Computer Systems Science & Engineering
DOI:10.32604/csse.2022.021564
Article

Tech Science Press

A Usability Management Framework for Securing Healthcare Information System

Hosam Alhakami[1], Abdullah Baz[2], Wajdi Alhakami[3], Abhishek Kumar Pandey[4], Alka Agrawal[4] and Raees Ahmad Khan[4,*]

[1]Department of Computer Science, College of Computer and Information Systems, Umm Al-Qura University, Makkah, 21955, Saudi Arabia
[2]Department of Computer Engineering, College of Computer and Information Systems, Umm Al-Qura University, Makkah, 21955, Saudi Arabia
[3]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
[4]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, 226025, India
*Corresponding Author: Raees Ahmad Khan. Email: khanraees@yahoo.com
Received: 07 July 2021; Accepted: 08 August 2021

Abstract: Transformation from conventional business management systems to smart digital systems is a recurrent trend in the current era. This has led to digital revolution, and in this context, the hardwired technologies in the software industry play a significant role However, from the beginning, software security remains a serious issue for all levels of stakeholders. Software vulnerabilities lead to intrusions that cause data breaches and result in disclosure of sensitive data, compromising the organizations' reputation that translates into, financial losses and compromising software usability as well. Most of the data breaches are financially motivated, especially in the healthcare sector. The cyber invaders continuously penetrate the E- Health data because of the high cost of the data on the dark web. Therefore, security assessment of healthcare web-based applications demands immediate intervention mechanisms to weed out the threats of cyber-attacks for the sake of software usability. The proposed disclosure is a unique process of three phases that are combined by researchers in order to produce and manage usability management framework for healthcare information system. In this most threatened time of digital era where, Healthcare data industry has borne the brunt of the highest number of data breach episodes in the last few years. The key reason for this is attributed to the sensitivity of healthcare data and the high costs entailed in trading the data over the dark web. Hence, usability management of healthcare information systems is the need of hour as to identify the vulnerabilities and provide preventive measures as a shield against the breaches. The proposed unique developed model of usability management workflow is prepared by associating steps like learn; analyze and manage. All these steps gives an all in one package for the healthcare information management industry because there is no systematic model available which associate identification to implementation steps with different evaluation steps.

Keywords: Smart healthcare; healthcare industry; usability; security

1 Introduction

Pervasive technologies have greatly influenced the conventional healthcare infrastructure and provided effective means to enhance the present day healthcare services. E-health has been the harbinger of the revolutionary changes in the healthcare sector. The digital health services are not only cost effective but have massive outreach [1,2]. Higher levels of accessibility to E-health services has also improved the patient-doctor interaction as patients can now contact their doctors from any remote locale without making frequent visits to the hospitals. Healthcare Information Software Systems (P) have gained consistent popularity in healthcare sector [3,4], and thus, healthcare data is deemed to be one of the most sensitive and confidential data in such a context [5,6]. The present day priority of the healthcare sector is to optimize the use of P healthcare service providers to manage and utilize health related data in an efficient way. But ensuring the security of these software systems carrying confidential data and keeping them breach-proof has become a significant issue for both the service providers and patients [7,8]. Healthcare sector recorded the highest number of data breaches in the year 2019 [9,10]. In the first half of the present year-2020 itself, 255 healthcare data breach cases have been reported.130 of these instances are because of hacking/IT incidents, i.e., 50.98% of the total [11,12]. These statistics prove that software systems used in healthcare sector either provide immature security services, or such complex security services that directly impact the systems' usability.

Just as a flawed software system is vulnerable and prey to attacks, a software system with complex security also lacks in usability and, therefore, is of no value [13,14]. Such systems can lead to loss of business continuity and increase the user error rate. Moreover, the quality of the software is significantly influenced by usable-security [15,16]. To address these issues there is a need to have a systematic workflow model that gives an innovative and unique usability management of system after the vulnerability identification and prevention. Because managing the whole system after a deep identification and management is still a challenging task for digital healthcare systems and it's crucial also for them to retrieve the system in previous systematic condition.

Further, To attain the usability significance and its issues in relevant field we describe some incidents for better understanding as several software business studies have cited that from $37.48 billion in 2017, the software market is likely to amass $74.96 billion in 2022; an increment of 50% [17,18]. Hence, this expansion in demand needs to be met with ideal usable-security mechanisms. Designing and building secure software products is in itself a complex task, but the complex security mechanism of these products makes them less usable [19,20]. Thus, usable-security continues to be a contentious issue for the developers as they seek for the perfect amalgamation of optimum security as well as usability, without affecting the usability of the systems.

In the view of the forgoing discussion it is clearly portrayed that there is a need to have a systematic and effective workflow model that guide the healthcare digital systems to manage the data and its condition after a deep identification and prevention of threat.

2 Theoretical Framework

To understand the proposed developed process of usability management framework of secure healthcare information system it is important to understand every step in a detailed way for better understanding. It will nevertheless be understood that no limitation of the scope of the development is thereby intended, such alterations and further modifications in the illustrated system, and such further applications of the principles of the development as illustrated therein being contemplated as would normally occur to one skilled in the art to which the development relates.

It will be understood by those skilled in the art that the foregoing general description and the following detailed description are exemplary and explanatory of the development and are not intended to be restrictive thereof.

Now, embodiment with a detailed description of the proposed process is written below with appropriate reference of figures.

Fig. 1 describes the whole proposed process which is created by authors to produce usability management framework for secure healthcare information system by attaining three major and eight minor uniquely combined steps.

