as intended for a specific purpose, when needed, with new changes that have been done recently, and without unwanted side effects, behaviors, or exploitable vulnerabilities. Trustworthiness is the assurance that the software will perform as expected [7]. There are many attributes of trustworthiness but few affects security durability which is shown in Figure 3.

Figure 3 shows the attributes of trustworthiness that are affecting the life span of security services. Hence, according to its definition, trustworthiness depends on the availability, reliability, maintainability, accountability, and survivability [36]. Further, security durability requires that the software at least works for a specified time period by strengthening the maintainability of security of software services, henceforth improving the trustworthiness of security. The term operational resilience, which strengthens trustworthiness of security, is a set of techniques that allows people, processes, and informational systems to adapt to changing patterns [37]. This term directly points out that the maintainability affects secure life span of software. The quantitative definition formulates that trustworthiness is also related to availability, reliability, accountability, and survivability [36]. For the purpose of assessment, attributes of durable security with respect to trustworthiness at level 2 and level 3 are denoted as C21 ⋯ ⋯ C25 and C211 ⋯ ⋯ ⋯ .C215, and so on, which are shown in Figure 3.

3.3. Human Trust

In relation to human–human interaction, human trust is mostly defined as a sensitive issue where the trusted party has a moral responsibility to the trusting party [38]. In software terms, consumer's trust on the developers is identified as human trust. Consumers' trust, when using software, is dependent on the security design of the software and that the software will work for an expected duration and secure their data or information. Security durability and human trust are the attributes that strengthen each other [7]. There are many attributes of human trust but few are affecting security durability, which is shown in Figure 4.

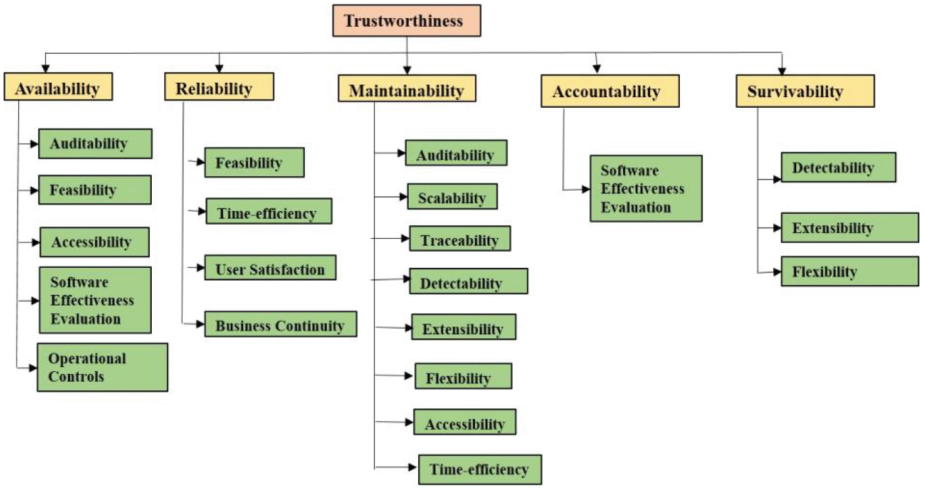

Figure 3 | Attributes of trustworthiness affecting security durability.

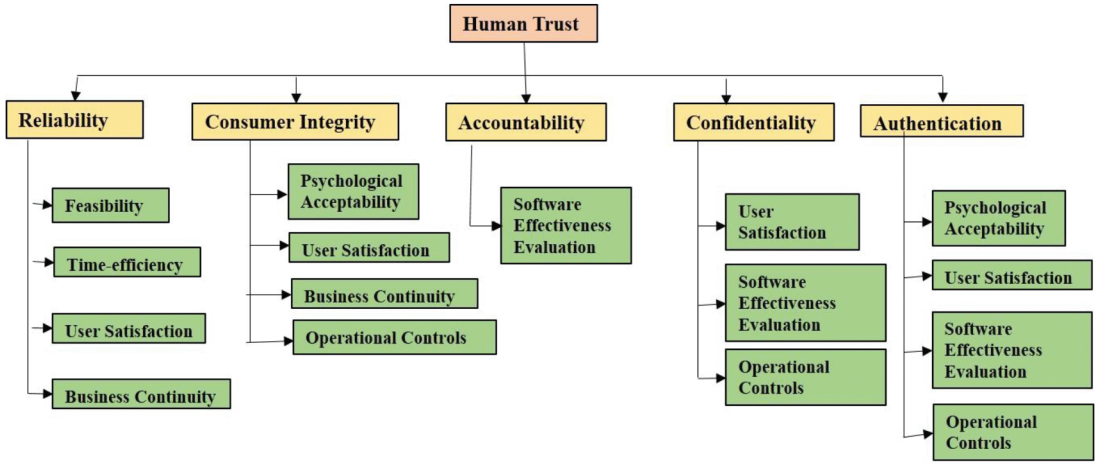

Figure 4 Attributes of human trust affecting security durability.

Figure 4 shows the attributes of human trust that are affecting the life span of security services. Software with security durability will perform to improve human trust and in turn will improve the consumer's reliability on an organization's software services [6]. Human trust is a willingness to rely on the software with confidence [38]. According to its definition, it is found that five security attributes that may affect human trust include reliability, consumer integrity, accountability, confidentiality, and authentication. Human trust invariably depends on these factors [38]. Hence strength of these five factors is important in building stronger human trust. For the purpose of assessment, attributes of durable security with respect to human trust at level 2 and level 3 are denoted as C31 ⋯ ⋯ C35 and C311 ⋯ ⋯ ⋯ .C315, and so on, which are shown in Figure 4.

A considerable measure of research is accessible, trying to comprehend and characterize the manners by which the security of software can be upgraded [6]. While there has consistently been a hole among hypothesis and practice which is difficult to fill completely, the lacunae can be bridged by building up a common terminology and enhancing the availability of research results. With the investigation of security and durability in this work, it has been attempted to create a quantitative assessment of security durability attributes for evaluating the importance. To assess security durability during software development identified security durability attributes are for measuring the impact of these attributes on the secure life span of software. Assessment of security durability attributes may allow decision-makers to make appropriate decisions as well as action [39]. However, to be able to take appropriate action, decision-makers are not only needed to know about security and durability attributes but their mapping also. In this paper, authors are converting the security durability attributes (attributes are identified and classified in previous work) into a hierarchy; the hierarchy is shown in Figures 1–4.

Figures 1–4 show various attributes of durability affecting security. For example, confidentiality affects software effectiveness, user satisfaction, and operational controls; availability affects auditability, feasibility, accessibility, software effectiveness evaluation, operational controls; reliability affects feasibility, time-efficiency, user satisfaction, business continuity; maintainability affects auditability, scalability, traceability, detectability, accessibility, time-efficiency, extensibility, effectiveness, flexibility; consumer integrity affects psychological acceptability, user satisfaction, business continuity; accountability affects software effectiveness evaluation; survivability affects detectability, extensibility, flexibility; authentication affects user satisfaction, psychological acceptability, software effectiveness evaluation, and operational controls. Level wise full descriptions of the above hierarchy or mapping are followed.

Figures 1–4 show the hierarchies of security durability which is further classified in three levels. An attribute at one level affects one or more attributes of the higher level but its effect is not the same on them. It may vary. For example, reliability has an impact on dependability, human trust, and trustworthiness as well, but its impact values are not same either [4,9]. The hierarchies of attributes help to differentiate among the impacts of the same attributes to the others attribute at a higher level. For the longer security, practitioners need to understand and assess security durability during the software development process.

