A Multi-Perspective Benchmarking Framework for Estimating Usable-Security of Hospital Management System Software Based on Fuzzy Logic, ANP and TOPSIS Methods

Rajeev Kumar[1,2], Md Tarique Jamal Ansari[3], Abdullah Baz[4], Hosam Alhakami[5], Alka Agrawal[1*], and Raees Ahmad Khan[1]

[1]Department of Information Technology, Babasaheb Bhimrao Ambedkar University
Lucknow, 226025, Uttar Pradesh, India
[e-mail: rs0414@gmail.com, alka_csjmu@yahoo.co.in, khanraees@yahoo.com]
[2]Department of Computer Application, Shri Ramswaroop Memorial University
Lucknow-Deva Road, Barabanki, 225003, Uttar Pradesh, India
[3]Department of Computer Application, Integral University
Lucknow, 226026, Uttar Pradesh, India,
[e-mail: tjtjansari@gmail.com]
[4]Department of Computer Engineering, College of Computer and Information Systems
Umm Al-Qura University, Makkah, Saudi Arabia
[e-mail: aobaz01@uqu.edu.sa]
[5]Department of Computer Science, College of Computer and Information Systems
Umm Al-Qura University, Makkah, Saudi Arabia
[e-mail: hhhakam@uqu.edu.sa]
[*]Corresponding author: Alka Agrawal

Received November 3, 2019; revised July 21, 2020; accepted November 5, 2020; published January 31, 2021

Abstract

One of the biggest challenges that the software industry is facing today is to create highly efficient applications without affecting the quality of healthcare system software. The demand for the provision of software with high quality protection has seen a rapid increase in the software business market. Moreover, it is worthless to offer extremely user-friendly software applications with no ideal security. Therefore a need to find optimal solutions and bridge the difference between accessibility and protection by offering accessible software services for defense has become an imminent prerequisite. Several research endeavours on usable security assessments have been performed to fill the gap between functionality and security. In this context, several Multi-Criteria Decision Making (MCDM) approaches have been implemented on different usability and security attributes so as to assess the usable-security of software systems. However, only a few specific studies are based on using the integrated approach of fuzzy Analytic Network Process (FANP) and Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) technique for assessing the significant usable-security of hospital management software. Therefore, in this research study, the authors have employed an integrated methodology of fuzzy logic, ANP and TOPSIS to estimate the usable – security of

Hospital Management System Software. For the intended objective, the study has taken into account 5 usable-security factors at first tier and 16 sub-factors at second tier with 6 hospital management system softwares as alternative solutions. To measure the weights of parameters and their relation with each other, Fuzzy ANP is implemented. Thereafter, Fuzzy TOPSIS methodology was employed and the rating of alternatives was calculated on the foundation of the proximity to the positive ideal solution.

Keywords: Hospital Management System, Security Assessment, Usable-Security, Fuzzy-ANP, Fuzzy-TOPSIS

1. Introduction

Nowadays, the modern culture, financial system, and vital infrastructure are increasingly reliant on software and knowledge networks systems of Engineering. However, the unprecedented increase in availing the benefits of information technology has also seen an appalling growth in cybersecurity threats which are potentially more devastating. Inadequecy in the usable-security services of software today is the reason behind the rapid growth of data breaches. The extensive usage of information and communication technology (ICT) depicts that the users and organizations today need an enormous amount of physical as well as electronic data assets. But, these assets are at great risk in the wake of cyber invasions. In the context of healthcare, digital healthcare technologies have changed almost every healthcare process by making it more appropriate, efficient and less expensive. The main objective and function of the integration of information technology in healthcare is to ensure that the digital health records are available to many interested parties. In healthcare organizations, safety is more important than ever. Healthcare programs need to capture several forms of identification about their patients, comprising their names, family background, date and place of birth, security numbers, account statements, and also their present situation and illnesses. Any mixture of such pieces of data may be of great benefit to an attacker and would be extremely damaging to the patient. Digital health security is so important that significant implementations require protection to be a part of the solution with accessibility, usability, and compatibility [1].

As per the report published by the HIPAA Journal, there were 3,054 data security breaches in the healthcare sector that included over 500 confidential records from 2009 and 2019. All these violations triggered the damage, fraud, exposed or illegal disclosure of 230,954,151 data in healthcare industry. This is equivalent to more than 69.78 % of the overall population of the USA. Infringements, security breaches in healthcare records were reported at a frequency of 1.4 each day in the year 2019 [2]. The following **Fig. 1** shows the graphical representation of this report.