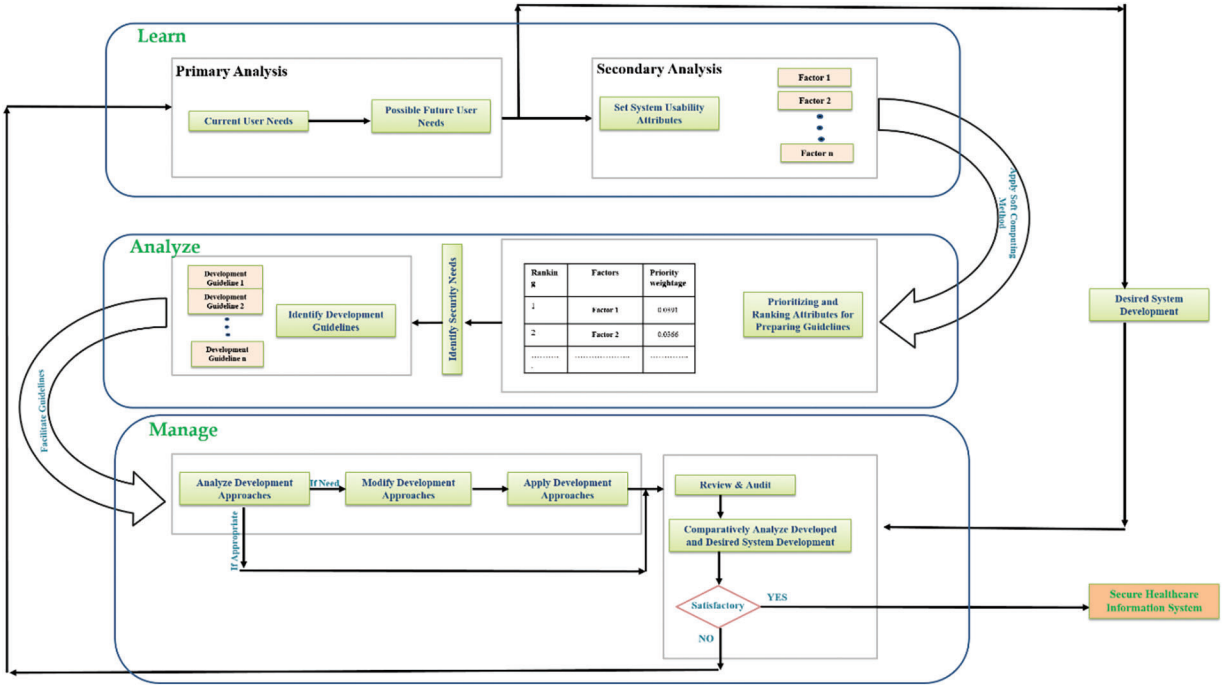

Figure 1: The proposed unique processes

All these three major and eight minor steps associate learn; analyze and management as major steps. Now if we get into the detailed description of proposed process the first initial step is learn. Learn is a step where the proposed snake model starts its process. As a first minor step in this major step model initially analyze and document the current user needs and then after that analyze possible future user needs as shown in Fig. 2 for systematic and long usability of system from its base.

Now, as a second minor step of this proposed major phase of model is identifying and setting up attributes of desired system that are significantly necessary for development and long usability of system.

Further, after identifying the needs from current and possible future users there is another unique step (shown in Fig. 3) is present in proposed model which is preparing a desired system development and its functionality demo based on the assessment of user needs for further use in next phases. This type of stepping is unique in itself.

Moreover, after successfully extracting the attributes in first major phase of model the process applies a soft computing method for prioritizing and assigning ranks to those in second analyze phase of model (shown in Fig. 4).

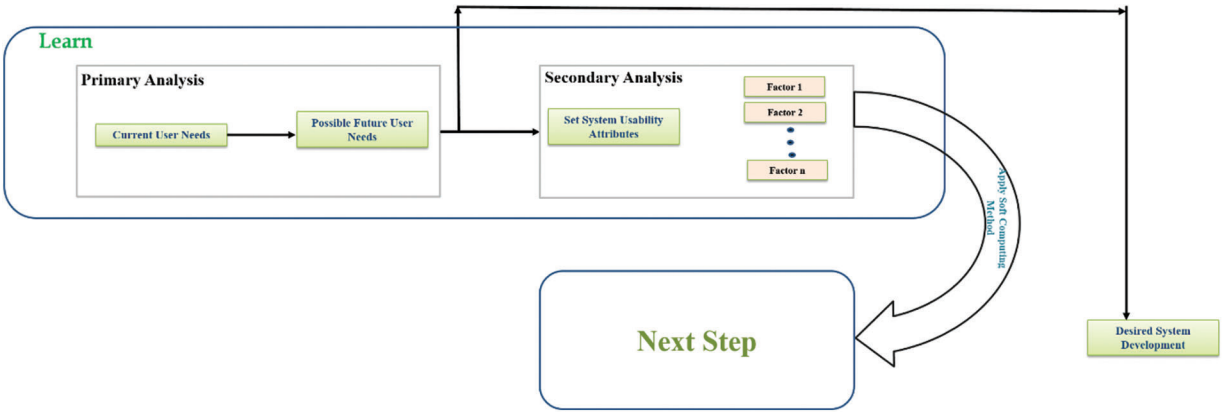

Figure 2: Briefly portray the first learn step of proposed snake model. The step illustrate the initial start of model where the process gets start with brainstorming step like: user needs analysis and its documentation

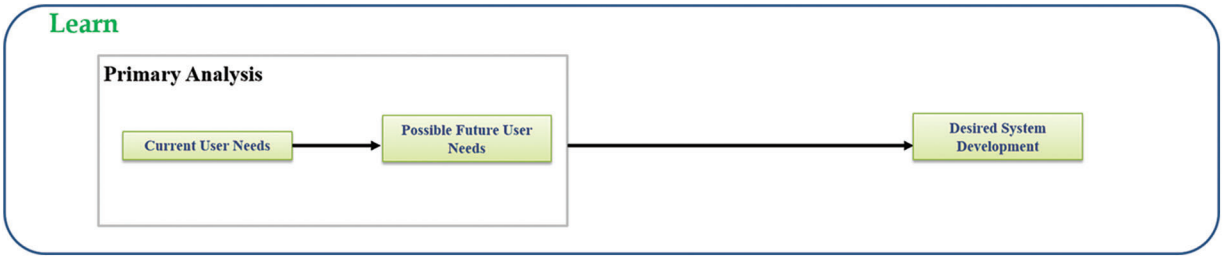

Figure 3: A descriptive illustration of additional step for preparing replica of desired system design which is unique idea that is associated in model