There are eight attributes at level 2 which affect security durability and defined as follows:

- *Confidentiality*: Confidentiality refers to allowing authorized access to sensitive and secure data [3].
- *Consumer Integrity*: Consumer integrity is defined as the attribute maintaining the consistency, accuracy, and trustworthiness of consumer all over the life cycle of a software product and its security [7].
- *Authentication*: Authentication is the factor which is responsible for the identity of the user profile. It is the process of determining whether a user is, in fact, who it is declared to be [6].
- *Reliability:* Reliability is the ability of security to consistently perform according to its specifications. It is considered to be very important aspects while designing security [4].
- *Maintainability:* It is the probability that a system can be repaired in the said environment or situations [2].
- *Accountability:* Accountability means that every individual user who works with the software should have specific

responsibilities for security assurance. These tasks include individual responsibilities as part of the overall security plan because software may become vulnerable by a responsible person such as a developer [9].

- *Survivability:* Survivability is the ability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents [6].
- *Availability:* Availability means the information is accessible by only authorized users. Availability, in the context of a computer system, refers to the ability of a user to access information or resources for a specified duration [7].

There are fourteen attributes at level 3 that are defined as follows:

- *Auditability:* The capability of supporting a systematic and independent security process for obtaining audit evidence and evaluating it accurately to determine the extent to which audit criteria are fulfilled [7].
- *Scalability:* Scalability is the measure of how well security can grow to meet the increasing performance demands [6].
- *Feasibility:* A feasibility study is an analysis of how successful a project can be completed, accounting for factors that affect it such as economic, technological, legal, and scheduling factors [4].
- *Detectability:* Detectability is responsible for the detection of security failures or crashes in software for a particular duration of time [7].
- *Accessibility:* Accessibility is the degree to which a software security service or environment is available to as many people as possible [7].
- *Time-Efficiency:* The capability to provide the appropriate performance of security, relative to the number of resources used in the understated conditions within specific time duration [9].
- *Extensibility:* The ease with which security can be enhanced in the future to meet changing security requirements or goals [5].
- *Psychological Acceptability:* Acceptance in human psychology is a person's assent to the reality of a situation, recognizing a process or condition without attempting to change it, protest it [1].
- *User Satisfaction:* User satisfaction is a degree of how secure services provided by an organization meet the customer expectation [6].
- *Business Continuity:* Business continuity encompasses a loosely defined set of planning, preparation, and related activities for software security which are intended to ensure that an organization's critical business functions will either continue to operate within a period [7].
- *Software Effectiveness Evaluation:* Effectiveness is a degree to which something is successful in producing the desired result; success [6].
- *Flexibility:* The capability of secure software to respond to potential internal or external changes affecting its value within timely and cost-effective manner [7].
- *Operational Controls:* The most difficult task of management pertains to monitoring the behavior of individuals, comparing security performance to some standard, and providing rewards as specified [7].

From the foregoing discussion, the researcher classified the security durability attributes into three main levels, the first level, second level, and third level attributes on which the security durability depends, directly or indirectly. These attributes help the researchers to assess the security durability of the software. There is no mechanism available to evaluate the importance of security durability attributes. Security durability of software may be improved through a well-planned, well-categorized, and well-manageable process during the Software Development Life Cycle (SDLC). Without an assessment of security durability, it is not possible to improve it. Hence, the paper evaluates the rating of security durability through a case study of BBAU software. For this, hybrid techniques including fuzzy MCDM is used. Because fuzzy decision-making methods have been developed to solve the problem of imprecision in assessing the relative importance of attributes. Imprecision may arise from a variety of various attributes of a different nature. Traditional methods cannot effectively handle problems with such imprecise information [40]. To resolve this difficulty, the fuzzy set theory has been introduced by Zadeh [21]. Fuzzy with other methodologies such as Neural, SAM, AHP, and so on, give precise results [39–41].

4. EVALUATING THE IMPORTANCE OF SECURITY DURABILITY ATTRIBUTES

A rating is the evaluation or assessment of something, in terms of quality, quantity, or some combination of both [21,22]. The paper is using the fuzzy Simple Average Method (fuzzy SAM) for evaluating the ratings of security durability attributes at different levels. The FSAM methodology is applied in real-time application of entrance software BBA University. It is one of the most popular techniques of MCDM for evaluating the rating of the attributes [12,16]. After the identification of durable security attributes, the authors prepared a questionnaire about the BBAU software and took the opinions of 50 practitioners. From which, 20 valid responses are used in this research. With the help of the opinions for BBAU software and its performance, authors gave the rating to security durability attributes which further can be helpful to assess security durability. To overcome decision-maker's uncertainty, fuzzy SAM technique uses a choice of standard. Practitioners assigned scores to the attributes affecting the values in a quantitative way according to scale which is shown in Table 1.

Table 1 shows the rating scale of 0 to 1 in scale as 0.1 describes Very Low (VL), 0.3 describes Low (L), and so on. The associated fuzzy values are assigned to every data received from the expert. Let,

Table 1 Linguistic rating scale.

S. No.	Linguistic Value	Numeric Value of Ratings	TFNs
1	VL	0.1	(0.0, 0.1, 0.3)
2	L	0.3	(0.1, 0.3, 0.5)
3	M	0.5	(0.3, 0.5, 0.7)
4	H	0.7	(0.5, 0.7, 0.9)
5	VH	0.9	(0.7, 0.9, 1.0)

TFNs, triangular fuzzy numbers; VL, very low; L, low; M, medium; H, high; VH, very high.

triangular fuzzy numbers (TFNs) is equal to (b_{ij}, m_{ij}, u_{ij})., where b_{ij}, m_{ij}, u_{ij}, are the lower, medium, and upper limits of the TFN, respectively.

4.1. Aggregate the TFNs

Data of level 1, level 2, and level 3 are collected. Various linguistic data gets converted into quantitative data in terms of TFNs. To confine the vagueness of the parameters which are related, alternatives such as TFNs are used [16,21]. A fuzzy number M on F is called TFN, if its membership function is given as follows:

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

$$\mu_a\,(x) = \begin{cases} \dfrac{x}{mi-b} - \dfrac{b}{mi-b} & x \in [b, mi] \\ \dfrac{x}{mi-u} - \dfrac{u}{mi-u} & x \in [mi, u] \\ 0 & Otherwise \end{cases} \tag{2}$$

Here b, mi, and u are defined as a lower limit, middle limit, and upper limit, respectively, in the triangular membership function. Equations (3–5) help to aggregate TFN values. Consider two TFNs M_1 and M_2, $M_1 = (b_1, mi_1, u_1)$ and $M_2 = (b_2, mi_2, u_2)$.

The rules of operations on them are as follows:

$$(b_1, mi_1, u_1) + (b_2, mi_2, u_2) = (b_1 + b_2, mi_1 + mi_2, u_1 + u_2) \tag{3}$$

$$(b_1, mi_1, u_1) \times (b_2, mi_2, u_2) = (b_1 \times b_2, mi_1 \times mi_2, u_1 \times u_2) \tag{4}$$

$$(b_1, mi_1, u_1)^{-1} = \left(\frac{1}{u_1}, \frac{1}{mi_1}, \frac{1}{b_1}\right) \tag{5}$$

It is based on the rationality of uncertainty due to imprecision. A major contribution of fuzzy set theory is its capability of dealing with uncertainty. Fuzzy SAM method is used in various research areas for decision-making in different fields such as decision-making, rating, and so on [21,22,39,40]. In the context of the present paper, it has been used for the rating of security durability attributes. To aggregate the TFN, the average method is used which is shown in Equation (6).

$$R = (N_1 + N_2 + N_3 + N_3 \ldots \ldots \ldots .N_M) \div M \tag{6}$$

where N is the number of criteria and M is the total criteria. Fuzzified average rating of different levels attributes is shown in Table 2.

4.2. Defuzzification and Local Ratings

Different defuzzification methods are available in literature such as centroid, the center of sums, alpha cut, and so on [39–41]. This paper has adopted the alpha cut method for defuzzification of fuzzified rating. The equations of the alpha cut method are shown in Equations (7–9).

$$\gamma_{\alpha,\beta}\left(\eta_{ij}\right) = \ \left[\beta.\eta_{\alpha}\left(b_{ij}\right) + (1-\beta).\eta_{\alpha}\left(u_{ij}\right)\right] \tag{7}$$

$$\text{where } 0 \le \alpha \le 1 \quad and \quad 0 \le \beta \le 1$$

Table 2 Fuzzified average ratings.

S. No.	Characteristics of Level 1	Fuzzified Average Rating
1	Dependability	0.46, 0.62, 0.76
2	Trustworthiness	0.46, 0.63, 0.75
3	Human trust	0.44, 0.60, 0.74
	Characteristics of Level 2	
1	Reliability	0.53, 0.72, 0.87
2	Availability	0.46, 0.63, 0.78
3	Authentication	0.38, 0.55, 0.71
4	Maintainability	0.45, 0.64, 0.79
5	Confidentiality	0.56, 0.72, 0.84
6	Accountability	0.45, 0.62, 0.77
7	Consumer integrity	0.46, 0.64, 0.78
8	Survivability	0.50, 0.68, 0.83
	Characteristics of Level 3	
1	Software effectiveness evaluation	0.66, 0.60, 0.88
2	User satisfaction	0.64, 0.81, 0.94
3	Feasibility	0.49, 0.57, 0.84
4	Operational controls	0.75, 0.67, 0.99
5	Time-efficiency	0.35, 0.52, 0.77
6	Auditability	0.56, 0.6, 0.88
7	Psychological acceptability	0.43, 0.58, 0.90
8	Business continuity	0.42, 0.57, 0.91
9	Accessibility	0.49, 0.61, 0.80
10	Extensibility	0.44, 0.60, 0.89
11	Flexibility	0.50, 0.66, 0.84
12	Detectability	0.51, 0.56, 0.83
13	Scalability	0.46, 0.62, 0.90
14	Traceability	0.40, 0.57, 0.85

such that,

$$\eta_{\alpha}\left(b_{ij}\right) = \ \left(mi_{ij} - b_{ij}\right).\alpha + b_{ij} \tag{8}$$

$$\eta_{\alpha}\left(u_{ij}\right) = u_{ij} - \ \left(u_{ij} - mi_{ij}\right).\alpha \tag{9}$$

In this context, α and β carry the meaning of preferences and risk tolerance of participants. Particularly, α and β can be stable or in a fluctuating condition. The range of uncertainty is greatest when $\alpha = 0$. Meanwhile, the value of α comes to a stable state when it is increasing particularly. Additionally, α can be any number between 0 and 1, and analysis is normally set as the following 10 numbers, 0.1, 0.2, up to 1.0 for uncertainty emulation. Hence for being on a particular stable state, we have taken the value of α and β as 0.5 both, so that best results can be achieved [39]. Sensitivity analysis can be done by making the fluctuations in values of α and β to know the fluctuations in final ratings. Further, Table 3 describes the independent or local ratings of the attributes of levels 1, 2, and 3.

4.3. Final Rating through the Hierarchy

Table 3 shows the independent ratings of every attribute at levels 1, 2, and 3. Next step in this row is to calculate the final ratings of attributes according to their existence in the hierarchy (combination of Figures 1–4). For calculating the final ratings the lower level ratings are multiplied to the higher level ratings.

Difference between local rating and the final rating is that the final rating is achieved by putting the attributes according to hierarchy, while local rating is an only a general rating of an attribute for security durability of BBAU software. This can be better understood by an example such as local rating of availability is 0.624 while the final rating of availability is 0.379, which is achieved by the hierarchical structure of security durability attributes.

Table 3 Independent ratings.

S. No.	Characteristics of Level 1	Defuzzified Local Rating
1	Dependability	0.61
2	Trustworthiness	0.62
3	Human trust	0.60
	Characteristics of Level 2	
1	Reliability	0.71
2	Availability	0.63
3	Authentication	0.55
4	Maintainability	0.63
5	Confidentiality	0.71
6	Accountability	0.61
7	Consumer integrity	0.63
8	Survivability	0.67
	Characteristics of Level 3	
1	Software effectiveness evaluation	0.63
2	User satisfaction	0.80
3	Feasibility	0.62
4	Operational controls	0.77
5	Time-efficiency	0.54
6	Auditability	0.66
7	Psychological acceptability	0.62
8	Business continuity	0.60
9	Accessibility	0.63
10	Extensibility	0.64
11	Flexibility	0.67
12	Detectability	0.62
13	Scalability	0.65
14	Traceability	0.60

In Table 4, many attributes at level 2 and level 3 are repeated but their impact on its higher level attributes is different. For better understanding, aggregation is done to evaluate the ratings of each level's attribute. Ratings of different attributes at a different level are shown in Tables 5–7 with their graphical structure representing their contribution towards durability rating. According to Table 5 and Figure 5, the rating of dependability is 0.608, trustworthiness is 0.619 and human trust is 0.595. Results show that the contribution of trustworthiness is highest among all three attributes in the first level.

Figure 5 Graphical representation of level 1.

After aggregating the ratings of the second level, attributes are shown in Table 6 and Figure 6. The final rating of reliability is 0.4307, availability is 0.3825, authentication is 0.3385, maintainability is 0.3840, confidentiality is 0.4265, accountability is 0.4230, consumer integrity is 0.3740, and survivability is 0.4150. Among the all attributes the result shows that the rating of reliability is highest on level 2.

After aggregating the ratings of level 3, the results are shown in Table 7 and Figure 7. Rating of software effective evaluation is 0.3068, user satisfaction is 0.3193, feasibility 0.2536, operational controls 0.2931, time-efficiency is 0.2226, auditability is 0.2525, psychological acceptability is 0.2183, business continuity is 0.2720, accessibility is 0.2400, extensibility is 0.2497, flexibility is 0.2623, detectability is 0.2423, scalability is 0.2490, and traceability is 0.2290. In all attributes of level 3, user satisfaction has the highest rating among all.

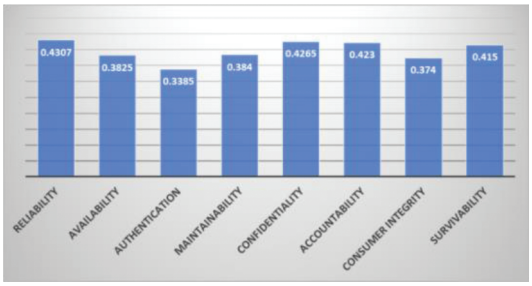

Figure 6 Graphical representation of level 2.

5. SENSITIVITY ANALYSIS

Sensitivity analysis is defined as the technique used to determine how different values of an independent variable will impact a particular dependent variable under a given set of assumptions [4]. Here, we are assuming the threshold value (values of α and β) is 0.5. Value of α and β lies between 0 and 1. Variations due to values of α and β are shown in Tables 8–10. The graphical representations of the variation are shown in Figures 8–10. Variations are showing the negligible difference between ratings of levels 1, 2, and 3, which gives the most optimistic and generalized results.

Table 8 and Figure 8 are describing the variations in ratings of first level attributes. The lesser variations are seen in the rating of human trust as the value of α and β variations.

Table 9 and Figure 9 are showing the rating variations in second level attributes of security durability through the values of α and β.

Table 10 and Figure 10 represent the fluctuations in ratings of third level attributes. It can be seen from the sensitivity analysis of ratings of security durability attributes depend upon α and β values and the ratings are higher correlated.