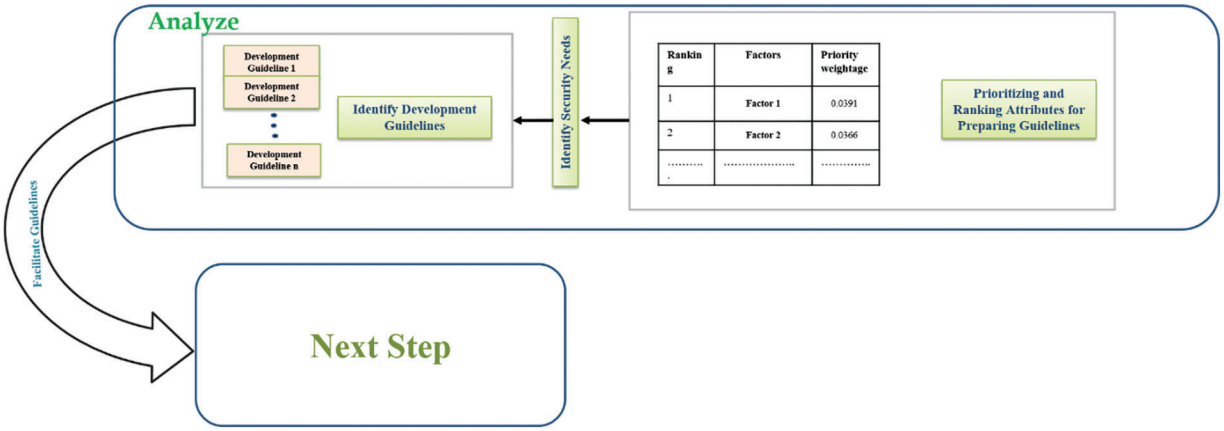

Figure 4: An illustration of second analyze step where the proposed model assess requirements of system by applying soft computing techniques

Which make them easier to understand and adopt by designer based on their ranking. This step has also a unique idea of ranking which gives the system a solid foundation from its base. Further, in this major phase the next step is identifying the security needs according to evaluated attributes and their rank for systematic compatibility in security and usability of system. Now, after identifying the appropriate security needs of evaluated attributers the process prepare or identify the guidelines for development of system based on

previous steps result as shown in Fig. 4. Therefore, after successfully preparing the guidelines in second phase of model the process now jump into the last and third phase (shown in Fig. 5) of model management by a step named apply guidelines.

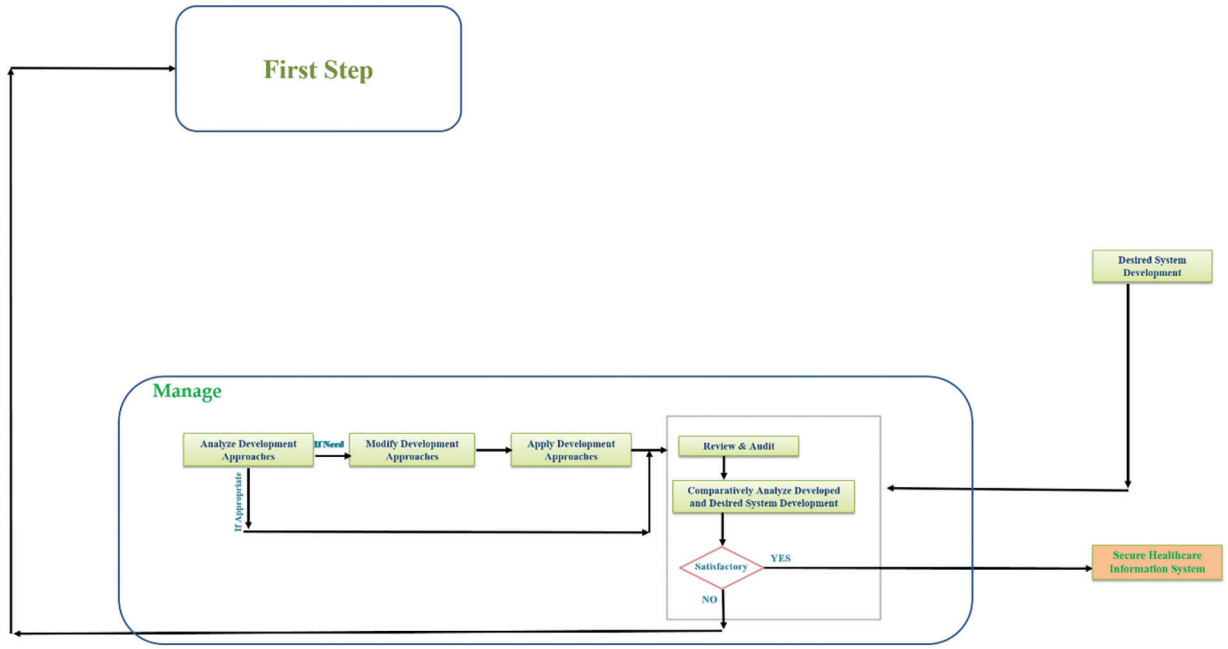

Figure 5: A description of third and last step which is manage from the proposed snake model. The illustrated figure systematically preview the steps of management for secure healthcare information system development or management

This step allows the process to implement the prepared guidelines into the development and then the first step of this phase starts by analyzing the applied guidelines in a security as well as usability manner. Now here if the analysis is satisfied then the process directly hump into the second minor step of this last phase. However, if the analysis report has some issue with the implementation of guidelines in development steps then the model direct the process on modification of development approach step and after this step the process goes to apply modified development approach. The second step of last phase in review and audit. Which associate some unique stepping and idea of comparison for better development in the field. This last step has a process which review and then audit (shown in Fig. 6) the developed system and its functionality from the demo replica of desired system and its functionality prepared in first phase of model.

This type of step creates a possibility for managing the system in a more solid manner and gives an ideal pathway to the designer in managing security and usability both at the same time. Now during this review and audit step there is an inner step which gives a decision making step to the process and ask if the review and audit finds everything satisfying and appropriate based on the currently developed and desired ones comparison the it allows the model to produce secure healthcare information system. However, it the review and audit report find anything not satisfactory then the model direct the process return towards the start from first phase again. This type of cycle process gives a loop power to the proposed designing model.

This is the descriptive working functionality of the model. Now after defining the working process of proposed model, authors also test the developed process on selected healthcare organization named SGPGI (Sanjay Gandhi Post Graduate Institute), Lucknow, India [13]. The simulated experiment is obtained by implementing Fuzzy AHP-TOPSIS (Fuzzy based Analytical Hierarchy Process and

Technique for Order of Preference by Similarity to Ideal-Solutions) which is described in detail by authors in their scientific publication [21–23]. Detailed results in numeric form are described and analyzed in next section of the paper which prove the industrial applicability of proposed model.