6. VALIDATION

Fuzzy SAM and SAM methods are appropriate for assessment of rating [30,31,34,35]. However, these two methods have some advantages and disadvantages on application. When there are large numbers of attributes in assessment, conflictions may arise [32]. Different methods provide different results on the same data; decision-makers mostly use two methods to validate the model. Hence in order to get the accuracy in the results, a comparative study is needed. This work has also evaluated the ratings of security durability attributes through SAM. Differences between results of fuzzy SAM and SAM are negligible and have a higher correlation (Pearson correlation) between the results which are shown in Tables 11–13. The graphical representations of the difference are shown in Figures 11–13.

Table 4 Dependent ratings.

The First Level	The Ratings of Durability Factors of the First Level	The Second Level Attributes	Local Ratings of the Second Level	The Dependent Ratings of the Second Level	The Attributes of the Third Level	The Local Ratings of the Third Level	The Dependent Ratings of the Third Level
					C111	0.66	0.25
					C112	0.62	0.23
		C11	0.63	0.38	C113	0.63	0.24
					C114	0.78	0.30
					C115	0.77	0.29
					C121	0.62	0.27
		C12	0.71	0.43	C122	0.54	0.23
					C123	0.80	0.34
					C124	0.62	0.27
					C131	0.66	0.25
					C132	0.65	0.25
					C133	0.60	0.23
C1	0.61	C13	0.63	0.38	C134	0.62	0.23
					C135	0.63	0.24
					C136	0.67	0.25
					C137	0.63	0.24
					C138	0.54	0.21
					C141	0.80	0.34
		C14	0.71	0.43	C142	0.78	0.34
					C143	0.77	0.33
					C151	0.62	0.22
		C15	0.58	0.35	C152	0.80	0.28
					C153	0.78	0.27
					C154	0.77	0.27
					C211	0.66	0.25
					C212	0.62	0.24
		C21	0.62	0.39	C213	0.63	0.24
					C214	0.78	0.30
					C215	0.77	0.30
					C221	0.62	0.27
		C22	0.71	0.44	C222	0.54	0.24
					C223	0.80	0.35
					C224	0.62	0.27
					C231	0.66	0.26
					C232	0.65	0.25
					C233	0.60	0.23
C2	0.62	C23	0.63	0.39	C234	0.62	0.24
					C235	0.63	0.25
					C236	0.67	0.26
					C237	0.63	0.24
					C238	0.54	0.21
		C24	0.61	0.48	C241	0.78	0.38
					C251	0.62	0.26
		C25	0.67	0.42	C252	0.63	0.26
					C253	0.67	0.28
		C31	0.71	0.42	C311	0.62	0.26
					C312	0.54	0.23
					C313	0.80	0.34
					C314	0.62	0.26
		C32	0.63	0.37	C321	0.62	0.23
					C322	0.80	0.30
					C323	0.78	0.29
					C324	0.77	0.29
C3	0.60	C33	0.61	0.36	C331	0.78	0.28
					C341	0.80	0.34
		C34	0.71	0.42	C342	0.78	0.33
					C343	0.77	0.32
		C35	0.55	0.33	C351	0.62	0.20
					C352	0.80	0.26
					C353	0.78	0.26
					C354	0.80	0.25

Table 5 Rating of level 1 attributes.

S. No.	Characteristics of Level 1	Fuzzy SAM	
1	Dependability	0.6080	C1
2	Trustworthiness	0.6190	C2
3	Human trust	0.5950	C3

SAM, simple average method.

Tables 11–13 and Figures 11–13 show that rating evaluation of security durability attributes of the first level are highly correlated. Fuzzy SAM method gives better readings in comparison to the SAM.

Table 6 Rating of level 2 attributes.

S. No.	Characteristics of Level 2	Fuzzy SAM	
1	Reliability	0.4307	[C12 + C22 + C31]/3
2	Availability	0.3825	[C11 + C21]/2
3	Authentication	0.3385	[C15 + C35]/2
4	Maintainability	0.3840	[C13 + C23]/2
5	Confidentiality	0.4265	[C14 + C34]/2
6	Accountability	0.4230	[C24 + C33]/2
7	Consumer integrity	0.3740	C32
8	Survivability	0.4150	C25

SAM, simple average method.

Table 7 Rating of level 3 attributes.

S. No.	Characteristics of Level 3	Fuzzy SAM	
1	Software effectiveness evaluation	0.3068	[C114 + C142 + C153 + C214 + C241 + C331 + C342 + C353]/8
2	User satisfaction	0.3193	[C123 + C141 + C152 + C223 + C313 + C322 + C341 + C352]/8
3	Feasibility	0.2536	[C112 + C121 + C212 + C221 + C311]/5
4	Operational controls	0.2931	[C115 + C143 + C154 + C215 + C324 + C343 + C354]/7
5	Time-efficiency	0.2226	[C122 + C138 + C222 + C238 + C312]/5
6	Auditability	0.2525	[C111 + C131 + C211 + C231]/4
7	Psychological acceptability	0.2183	[C151 + C321 + C351]/3
8	Business continuity	0.2720	[C124 + C224 + C314 + C323]/4
9	Accessibility	0.2400	[C113 + C137 + C213 + C237]/4
10	Extensibility	0.2497	[C135 + C235 + C252]/3
11	Flexibility	0.2623	[C136 + C236 + C253]/3
12	Detectability	0.2423	[C134 + C234 + C251]/3
13	Scalability	0.2490	[C132 + C232]/2
14	Traceability	0.2290	[C133 + C233]/2

SAM, simple average method.

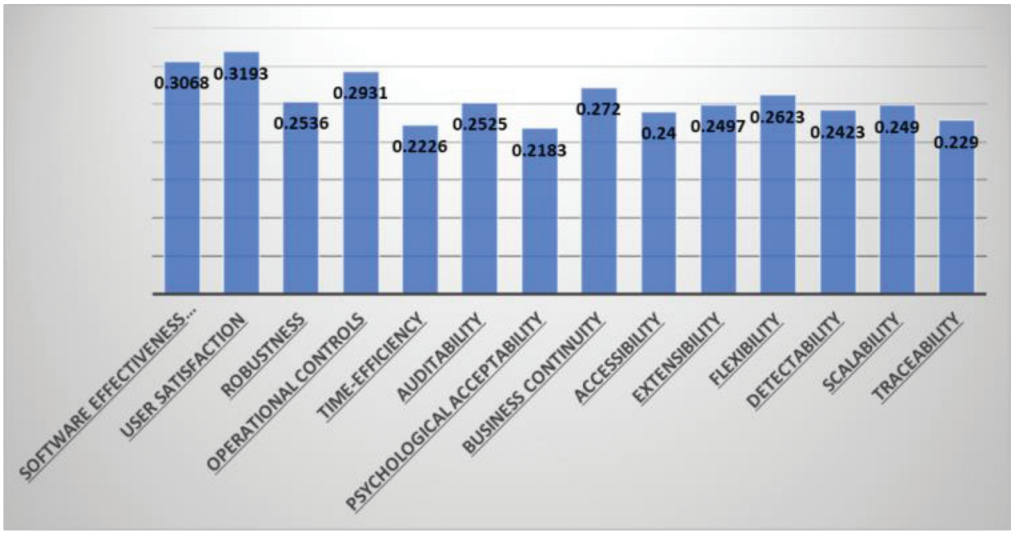

Figure 7 Graphical representation of level 3.

Table 8 Variations in ratings of level 1 attributes.

	Variation in Ratings								
(Preferences of Participants) α	**0.5**	**0.5**	**0.5**	**0.5**	**0.5**	**0.1**	**0.3**	**0.7**	**0.9**
(Risk Tolerance of Participants) β	**0.1**	**0.3**	**0.7**	**0.9**	**0.5**	**0.5**	**0.5**	**0.5**	**0.5**
Characteristics of Level 1									
Dependability	0.6700	0.6390	0.5770	0.5460	0.6080	0.6020	0.6050	0.6110	0.6140
Trustworthiness	0.6760	0.6470	0.5900	0.5620	0.6190	0.6020	0.6100	0.6270	0.6360
Human Trust	0.6550	0.6250	0.5650	0.5370	0.5950	0.5910	0.5930	0.5970	0.5990

Correlation coefficient between the both signifies that these values are highly related. Figures 11–13 clear that ratings by Fuzzy SAM method are higher than the other. The accuracy of assessment in the form of rating is best achieved by using Fuzzy with SAM. Though SAM is already proved to be an accurate method but using Fuzzy with it gives more precise results with multi-criteria decision-making problems.

7. DISCUSSION

The assessment of software security durability attributes provides ways to develop secure and durable software. This assessment revealed many things including the most important attributes of security durability to consider while developing a software security. Quantitative evaluation of software security durability is helpful in deciding the high order attributes to be considered for achieving high durability of security services.

Security is one of the biggest concerns in the present era. Organizations want more secure software with a long life span. Durable security plays a key role in the service life of the software. Quantitative analysis of security durability is essential to measure the contribution of it. A hierarchical structure helps to find out the relation between the attributes which contribute to longer security

Figure 8 | Graphical representation of variations in level 1 attributes.

Table 9 | Variations in ratings of level 2 attributes.

	Variation in Ratings								
(Preferences of Participants) α	**0.5**	**0.5**	**0.5**	**0.5**	**0.5**	**0.1**	**0.3**	**0.7**	**0.9**
(Risk Tolerance of Participants) β	**0.1**	**0.3**	**0.7**	**0.9**	**0.5**	**0.5**	**0.5**	**0.5**	**0.5**
Characteristics of Level 2									
Reliability	0.5177	0.4727	0.3893	0.3523	0.4307	0.4187	0.4240	0.4363	0.4427
Availability	0.4620	0.4215	0.3455	0.3105	0.3825	0.3730	0.3775	0.3875	0.3930
Authentication	0.4065	0.3670	0.2940	0.2610	0.3385	0.3260	0.3275	0.3405	0.3335
Maintainability	0.4680	0.4250	0.3455	0.3085	0.3840	0.3730	0.3785	0.3900	0.3960
Confidentiality	0.5060	0.4650	0.3890	0.3540	0.4265	0.4175	0.4215	0.4310	0.4355
Accountability	0.5050	0.4630	0.3850	0.3490	0.4230	0.4215	0.4225	0.4230	0.4245
Consumer Integrity	0.4530	0.4130	0.3370	0.3030	0.3740	0.3680	0.3720	0.3770	0.3800
Survivability	0.4990	0.4560	0.3760	0.3390	0.4150	0.4000	0.4070	0.4230	0.4310

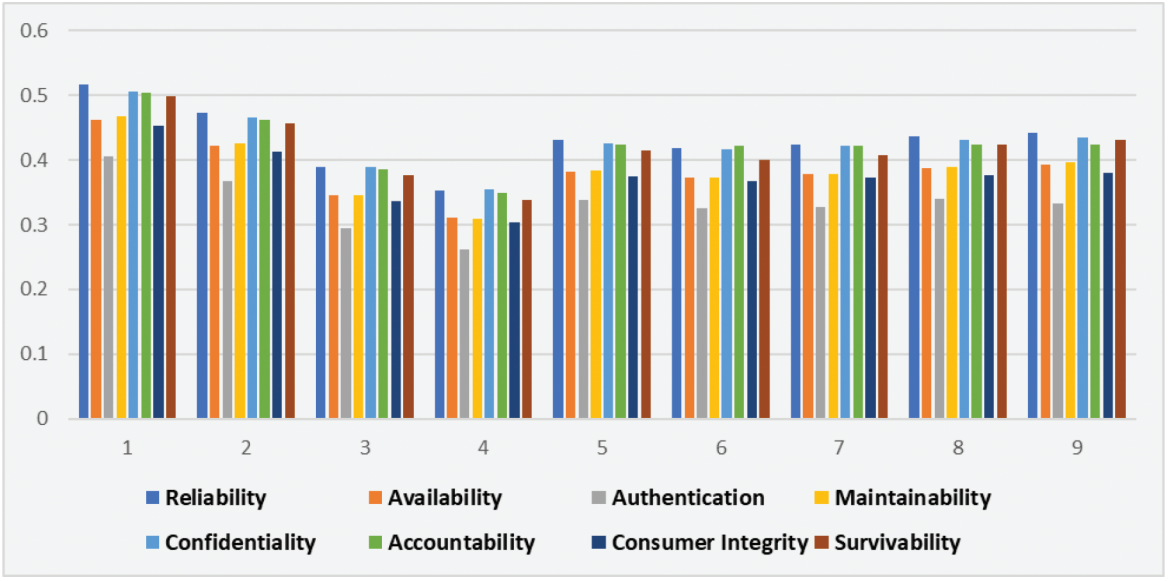

Figure 9 | Graphical representation of variations in level 2 attributes.

during the software development process. In this paper, we have taken a real-time case study of BBAU software and collected the expert's opinions about the contributing security factors of the particular software. Collected expert's data is compiled by Fuzzy SAM and further the results are validated by SAM method. The results show that the rating of security durability attributes lies between 0 and 1 where 1 is the highest rating. Significance of the work can be summarized as follows:

Table 10 Variations in ratings of level 3 attributes.

	Variation in Ratings								
(Preferences of Participants) α	**0.5**	**0.5**	**0.5**	**0.5**	**0.5**	**0.1**	**0.3**	**0.7**	**0.9**
(Risk Tolerance of Participants) β	**0.1**	**0.3**	**0.7**	**0.9**	**0.5**	**0.5**	**0.5**	**0.5**	**0.5**
Characteristics of Level 3									
Software Effectiveness Evaluation	0.3959	0.3486	0.2654	0.2294	0.3068	0.3098	0.3075	0.3041	0.2996
User Satisfaction	0.4109	0.3619	0.2789	0.2395	0.3193	0.3073	0.3120	0.3240	0.3279
Feasibility	0.3392	0.2944	0.2166	0.1836	0.2536	0.2612	0.2576	0.2494	0.2448
Operational Controls	0.3736	0.3303	0.2547	0.2233	0.2931	0.3150	0.3030	0.2807	0.2664
Time-efficiency	0.3104	0.2640	0.1852	0.1528	0.2226	0.2224	0.2224	0.2222	0.2220
Auditability	0.3355	0.2918	0.2165	0.1848	0.2525	0.2630	0.2575	0.2468	0.2413
Psychological Acceptability	0.2433	0.2560	0.1777	0.1453	0.2183	0.2210	0.2193	0.2133	0.2057
Business Continuity	0.3575	0.3040	0.2138	0.1763	0.2720	0.2650	0.2760	0.2520	0.2470
Accessibility	0.3195	0.2780	0.2060	0.1750	0.2400	0.2380	0.2395	0.2410	0.2418
Extensibility	0.3460	0.2950	0.2090	0.1730	0.2497	0.2517	0.2503	0.2483	0.2473
Flexibility	0.3503	0.3043	0.2247	0.1907	0.2623	0.2550	0.2587	0.2660	0.2693
Detectability	0.3247	0.2910	0.2073	0.1757	0.2423	0.2517	0.2473	0.2377	0.2327
Scalability	0.3445	0.2940	0.2090	0.1735	0.2490	0.2500	0.2500	0.2485	0.2475
Traceability	0.3205	0.2745	0.1910	0.1565	0.2290	0.2300	0.2300	0.2280	0.2270