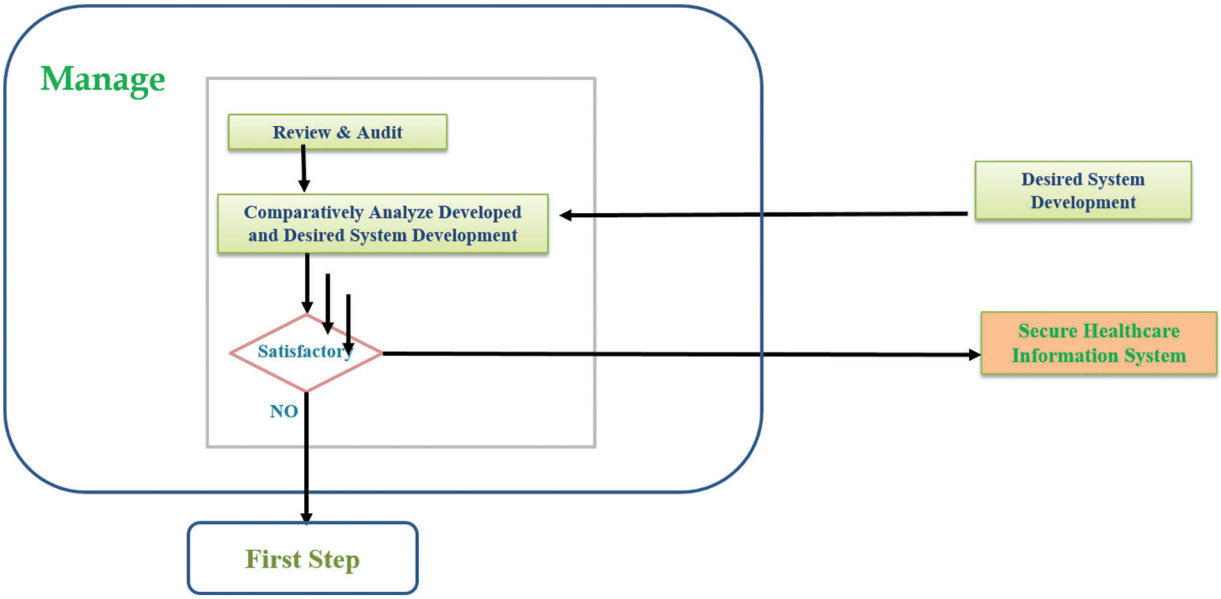

Figure 6: A brief description of last step review and audit which incorporate comparison based unique idea of model through figure

3 Industry Applicability

To make it more systematic and efficient as proposed model, authors describe all the analysis results during the implementation process. In order to apply the adopted simulation mechanism fuzzy based AHP approach is used to categorize specific weights of the steps and their sub steps by implementing various formulas described in [24–26]. Measuring quality of a system which also includes usable-security is not an easy task [27] because making quantitative evaluation of a qualitative attribute, by rationale, is a complex work. Numerical analysis of this work would provide a quantitative evaluation of usable-security of healthcare information systems. For this, a case study on 6 different healthcare information software systems was undertaken. The use of AHP-TOPSIS under the fuzzy environment made this work more effective and efficient [28,29]. A tabular form of industry performance evaluation is shown in Tabs. 1–17.

On the basis of the preference scores, the ranking order of the 6 selected healthcare projects for performance simulation is as: HISS-2, HISS-1, HISS-5, HISS-3, HISS-4, and HISS-6. From this analysis, it has been found that the performance assessment performed on 6 different healthcare information systems projects shows that HISS-2 provides better results to address main security as well as usability management based on the proposed model.

Table 1: Fist level attributes fuzzy pair-wise comparison matrix

	S1	S2	S3	S4	S5
S1	1.00000, 1.00000, 1.00000	1.87000, 2.57000, 3.21000	1.46000, 1.68000, 1.97000	1.44000, 2.44000, 3.38650	0.47000, 0.57000, 0.79000
S2	-	1.00000, 1.00000, 1.00000	0.61000, 0.78000, 1.03000	0.77100, 0.95000, 1.24000	0.16000, 0.20000, 0.25000
S3	-	-	1.00000, 1.00000, 1.00000	0.77000, 1.05000, 1.36000	0.21000, 0.25000, 0.31000
S4	-	-	-	1.00000, 1.00000, 1.00000	0.20000, 0.23000, 0.29000
S5	-	-	-	-	1.00000, 1.00000, 1.00000

Table 2: Local fuzzy pair-wise comparison matrix for level 2nd attributes S11 and S12

	S11	S12
S11	1.00000, 1.00000, 1.00000	0.30100, 0.39000, 0.56100
S12	-	1.00000, 1.00000, 1.00000

Table 3: Local fuzzy pair-wise comparison matrix for level 2nd attributes S21, S22 and S23

	S21	S22	S23
S21	1.00000, 1.00000, 1.00000	0.41000, 0.55000, 0.79000	0.50000, 0.70000, 0.93000
S22	-	1.00000, 1.00000, 1.00000	0.79000, 0.88000, 1.02000
S23	-	-	1.00000, 1.00000, 1.00000

Table 4: Local fuzzy pair-wise comparison matrix for level 2nd attributes S31, S32, and S33

	S31	S32	S33
S31	1.00000, 1.00000, 1.00000	0.55100, 0.58800, 0.66500	0.22600, 0.27600, 0.35700
S32	-	1.00000, 1.00000, 1.00000	0.69000, 0.88600, 1.10000
S33	-	-	1.00000, 1.00000, 1.00000

Table 5: Local fuzzy pair-wise comparison matrix for level 2nd attributes S41 and S42

	S41	S42
S41	1.00000, 1.00000, 1.00000	0.56950, 0.78600, 1.15600
S42	-	1.00000, 1.00000, 1.00000

Table 6: Local fuzzy pair-wise comparison matrix for level 2nd attributes S51 and S52

	S51	S52
S51	1.00000, 1.00000, 1.00000	0.56980, 0.71950, 0.96990
S52	-	1.00000, 1.00000, 1.00000

Table 7: Defuzzification and local weights of 1st level attributes

	S1	S2	S3	S4	S5	Weights
S1	1.00000	2.55000	1.70000	2.43000	0.59900	0.24000
S2	0.39200	1.00000	0.79600	0.97700	0.20700	0.09500
S3	0.58800	1.25600	1.00000	1.05600	0.25300	0.12200
S4	0.41200	1.02400	0.94700	1.00000	0.23600	0.10300
S5	1.66900	4.82400	3.95000	4.24300	1.00000	0.44200
C.R.=0.002500						

Table 8: Defuzzified local weights of level 2nd attributes S11 and S12

	S11	S12	Weights
S11	1.00000	0.41000	0.29100
S12	2.43250	1.00000	0.70900
C.R.=0.000000			

Table 9: Defuzzified local weights of level 2nd attributes S21, S22, and S23

	S21	S22	S23	Weights
S21	1.00000	0.57300	0.70900	0.24200
S22	1.74400	1.00000	0.89500	0.37900
S23	1.41100	1.11800	1.00000	0.38000
C.R.= 0.005800				