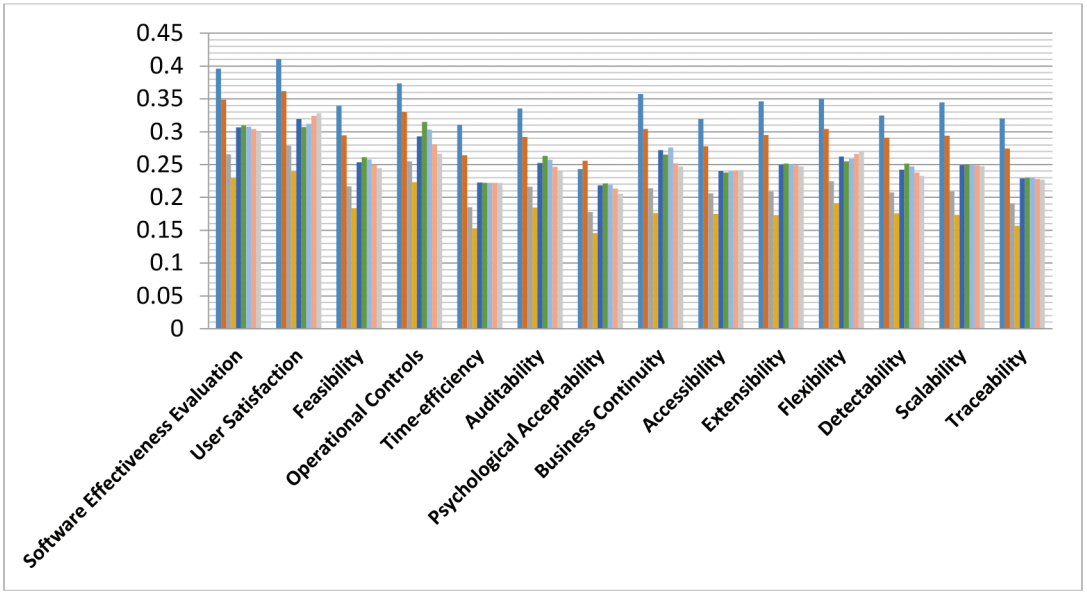

Figure 10 Graphical representation of variations in level 3 attributes.

Table 11 Difference between ratings of level 1 attributes.

S. No.	Characteristics of Level 1	Fuzzy SAM	SAM	Correlation Coefficient
1	Dependability	0.6080	0.6100	0.9463
2	Trustworthiness	0.6190	0.6400	
3	Human trust	0.5950	0.6000	

SAM, simple average method.

Table 12 Difference between ratings of level 2 attributes.

S. No.	Characteristics of Level 2	Fuzzy SAM	SAM	Correlation Coefficient
1	Reliability	0.4307	0.4440	0.8160
2	Availability	0.3825	0.3935	
3	Authentication	0.3385	0.3510	
4	Maintainability	0.3840	0.3935	
5	Confidentiality	0.4265	0.3845	
6	Accountability	0.4230	0.4230	
7	Consumer integrity	0.3740	0.3780	
8	Survivability	0.4150	0.4350	

SAM, simple average method.

Table 13 Difference between ratings of level 3 attributes.

S. No.	Characteristics of Level 2	Fuzzy SAM	SAM	Correlation Coefficient
1	Software effectiveness evaluation	0.3068	0.2911	0.9115
2	User satisfaction	0.3193	0.3220	
3	Feasibility	0.2536	0.2416	
4	Operational controls	0.2931	0.2521	
5	Time-efficiency	0.2226	0.2206	
6	Auditability	0.2525	0.2365	
7	Psychological acceptability	0.2183	0.2087	
8	Business continuity	0.2720	0.2435	
9	Accessibility	0.2400	0.2400	
10	Extensibility	0.2497	0.2447	
11	Flexibility	0.2623	0.2690	
12	Detectability	0.2423	0.2283	
13	Scalability	0.2490	0.2440	
14	Traceability	0.2290	0.2245	

SAM, simple average method.

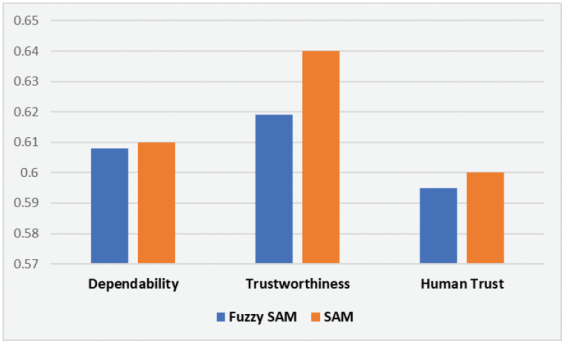

Figure 11 | Difference between results of level 1 attributes.

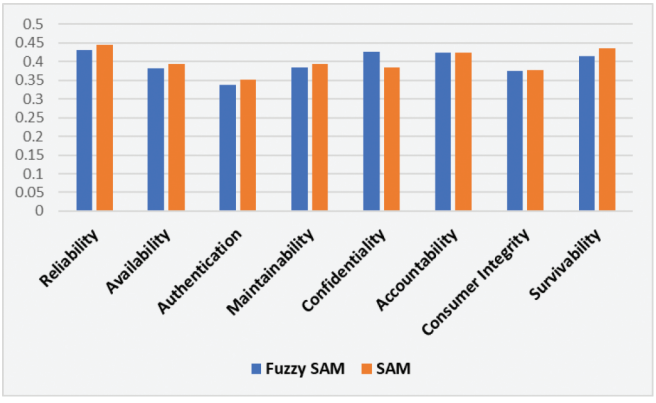

Figure 12 | Difference between the results of level 2 attributes.

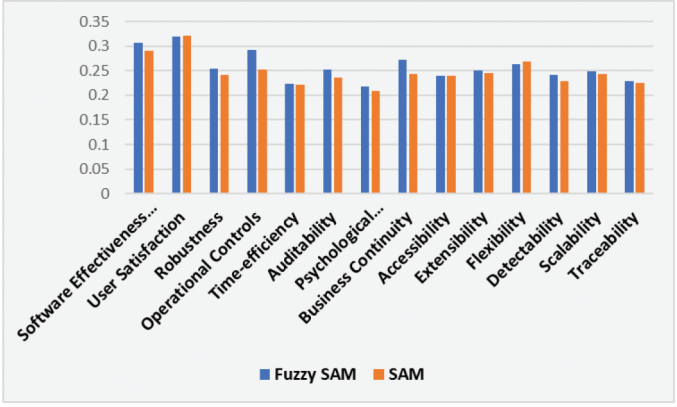

Figure 13 | Difference between results of level 3 attributes.

- Security durability depends on its attributes such as dependability, human trust, and trustworthiness and it can be assessed by quantifying its attributes and its hierarchical sub-attributes.
- The findings of the work will help in improving security durability of software by improving its life at user-end.
- The results will also help the developers to consider higher prioritized attributes of security durability while developing software so that users gets software whose security is longer.
- Also the results of this assessment would help to produce and direct guidelines for developers to tackle the problem of software durability and security.
- Sensitivity analysis has been done to show the variations between results. This validates that the results are highly dependent on its variable of defuzzification which α and β.
- For statistical validation correlation coefficient is calculated. It ranges near 1 and hence proves the strength of bond between the results of Fuzzy SAM and SAM are negligible.
- The Fuzzy SAM used in this analysis may be improved by attaching weights into it. Hence, further new methods can be developed to assess software security durability in future.
- Further work can be done on improving usability with security durability in software to improve the overall quality in customer satisfaction.