Table 10: Defuzzified local weights of level 2nd attributes S31, S32, and S33

	S31	S32	S33	Weights
S31	1.00000	0.59800	0.28400	0.16900
S32	1.67300	1.00000	0.89100	0.34900
S33	3.52000	1.12300	1.00000	0.48200
C.R.= 0.022700				

Table 11: Defuzzified local weights of level 2nd attributes S41 and S42

	R41	R42	Weights
S41	1.00000	0.82400	0.45200
S42	1.21300	1.00000	0.54800
C.R.=0.000000			

Table 12: Defuzzified local weights of level 2nd attributes S51 and S52

	S51	S52	Weights
S51	1.00000	0.74500	0.42700
S52	1.34300	1.00000	0.57300
C.R.=0.000000			

Table 13: Summarized results of level 1st and level 2nd local and global attribute weights

Main	Local weights	Sub	Local weights	Overall weights	Ranks
S1	0.24000	S11	0.29100	0.06984	4
		S12	0.70900	0.17016	3
S2	0.09500	S21	0.24200	0.02299	11
		S22	0.37900	0.03601	10
		S23	0.38000	0.03610	9
S3	0.12200	S31	0.16900	0.02062	12
		S32	0.34900	0.04258	8
		S33	0.48200	0.05881	5
S4	0.10300	S41	0.45200	0.04656	7
		S42	0.54800	0.05644	6
S5	0.44200	S51	0.42700	0.18873	2
		S52	0.57300	0.25327	1

4 Sensitivity Analysis

With the help of same data and method, sensitivity analysis as a technique or tool has a significant role in validating a research analysis. It is practiced for finding the impact or effect of independent variable on dependent variable when changes are made in the independent variable values. Such an approach helps the researchers in corroborating the results [20–23]. The resulted weights generated by fuzzy based AHP-TOPSIS have been considered as variables. The selected attribute's weight is changed in every experiment, while the weights of the other attributes remain constant. 12 usable-security attributes have been selected for this study at the last (2nd) level of the hierarchical attribute tree. Therefore, twelve experiments have been carried out, one for each independently and the calculated results are enlisted in the Tab. 18 and Fig. 7.

Table 14: Subjective cognition results of the evaluators in linguistic terms

	HISS-1	HISS-2	HISS-3	HISS-4	HISS-5	HISS-6
S11	4.1800, 6.0900, 7.6400	0.7300, 2.2700, 4.2700	1.0000, 2.6400, 4.6400	1.0000, 2.6400, 4.6400	1.2000, 3.0000, 5.0000	2.8200, 4.8200, 6.7300
S12	4.4500, 6.4500, 8.1800	4.4500, 6.4500, 8.1800	0.7300, 2.2700, 4.2700	0.7300, 2.2700, 4.2700	1.0000, 2.6400, 4.6400	2.0900, 3.9100, 5.8200
S21	1.0000, 2.6400, 4.6400	1.2000, 3.0000, 5.0000	0.8200, 2.4500, 4.4500	4.4500, 6.4500, 8.1800	4.1800, 6.0900, 7.6400	2.8200, 4.8200, 6.6400
S22	0.7300, 2.2700, 4.2700	1.0000, 2.6400, 4.6400	2.9100, 4.8200, 6.7300	1.2000, 3.0000, 5.0000	4.4500, 6.4500, 8.1800	3.5500, 5.5500, 7.3600
S23	4.4500, 6.4500, 8.1800	1.6400, 3.3600, 5.3600	0.7300, 2.2700, 4.2700	2.8200, 4.8200, 6.7300	1.0000, 2.6400, 4.6400	4.4500, 6.4500, 8.1800
S31	1.2000, 3.0000, 5.0000	0.8200, 2.4500, 4.4500	4.4500, 6.4500, 8.1800	1.6400, 3.3600, 5.3600	0.7300, 2.2700, 4.2700	1.2000, 3.0000, 5.0000
S32	1.0000, 2.6400, 4.6400	1.0000, 2.6400, 4.6400	1.2000, 3.0000, 5.0000	0.8200, 2.4500, 4.4500	4.4500, 6.4500, 8.1800	1.0000, 2.6400, 4.6400
S33	0.7300, 2.2700, 4.2700	0.7300, 2.2700, 4.2700	1.0000, 2.6400, 4.6400	1.0000, 2.6400, 4.6400	1.2000, 3.0000, 5.0000	2.8200, 4.8200, 6.7300
S41	0.8200, 2.4500, 4.4500	4.4500, 6.4500, 8.1800	0.7300, 2.2700, 4.2700	0.7300, 2.2700, 4.2700	1.0000, 2.6400, 4.6400	2.0900, 3.9100, 5.8200
S42	4.1800, 6.0900, 7.6400	1.2000, 3.0000, 5.0000	0.8200, 2.4500, 4.4500	4.4500, 6.4500, 8.1800	4.1800, 6.0900, 7.6400	2.8200, 4.8200, 6.6400
S51	4.4500, 6.4500, 8.1800	1.0000, 2.6400, 4.6400	2.9100, 4.8200, 6.7300	1.2000, 3.0000, 5.0000	4.4500, 6.4500, 8.1800	3.5500, 5.5500, 7.3600
S52	6.2700, 8.2700, 9.4500	3.1800, 5.1800, 7.0000	1.6400, 3.3600, 5.3600	1.0000, 2.6400, 4.6400	6.2700, 8.2700, 9.4500	3.9100, 5.9100, 7.5500

Table 15: The normalized fuzzy-decision matrix

	HISS-1	HISS-2	HISS-3	HISS-4	HISS-5	HISS-6
S11	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
S12	0.4600, 0.6700, 0.8600	0.5400, 0.7500, 0.9200	0.5400, 0.7500, 0.9200	0.4600, 0.6700, 0.8600	0.6000, 0.8100, 1.0000	0.4600, 0.6800, 0.8800
S21	0.4600, 0.6700, 0.8600	0.3900, 0.5900, 0.7900	0.3900, 0.5900, 0.7900	0.5000, 0.7100, 0.8900	0.4600, 0.6700, 0.8600	0.5200, 0.7400, 0.9200
S22	0.5200, 0.7400, 0.9200	0.2000, 0.4700, 0.7700	0.4600, 0.6700, 0.8600	0.4700, 0.6800, 0.8800	0.4600, 0.6800, 0.8800	0.5400, 0.7500, 0.9200
S23	0.6000, 0.8100, 1.0000	0.4200, 0.6900, 0.9900	0.4600, 0.6700, 0.8600	0.6100, 0.8200, 0.9800	0.5200, 0.7400, 0.9200	0.5900, 0.8000, 0.9700

(Continued)

Table 15 (continued)

	HISS-1	HISS-2	HISS-3	HISS-4	HISS-5	HISS-6
S31	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	0.4600, 0.6700, 0.8600
S32	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	0.5400, 0.7500, 0.9200
S33	0.4600, 0.6700, 0.8600	0.3900, 0.5900, 0.7900	0.3900, 0.5900, 0.7900	0.5000, 0.7100, 0.8900	0.4600, 0.6700, 0.8600	0.5200, 0.7400, 0.9200
S41	0.5200, 0.7400, 0.9200	0.2000, 0.4700, 0.7700	0.4600, 0.6700, 0.8600	0.4700, 0.6800, 0.8800	0.4600, 0.6800, 0.8800	0.5400, 0.7500, 0.9200
S42	0.6000, 0.8100, 1.0000	0.4200, 0.6900, 0.9900	0.4600, 0.6700, 0.8600	0.6100, 0.8200, 0.9800	0.5200, 0.7400, 0.9200	0.5900, 0.8000, 0.9700
S51	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	0.4600, 0.6700, 0.8600
S52	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	0.5400, 0.7500, 0.9200

Table 16: The weighted normalized fuzzy-decision matrix

	HISS-1	HISS-2	HISS-3	HISS-4	HISS-5	HISS-6
S11	0.0020, 0.0070, 0.0240	0.0020, 0.0080, 0.0270	0.0020, 0.0080, 0.0250	0.0020, 0.0080, 0.0250	0.0020, 0.0070, 0.0270	0.0020, 0.0060, 0.0200
S12	0.0020, 0.0070, 0.0240	0.0010, 0.0050, 0.0180	0.0020, 0.0070, 0.0220	0.0020, 0.0070, 0.0220	0.0020, 0.0070, 0.0240	0.0030, 0.0120, 0.0420
S21	0.0020, 0.0080, 0.0250	0.0010, 0.0060, 0.0190	0.0020, 0.0070, 0.0240	0.0020, 0.0060, 0.0200	0.0020, 0.0070, 0.0240	0.0020, 0.0080, 0.0250
S22	0.0020, 0.0070, 0.0220	0.0020, 0.0080, 0.0270	0.0020, 0.0070, 0.0240	0.0020, 0.0080, 0.0250	0.0020, 0.0080, 0.0250	0.0020, 0.0080, 0.0250
S23	0.0030, 0.0120, 0.0420	0.0020, 0.0100, 0.0370	0.0020, 0.0080, 0.0250	0.0020, 0.0100, 0.0390	0.0020, 0.0070, 0.0220	0.0020, 0.0070, 0.0240
S31	0.0020, 0.0060, 0.0200	0.0010, 0.0050, 0.0190	0.0020, 0.0070, 0.0220	0.0010, 0.0040, 0.0170	0.0030, 0.0120, 0.0420	0.0020, 0.0080, 0.0250
S32	0.0030, 0.0120, 0.0420	0.0020, 0.0100, 0.0370	0.0030, 0.0120, 0.0420	0.0020, 0.0100, 0.0390	0.0020, 0.0060, 0.0200	0.0020, 0.0070, 0.0220
S33	0.0020, 0.0080, 0.0250	0.0020, 0.0070, 0.0270	0.0020, 0.0060, 0.0200	0.0000, 0.0040, 0.0170	0.0030, 0.0120, 0.0420	0.0030, 0.0120, 0.0420
S41	0.0010, 0.0050, 0.0180	0.0010, 0.0050, 0.0180	0.0030, 0.0120, 0.0420	0.0010, 0.0040, 0.0170	0.0020, 0.0080, 0.0250	0.0020, 0.0060, 0.0200
S42	0.0010, 0.0050, 0.0180	0.0020, 0.0060, 0.0200	0.0020, 0.0080, 0.0250	0.0020, 0.0100, 0.0390	0.0010, 0.0050, 0.0180	0.0030, 0.0120 0.0420

(Continued)

Table 16 (continued)

	HISS-1	HISS-2	HISS-3	HISS-4	HISS-5	HISS-6
S51	0.0020, 0.0070, 0.0250	0.0030, 0.0120, 0.0420	0.0010, 0.0050, 0.0180	0.0000, 0.0040, 0.0170	0.0300, 0.0120, 0.0420	0.0020, 0.0080, 0.0250
S52	0.0010, 0.0050, 0.0180	0.0020, 0.0080, 0.0250	0.0020, 0.0070, 0.0220	0.0020, 0.0070, 0.0240	0.0020, 0.0080, 0.0250	0.0010, 0.0050, 0.0180

Table 17: Closeness coefficients to the aspired level among the different alternatives

Alternatives	$dist^{+i}$	$dist^{-i}$	Gap degree of CC^{+i}	Satisfaction degree of CC^{-i}	Rank of alternatives
HISS-1	0.05500	0.03700	0.365500	0.625000	2
HISS-2	0.06500	0.03500	0.524600	0.644400	1
HISS-3	0.04700	0.05490	0.569900	0.444000	5
HISS-4	0.04500	0.03660	0.256200	0.527000	3
HISS-5	0.45130	0.05500	0.565700	0.467000	4
HISS-6	0.04520	0.05500	0.612600	0.388000	6

Table 18: Variations in results

Experiments	Weights/ Alternatives		HISS-1	HISS-2	HISS-3	HISS-4	HISS-5	HISS-6
	Original Weights	Satisfaction Degree (CC-i)	0.625000	0.644400	0.444000	0.527000	0.467000	0.388000
Expt-1	S11		0.540400	0.377900	0.418000	0.359700	0.383800	0.329100
Expt-2	S12		0.555500	0.363600	0.383800	0.329100	0.417800	0.360700
Expt-3	S21		0.591000	0.398100	0.417800	0.360700	0.383800	0.329100
Expt-4	S22		0.647300	0.434700	0.454800	0.397200	0.543400	0.478100
Expt-5	S23		0.726500	0.527600	0.543400	0.478100	0.534900	0.477700
Expt-6	S31		0.710000	0.520100	0.534900	0.477700	0.385600	0.328000
Expt-7	S32		0.591000	0.398100	0.417800	0.360700	0.383800	0.329100
Expt-8	S33		0.647300	0.434700	0.454800	0.397200	0.543400	0.478100
Expt-9	S41		0.726500	0.527600	0.543400	0.478100	0.534900	0.477700
Expt-10	S42		0.710000	0.520100	0.534900	0.477700	0.385600	0.328000
Expt-11	S51		0.591000	0.398100	0.417800	0.360700	0.383800	0.329100
Expt-12	S52		0.555500	0.363600	0.383800	0.329100	0.382900	0.321700