The discussion and future work illustrates that assessment of software security durability is significant and vital in its own way. Still this assessment may have some limitations which can be controlled in the future work. Limitations of the results are as follows:

- The data collected for the real-time application of BBAU entrance software is small. The results may vary if the data is large.
- There might be more security attributes other than those identified in this work. Results of ratings may change as per the number of attributes.
- The methodology proposed in this work is purely based on the data collected from experts, which may be biased or may not be the opinion of a large set of population. Hence, a large dataset may help in giving more precise and accurate results.

8. CONCLUSION

In order to provide a significant and improved measurement of security which lasts for the longer duration, it is required to correlate security and durability attributes. It is evident from the literature survey that there is no known, complete, and comprehensive work that exists to assess security durability and its attributes at an early stage of the development process. The proposed model, for the quantitative assessment of security durability attributes in the form of ratings, has been validated through statistical analysis. It is apparent that this methodology can be used effectively in assessing the life span of security and minimizing the cost and time spent over maintenance of security and flaws occurring from time to time. Statistical analysis has been made to strengthen the claim that experts' views are considerable while estimating the security durability attributes in the proposed model.

ACKNOWLEDGMENTS

Authors are thankful to College of Computer and Information Sciences, Prince Sultan University for providing the fund to carry out the work.

REFERENCES

[1] A Forrester Consulting Coverity, The software security risk report the road to application security begins in development September 2012, 2012, http://www.coverity.com/library/pdf/the-softwaresecurity-risk-report.pdf.

[2] C. Kelty, S. Erickson, The Durability of Software, Meson Press, Germany, 2015, pp. 1–13.
[3] Y. Asnar, P. Giorgini, M. Fabio, Z. Nicola, From trust to dependability through risk analysis, in Proceeding Of The Second International Conference on Availability, Reliability and Security, International Conference on Application of Concurrency to System Design, IEEE Xplore, 2007, pp. 19–26.
[4] Addressing software security in federal acquisition process. http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=55E94ECFDC445D24E058F6334BB525CD?doi=10.1.1.300.2941&rep=rep1&type=pdf.
[5] E. Nathan, When good software goes bad: the surprising durability of an ephemeral technology, in Mice (Mistakes, Ignorance, Contingency, and Error) Conference, Munich, 2014, pp. 1–16.
[6] R. Kumar, S.A. Khan, R.A. Khan, Durability challenges in software engineering, Crosstalk J. Defense Softw. Eng. 10 (2016), 29–31.
[7] R. Kumar, S.A. Khan, R.A. Khan, Revisiting software security: durability perspective, Int. J. Hybrid. Inf. Technol. (SERSC). 8 (2015), 311–322.
[8] B. Bulgurcu, H. Cavusoglu, I. Benbasat, Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness, Inf. Secur. Policy Compliance. 34 (2010), 523–548.
[9] C. Knittel, R. Feenstra, Re-assessing the U.S. quality adjustment to computer prices: the role of durability and changing software, Working Paper Series-Department of Economics, No 10857, NBER Working Papers from National Bureau of Economic Research, Inc., 2004, pp. 2–50.
[10] D. Linden, A. Rashid, The effect of software warranties on cybersecurity, ACM SIGSOFT Softw. Eng. Notes. 43 (2018), 31–35.
[11] E.V. Bartlett, S. Simpson, Durability and reliability, alternative approaches to assessment of component performance over time, 2013. https://www.irbnet.de/daten/iconda/CIB8616.pdf.
[12] T.L. Saaty, How to make a decision: the analytic hierarchy process, Eur. J. Oper. Res. 48 (1990), 9–26.
[13] Y. Xu, F.J. Cabrerizo, E. Herrera-Viedma, A consensus model for hesitant fuzzy preference relations and its application in water allocation management, Appl. Soft Comput. 58 (2017), 265–284.
[14] Y. Xu, C. Li, X. Wen, Missing values estimation and consensus building for incomplete hesitant fuzzy preference relations with multiplicative consistency, Int. J. Comput. Intell. Syst, 11 (2018), 101–119.
[15] Y. Xu, X. Wen, H. Sun, H. Wang, Consistency and consensus models with local adjustment strategy for hesitant fuzzy linguistic preference relations, Int. J. Fuzzy Syst. 20 (2018), 2216–2233.
[16] H.N. Cho, H.H. Choi, K.Y. Kim, A risk assessment methodology for incorporating uncertainties using fuzzy concepts, Reliab. Eng. Syst. Safe. 78 (2002), 173–183.
[17] Y. Xu, L. Chen, R.M. Rodríguez, F. Herrera, H. Wang, Deriving the priority weights from incomplete hesitant fuzzy preference relations in group decision making, Knowl. Based Syst. Knowl. Based Syst. 99 (2016), 71–78.
[18] Y. Xu, X. Wen, W. Zhang, A two-stage consensus method for large-scale multi-attribute group decision making with an application to earthquake shelter selection, Comput. Ind. Eng. 116 (2018), 113–129.
[19] X. Liu, Y. Xu, R. Montes, R.-X. Ding, F. Herrera, Alternative ranking-based clustering and reliability index-based consensus reaching process for hesitant fuzzy large scale group decision making, IEEE Trans. Fuzzy Syst. 27 (2019), 159–171.
[20] L. Xia, Y. Xu, F. Herrera, Consensus model for large-scale group decision making based on fuzzy preference relation with self-confidence: detecting and managing overconfidence behaviors, Inf. Fusion. 52 (2019), 245–256.
[21] L.A. Zadeh, Fuzzy sets, Inf. Control. 8 (1965), 338–353.
[22] Y.-R. Syau, H.-T. Hsieh, E. Stanley Lee, Fuzzy numbers in the credit rating of enterprise financial condition, Rev. Quant. Finance Act. 17 (2001), 351–360.
[23] Z. Zieliski, J. Chudzikiewicz, J. Furtak, An approach to integrating security and fault tolerance mechanisms into the military IOT, in: R. Chakraborty, J. Mathew, A. Vasilakos (Eds.), Security and Fault Tolerance in Internet of Things, Springer, Singapore, 2019.
[24] H. Assal, S. Chiasson, Think secure from the beginning, a survey with software developers, in CHI Conference on Human Factors in Computing Systems Proceedings, ACM, Glasgow, 2019, pp. 1–13.
[25] T.D. Oyetoyan, M.G. Jaatun, D.S. Cruzes, Measuring developers' software security skills, usage, and training needs, in: Exploring Security in Software Architecture and Design, IGI Global, 2019.
[26] W. Kluwer, Starting Your Software Security Assurance Program, ITARC, Stockholm, 2015.
[27] D.B. Parker, Restating the foundation of information security, in Proceeding of the Eighth International Conference on Information Security, Netherlands, 1992, pp. 139–151.
[28] R. Thomas, Durable, low cost educational software, in Computer Assisted Learning: Selected Contributions from the CAL'93 Symposium, France, 1994, pp. 65–72.
[29] A. Takanen, Fuzzing for software security testing and quality assurance, 2010. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.398.6662&rep=rep1&type=pdf
[30] S.M. Baas, H. Kwakernaak, Rating and ranking of multiple - aspect alternatives using fuzzy sets, Automatica. 13 (1977), 47–58.
[31] S. Ammar, R. Wright, Applying fuzzy-set theory to performance evaluation, Socio-Econ. Plan. Sci. 34 (2000), 285–302.
[32] A. Mardani, A. Jusoh, K. MD Nor, Z. Khalifah, N. Zakwan, A. Valipour, Multiple criteria decision-making techniques and their applications – a review of the literature from 2000 to 2014, Int. J. Inf. Technol. Decis. Making. 17 (2018), 391–466.
[33] S.K. Dubey, S. Pandey, Measurement of usability of office application using a fuzzy multi-criteria technique, Int. J. Inf. Technol. Comput. Sci. 4 (2015), 64–72.
[34] L. Lin, H.M. Lee, A fuzzy software quality assessment model to evaluate user satisfaction, in Proceeding of the Second International Conference on Innovative Computing, Information and Control, Washington, 2007, pp. 438–442.
[35] J. Muñoz, F. Toutouh, F. Jaime, A review of dynamic verification of security and dependability properties, in: R. Abassi (Ed.), Artificial Intelligence Security Challenges Emerging Networks, IGI Global, Hershey, 2019.
[36] K. Ball, S.D. Esposti, S. Dibb, V. Pavone, E. Santiago-Gomez, Institutional trustworthiness and national security governance: evidence from six European countries, Governance. 32 (2019), 103–121.
[37] K. Bylykbashi, D. Elmazi, K. Matsuo, M.L. Barolli, Effect of security and trustworthiness for a fuzzy cluster management system in VANETs, Cogn. Syst. Res. 55 (2019), 153–163.