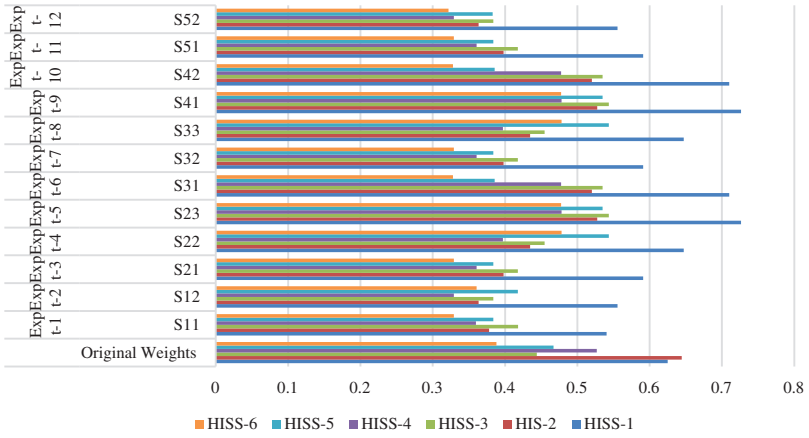

Figure 7: Sensitivity analysis of six alternatives

The graphical representation of sensitivity experiments is depicted in Fig. 7. Further, the weights of the attributes are represented as original weights in the same table. Twelve experiments have been carried out from Experiment.1 to Experiment.7. After calculating the satisfaction degree of each experiment, the final results are depicted in the Tab. 18. Moreover, the validation process is done objectively with the help of [24–26]. From the outcomes of sensitivity analysis, statistical analysis has been conducted to assure the outcomes. In this research work, authors have adopted the validation process [27–29] to calculate the statistical mean (x). The mean (x) is calculated for each experiment, and X is the average of the sample and determined as the sum of all observed results divided by the total number presented in Eq. (1) as follows:

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{1}$$

With the help of Eq. (1) and [27–29], the alternative HISS-1 gains the highest value in Exp.0, and HISS-2 gains the highest value in all other experiments. Further, HISS-6 for 0, Exp.1, Exp.3, Exp.5, Exp.6, Exp.7, Exp.9, Exp.10, Exp.11, Exp.12 and HISS-4 for Exp.2, Exp.4, Exp.8, respectively got the lowest values. According to analysis, result variation shows that the alternative rating is sensitive to the weights.

5 Comparison Between Fuzzy and Classical Based Methods

Problem domains where we are not able to decide whether the solution of the specified problem is completely true or completely false come under the ambit of MCDM problems. Efforts to derive solutions for these problems without considering their imprecision will produce inefficient results. To find efficient and effective results for these problems, Fuzzy-logic has a significant importance. It has the ability to address uncertainty that is present in the problem information [22–25] and can generate solutions of the problem in more than two possibilities. That can be in the form of 0, 0.1, 0.2, …, 0.9, 1 or can be completely true, completely false, partially true, or partially false. Therefore, to make Classical AHP or TOPSIS more efficient and powerful while addressing MCDM problems, we have to integrate fuzzy logic with it.

In this context, we have also provided a comparative study of both the classical and fuzzy based approach. From the analysis of different research studies, it has been found that applying different methods on the same data shows variations in the final results. This implies that a comparative study will be beneficial for achieving more reliable results [4,16–19]. Thus, the accuracy of results has been checked by researchers through the implementation of different techniques [6,22–26]. Authors of this

work have also checked the result's accuracy by applying AHP-TOPSIS integrated with fuzzy logic. Fuzzification and defuzzification of fuzzy logic changes the accuracy of results in F-AHP TOPSIS while comparing with classical AHP-TOPSIS. Thus, fuzzy based approach needs conversion from numeric to TFN values. The comparative results of this work are presented in the Tab. 19 and Fig. 8 with comparative values corresponding to each alternative (HISS-1 to HISS-6) under Classical and fuzzy based approach of AHP-TOPSIS.

Table 19: Comparison the results of classical and fuzzy AHP-TOPSIS methods

Methods/Alternatives	HISS-1	HISS-2	HISS-3	HISS-4	HISS-5	HISS-6
Fuzzy-AHP-TOPSIS	0.625000	0.644400	0.444000	0.527000	0.467000	0.388000
Classical-AHP-TOPSIS	0.614400	0.655400	0.445400	0.545100	0.452300	0.385400

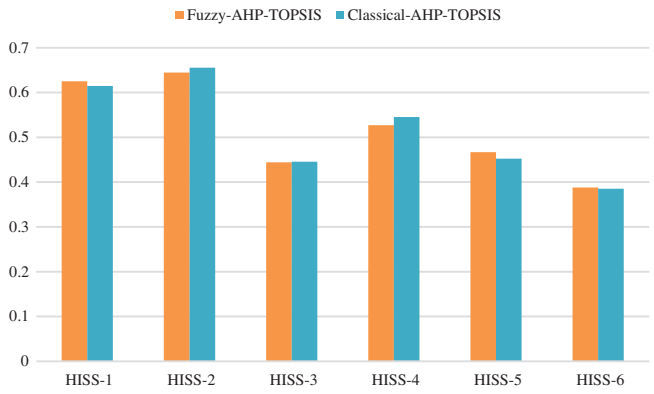

Figure 8: Comparative results of classical and fuzzy based AHP techniques

According to Tab. 19 and Fig. 8, AHP-TOPSIS generated results have got significant correlation (Pearson correlation coefficient is 0.92316) with classical approach results. AHP-TOPSIS integrated with fuzzy logic improved the efficiency in comparison of classical AHP TOPSIS. Fig. 8 depicts the graphical representation of the comparative results.

6 Conclusions

The proposed development is a solution to the problem that every healthcare information management system faces during the threat and attack situation. The development gives an ability to the system for manage its usability as same as before the attack by implementing various processes and steps.

Specifically, whenever a system gets attacked or breached by any attacker they temper and manipulate the internal functionality according to their comfort as an initial step. However, it is challenging to manage the same internal functionality and configuration after or during the remedy or prevention of attack. It is a challenging situation or issue that creates various serious issues and every healthcare information security expert tackle this situation with their specific process. This type of situation also creates a standard-less functionality situation in infrastructure.