[38] A.B. Saxena, M. Dawe, Trust framework for IAAS—a tool based on security checks through standards and certifications. in: S. Satapathy, A. Joshi (Eds.), Information and Communication Technology for Intelligent Systems, Springer, Singapore, 2019.
[39] C.-W. Chang, C.-R. Wu, H.-L. Lin, Integrating fuzzy theory and hierarchy concepts to evaluate software quality, Softw. Qual. J. 16 (2008), 263–276.
[40] P.R. Srivastava, A.P. Singh, K.V. Vageesh, Vageesh, Assessment of software quality: a fuzzy multi criteria approach, in: M. Chis (Ed.), Evolution of Computation and Optimization Algorithms in Software Engineering: Applications and Techniques, IGI Global, Hershey, 2010, pp. 200–219.
[41] L. Mikhailov, Deriving priorities from fuzzy pairwise comparison judgements, Fuzzy Sets Syst. 134 (2013), 365–385.

Appendix A

Table A1 Numeric data for level 1.

Attributes of Level 1/ Experts Opinion	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	E12	E13	E14	E15	E16	E17	E18	E19	E20
Dependability	0.3	1.0	0.7	0.1	1.0	0.3	0.9	0.7	0.9	0.7	0.3	0.1	0.9	0.7	0.3	1.0	0.9	0.7	0.1	0.7
Trustworthiness	0.7	0.9	0.3	0.7	0.9	0.7	0.1	0.3	1.0	0.3	0.9	0.7	1.0	0.3	0.9	0.3	0.7	0.3	0.9	0.9
Human Trust	0.1	0.3	0.9	0.3	0.7	0.9	1.0	0.9	0.3	0.1	1.0	0.3	0.7	0.1	0.7	0.1	1.0	0.9	0.7	1.0

Table A2 Numeric data for level 2.

Attributes of Level 3/ Experts Opinion	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	E12	E13	E14	E15	E16	E17	E18	E19	E20
Availability	0.3	0.1	0.7	1.0	0.3	1.0	0.7	0.9	0.7	1.0	0.7	0.3	0.9	0.1	0.7	0.9	0.3	1.0	0.7	0.3
Reliability	0.7	0.9	1.0	0.7	0.9	0.3	0.9	0.7	0.9	0.7	0.3	0.9	0.7	0.9	0.3	0.3	0.7	0.9	1.0	0.7
Maintainability	0.9	0.7	0.9	0.3	0.7	0.9	0.3	1.0	0.3	0.1	0.9	0.3	0.3	0.7	0.9	0.7	0.9	0.3	0.7	0.9
Confidentiality	1.0	0.3	0.7	0.7	0.9	0.1	1.0	0.9	1.0	0.9	0.7	0.1	1.0	0.3	1.0	0.9	0.3	0.7	0.9	1.0
Authentication	0.1	0.1	0.3	0.9	0.7	0.7	0.3	0.7	0.3	0.7	0.9	0.3	0.9	1.0	0.1	1.0	0.9	0.3	0.7	0.1
Accountability	0.3	1.0	0.7	1.0	0.9	0.9	0.7	0.9	0.7	0.1	0.3	0.7	0.1	0.7	0.3	0.7	1.0	0.1	0.3	0.9
Survivability	0.7	0.9	0.3	0.7	1.0	0.7	0.3	1.0	0.7	0.9	0.1	0.9	0.9	0.3	0.9	0.3	0.7	0.9	0.7	0.7
Consumer Integrity	1.0	0.7	0.9	0.3	0.7	0.3	0.9	0.3	0.1	1.0	0.7	1.0	0.7	0.9	0.7	0.1	0.3	0.9	0.9	0.3

Table A3 Numeric data for level 3.

Attributes of Level 2/ Experts Opinion	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	E12	E13	E14	E15	E16	E17	E18	E19	E20
Auditability	0.3	0.7	0.9	1.0	0.1	0.3	1.0	0.1	0.7	0.9	0.1	1.0	0.3	0.9	0.1	0.7	0.9	1.0	0.3	0.7
Feasibility	0.9	0.3	0.1	0.9	1.0	0.9	0.7	0.3	0.3	0.1	1.0	0.7	0.7	0.1	0.9	0.7	1.0	0.9	0.1	0.9
Accessibility	0.3	1.0	0.9	0.9	0.3	0.7	0.3	0.1	0.1	0.3	0.9	0.7	0.7	0.7	0.7	0.9	0.7	0.9	0.7	0.9
S/W Effective Evaluation	0.9	0.9	0.9	0.9	0.9	0.7	0.7	0.7	0.9	0.7	0.7	0.7	0.9	0.9	0.9	0.9	0.7	1.0	1.0	1.0
Operational Controls	1.0	1.0	0.9	0.9	1.0	0.9	1.0	0.9	0.7	0.9	0.7	0.9	1.0	1.0	0.7	0.9	0.9	0.9	1.0	1.0
Time-Efficiency	0.3	0.1	0.1	0.7	0.7	0.7	1.0	0.9	0.9	0.7	0.7	0.9	0.1	0.3	0.7	0.3	0.3	0.3	0.7	0.1
User Satisfaction	0.9	0.9	0.9	1.0	0.7	0.7	0.7	0.3	0.7	0.7	1.0	1.0	1.0	0.9	0.9	0.7	0.9	0.7	0.9	0.7
Business Continuity	0.7	0.7	0.3	0.1	0.1	0.7	0.7	0.1	0.1	0.3	0.3	0.7	0.7	1.0	1.0	0.7	0.7	0.9	0.9	0.7
Scalability	0.7	0.7	0.1	0.3	0.9	0.9	1.0	1.0	0.7	0.7	0.7	0.7	0.3	0.1	0.1	0.9	0.7	0.1	0.9	0.9
Traceability	0.7	0.7	0.1	0.1	0.3	0.3	0.7	0.7	0.9	0.7	0.7	0.9	0.7	0.9	0.1	0.3	0.7	0.3	0.7	0.9
Detectability	0.3	0.7	0.3	0.7	0.3	0.9	0.7	1.0	0.1	0.9	0.7	1.0	0.3	0.1	0.9	0.7	0.3	0.7	0.3	0.3
Extensibility	0.7	0.9	0.1	0.7	0.1	0.7	0.9	0.1	0.7	1.0	0.7	0.3	0.7	0.9	0.7	0.9	0.1	0.3	0.7	0.9
Flexibility	0.7	0.1	1.0	0.9	0.3	1.0	0.7	0.9	0.9	0.7	0.3	1.0	0.1	0.7	0.9	0.1	1.0	0.7	0.9	0.3
Psychological Acceptability	0.7	0.9	0.3	0.7	0.9	0.3	0.1	0.1	0.9	1.0	0.7	0.1	0.3	0.7	0.3	0.9	0.7	0.7	0.7	0.7