Moreover, to manage and provide them a well-established and tested process for adaptation the proposed development gives a step wise workflow model that associate various steps that help the organization into pick a proper systematic pathway for systematic development. The problem that causes these issues is

present in system for a long period of time sometimes. In this scenario a systematic phase wise model is immense need to the field for better development and management. By focusing on this type of need analyzed by authors of this development they prepare a simple, easy but effective workflow model that gives a pathway to the existing healthcare experts in managing this type of situation. The proposed creation associate steps that effectively manage healthcare information system.

Moreover, in we talk about the steps associated n this development then for portraying an effective start to the healthcare information system security towards usability management the prosed model associate three phase snake model which produce the secure healthcare information management system. The three steps that are associated in model are learn; analyze and manage.

Furthermore, as an advantage of this development authors can say that the proposed model can help the healthcare information management systems in managing their usability during or after the attack situation. It has potential to increase the resilience of information systems that is very effective and good for systems. The proposed development provides step wise identification, remedy and management working order that is effective and systematic for a healthcare information management system. The proposed development has a potential to minimize the usability issue of healthcare information systems and maximize the user friendly use of systems in healthcare field which is very beneficial for organizations and healthcare field.

Acknowledgement: The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code: (20UQU0066DSR). This project was supported by Taif University Researchers Supporting Project number (TURSP-2020/107), Taif University, Taif, Saudi Arabia.

Funding Statement: Taif University Researchers Supporting Project (TURSP), Taif University, Kingdom of Saudi Arabia under the grant number: TURSP-2020/107.

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

References

[1] J. Williams, "Social networking applications in health care: threats to the privacy and security of health information," in *Proc. of the ICSE Workshop on Software Engineering in Health Care*, Cape Town, South Africa, pp. 39–49, 2010.

[2] K. Sahu, F. A. Alzahrani, R. K. Srivastava and R. Kumar, "Hesitant fuzzy sets based symmetrical model of decision-making for estimating the durability of web application," *Symmetry*, vol. 12, no. 6, pp. 1770–1792, 2020.

[3] A. Attaallah, M. Ahmad, M. Tarique, A. K. Pandey, R. Kumar *et al.*, "Device security assessment of internet of healthcare things," *Intelligent Automation & Soft Computing*, vol. 27, no. 2, pp. 593–603, 2021.

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

[5] F. A. Alzahrani, M. Ahmad, M. Nadeem, R. Kumar and R. A. Khan, "Integrity assessment of medical devices for improving hospital services," *Computers, Materials & Continua*, vol. 67, no. 3, pp. 3619–3633, 2021.

[6] W. Alosaimi, R. Kumar, A. Alharbi, H. Alyami, A. Agrawal *et al.*, "Computational technique for effectiveness of treatments used in curing sars-cov-2," *Intelligent Automation & Soft Computing*, vol. 28, no. 3, pp. 617–628, 2021.

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

[8] K. Sahu, F. A. Alzahrani, R. K. Srivastava and R. Kumar, "Evaluating the impact of prediction techniques: Software reliability perspective," *computers*," *Materials & Continua*, vol. 67, no. 2, pp. 1471–1488, 2021.

[9] R. Kumar, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal *et al.*, "An integrated approach of fuzzy logic, AHP and TOPSIS for estimating usable-security of web applications," *IEEE Access*, vol. 8, no. 8, pp. 50944–50957, 2020.

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

[11] R. Kumar, S. A. Khan and R. A. Khan, "Secure serviceability of software: Durability perspective," *Communications in Computer and Information Science*, vol. 628, pp. 104–110, 2016.

[12] R. Kumar, S. A. Khan and R. A. Khan, "Durability challenges in software engineering," *CrossTalk*, vol. 42, no. 4, pp. 29–31, 2016.

[13] R. Kumar, M. T. J. Ansari, A. Baz, H. Alhakami, A. Agrawal *et al.*, "A multi-perspective benchmarking framework for estimating usable-security of hospital management system software based on fuzzy logic, ANP and TOPSIS methods," *KSII Transactions on Internet and Information Systems*, vol. 15, no. 1, pp. 240–263, 2021.

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

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

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

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

[18] W. Alosaimi, A. Alharbi, H. Alyami, M. Ahmad, A. K. Pandey *et al.*, "Impact of tools and techniques for securing consultancy services," *Computer Systems Science and Engineering*, vol. 37, no. 3, pp. 347–360, 2021.

[19] R. Kumar, S. A. Khan and R. A. Khan, "Durable security in software development: Needs and importance," *CSI Communications*, vol. 10, no. 10, pp. 34–36, 2015.

[20] R. Kumar, S. A. Khan and R. A. Khan, "Revisiting software security risks," *Journal of Advances in Mathematics and Computer Science*, vol. 11, no. 6, pp. 1–10, 2015.

[21] K. Sahu and R. K. Srivastava, "Revisiting software reliability," *Advances in Intelligent Systems and Computing*, vol. 802, pp. 221–235, 2019..

[22] R. Kumar, S. A. Khan and R. A. Khan, "Analytical network process for software security: A design perspective," *CSI Transactions on ICT*, vol. 4, no. 2, pp. 255–258, 2016.

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

[24] K. Sahu and R. K. Srivastava, "Predicting software bugs of newly and large datasets through a unified neuro-fuzzy approach: Reliability perspective," *Advances in Mathematics: Scientific Journal*, vol. 10, no. 1, pp. 543–555, 2021.

[25] R. Kumar, S. A. Khan and R. A. Khan, "Software security testing: A pertinent framework," *Journal of Global Research in Computer Science*, vol. 5, no. 3, pp. 23–27, 2014.

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

[27] M. T. J. Ansari, A. Baz, H. Alhakami, W. Alhakami, R. Kumar *et al.*, "P-STORE: Extension of store methodology to elicit privacy requirements," *Arabian Journal for Science and Engineering*, vol. 46, no. 3, pp. 8287–8310, 2021.

[28] R. Kumar, A. Baz, H. Alhakami, W. Alhakami, A. Agrawal *et al.*, "A hybrid fuzzy rule-based multi-criteria framework for sustainable-security assessment of web application, *Ain Shams Engineering Journal*, vol. 12, no. 2, pp. 2227–2240, 2021.

[29] R. M. Rodríguez, L. Martínez, V. Torra, Z. S. Xu and F. Herrera, "Hesitant fuzzy sets: State of the art and future directions," *International Journal of Intelligent Systems*, vol. 29, no. 6, pp. 495–524, 2019.