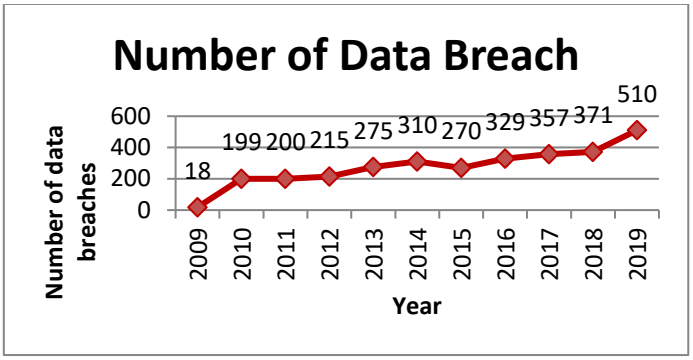


Fig. 1. Healthcare data breaches by year

The medical industry experiences the largest amount of breaches especially in comparison to the other industry sectors as per the Verizon's 2018 report. The report notes that there is a difference between the protection measures available and usability-safety. Usable-security ensures that it should be easily and effectively utilised by everyone who requires a security service. Security aims to prevent unauthorization, whereas usability relates to the ease with which users "*maintain simple*" consumer method. Strong usable security mechanisms can only be implemented effectively if the users can conceptualize the implementation of security in an adaptive manner. Hence, achieving the objective of maintaining a software with efficacious risk management that is easy to enforce and validate, without using a highly complex and technological process, has become a formidable challenge for the developers in the present scenario. Usability-security must be the major consideration of developers and software professionals therefore they must concentrate on how to sucessfully achieve this. To accomplish this objective, many authors have developed and incorporated different types of methods to calculate usable-security [3] and numerous research has been done on efficiently ranking the usability and security elements of the software product. Despite the challenges in this domain, only a few research studies have concentrated on prioritizing usable-security factors with potential application to complex challenges in order to enhance the significant usable-security of web based applications such as Hospital Management System Software (HMSS) solutions. The software application customer's biggest concern is the usable-security service. Operating to enhance the capabilities of usable security would therefore enhance the acceptability of the software and add to the users' satisfaction [4]. Furthermore, companies have their specific evaluation processes and procedures and because of this usable-security attribute evaluation is a decision-making problem [5]. Hence, the evaluation methodology undertaken in this study would be very useful for experts to recognize the objectives of the attributes and to proceed by making reasonable decisions while sustaining usable-security.

Evaluation process of usable-security factors is not only advantageous for software security measures but also enhances the system's performance. Hence, the authors of this article have used a hybrid Fuzzy ANP-TOPSIS technique to estimate the usable-security. Dr. Lotfi Zadeh of the University of California at Berkeley, in the 1960s, initially designed the conception of fuzzy logic. Dr. Zadeh focused on the issue of learning natural language by machine. Natural language cannot be readily converted into precise 0 and 1 values. This is similar to fuzzy logic like the way logic solves problems and it is merely a particular situation of binary or boolean reasoning [6]. Fuzzy-logic is based on the concept of real thinking, and also addresses the inaccuracy and ambiguity of decision-related issues convincingly. Fuzzy-ANP is imlemented to evaluate the weights of different factors whereas the fuzzy-TOPSIS method is implemented to rank the conceivable alternatives according to their output scores.

The remaining portion of this paper has been categorized into the given components: Unit 2 offers an overview into previous relevant studies; Unit 3 addresses the Usable-security of healthcare-based web application development; Unit 4 explains the methodology that has been used to solve the MCDM problem in this research paper; Unit 5 presents the statistical findings in this research study; Unit 6 deploys discussion of the presented reseach study; and finally, Unit 7 concludes the work.

2. Literature Review

Many steps have been taken by the software organisations to deliver customer-specific services which are both secure and reliable. Software security experts think complexity is needed to develop quality software. A complex protection system however disrupts the program's functionality as customers find it burdensome. Though the clients want maximum protection, they also want ease and convenience. Therefore there is a significant need for estimating the usable-security of security-critical software product. If a software development organization has inefficacious security, no one would ever buy its software product. Numerous studies have already been completed on the usable-security assessment by using different procedures and techniques. Together with fuzzy ANP, TOPSIS as well as fuzzy ANP including TOPSIS strategies, challenges such as multi-criteria decision making (MCDM) have also been solved in various fields of concern. Below are a few of the most recent and relevant research works:

- Alka Agarwal et al. (2019) - This study assessed the usable-security by using multi-level fuzzy AHP technique [3]. The study combined five security criteria as well as four usability criteria and implemented the fuzzy AHP hybrid technique to estimate usable-security. The most significant factor found amongst the nine usable-security factors was the user-error protection. The study concluded that the fuzzy AHP provided more efficient results than AHP.
- Zarour et al. (2020)- This research implemented the combination of two powerful MCDM approaches ANP and fuzzy TOPSIS strategy for selecting the most successful blockchain model in the healthcare industry for safe and optimistic EHRs delivery [7]. They used six main factors with 14 sub-factors to assess the six blockchain models for its features in healthcare sector. In order to measure the weighs of parameters, the Fuzzy Analytical Network (FANP) model was utilized. To identify the impact of alternative strategies, the Fuzzy TOPSIS was utilized by the researchers of this study.
- Bijoyeta Roy and Santanu Kr. Misra (2018) - This research study used fuzzy ANP with TOPSIS approach for the most appropriate software application selection [8]. The four alternative options such as Security, reliability, user friendly, and maintenance were chosen as relevant variables for software selection evaluation process. Fuzzy-ANP was implemented to evaluate the weights of the factors and also to assess the quality of interconnectivity between them. Lastly, the weights of criteria were provided as an input to the TOPSIS method to produce the overall alternative ranking.
- Keon Chul Park et al. (2014) - This research work extracted the most effective and ideal forms of authentication for mobile phone banking service with the help of ANP technique [9]. Authors analyzed three factors (security, convenience and cost) with eleven sub-factors, three sub-networks as well as four alternatives to build the entire network. The outcomes of the study indicated that user identification was the most suitable attribute/factor in the security dimension; OTP was the most suitable in the convenience aspect whereas public key certification was the most relevant in the coastal element. The

study concluded that OTP was the most optimal and effective method of authentication in overall performance in protection, functionality and cost.

- Al-Zahrani (2020) - The author assessed the healthcare software's usability-security. The research also proposed strategies that would allow the development of healthcare applications with maximum security while maintaining their usability on the basis of an empirical review of the detailed statistics [4]. Four attributes such as confidentiality, satisfaction, integrity and availability were considered for usable security evaluation.
- Pranab Biswas et al. (2015)- In this research analysis, the authors used the Neutrosophic aggregation operator to summarize the opinions of the experts, and Euclidean-distance technique to evaluate the ranges of each alternative solution from a positive-ideal solution (PIS) and a negative-ideal solution (NIS). The study's assessment was based on four alternatives as well as six parameters. Ultimately, authors concluded that TOPSIS system with neutrosophic set knowledge had a very strong likelihood of succeeding in solving multi-attribute decision making problems [10].
- Rakesh Ranjan Kumar et al. (2017) devised a model by using Analytic Hierarchy Process as well as fuzzy-TOPSIS approaches for cloud-service selection [11]. For preference selection of the cloud storage service, six alternative solutions and four cost criteria including six benefit criteria were mentioned. The ultimate findings demonstrated that Softlayer was the most workable component of cloud services accompanied by Amazon Web as well as Digital Ocean services.

3. Usable-Security of HMS Software

Since, the data assets of both businesses and groups are at risk, the security of all fields of web-based application software such as Hospital Management System (HMS) software has become the security designers and developers' main priority [11]. However, ensuring security of web application is a daunting task for clinicians because they face multiple challenges like usable security measures. Usable-security involves so many security resources that support the structure of the CIA triad without losing its usability, i.e. simple to comprehend and practice, and also deliver coverage of user inaccuracies [3]. Information-Security defends against malicious attack and unauthorized access, data storage and data management services. The term usability is demarcated by the point to which a specific client may use the system to achieve certain goals with efficiency, effectiveness as well as satisfaction for fulfilling CIA (*confidentiality, integrity and availability*) [12].

For conducting a conclusive and more encompassive estimation of usable-security of Hospital Management System (HMS), we undertook a through perusal of the evaluation techniques of previous research articles in this domain. Based on the reference done by us for the identification and selection of key attributes for usable-security assessment, we adopted 5 factors at Tier 1, and 16 sub - factors at Tier 2 with 6 alternative options for evaluating the efficacy of usable-security of various HMS application. Six separate hospitals in Varanasi, Uttar Pradesh, India were used for hospital management systems applications as alternatives. The HMSS1, HMSS2, HMSS4, HMSS5 and HMSS6 versions appeared. The following **Fig. 2** reflects the attributes of usable security and their mutual dependency. Five factors at Tier 1 for usable security evaluation of HMS Software are defined below:

- Confidentiality: Confidentiality ensures that the valuable personal data is not accessed by unauthorized individuals or procedures, and guarantees that only an authenticated user accesses information or communications network.

- Satisfaction: User satisfaction is consumer experience which is only a part of what attracts or dissatisfies a client. Adopting a comprehensive customer service plan in itself ensures ideal consumer satisfaction. This implies that the goods or services can be used by consumers without any inconvenience, and will meet the customers' needs and expectations.
- Integrity: Integrity is described as "*data protection from intentionally or accidentally unlawful alteration*." It is a responsibility of shielding information and other characteristics from consistency and reliability.
- Availability: The term *Availability* refers to the probability of the web application to operate appropriately, as and when the demand arises. In other terms, availability is the likelihood that when it has to be accessed, a device won't malfunction or experience a complete overhaul.
- Durability: Software durability in computer science refers to the ability of the software to serve solutions and to encounter the requirements of the consumers for a fairly long time. Durability of the program is the key factor in ensuring user satisfaction.

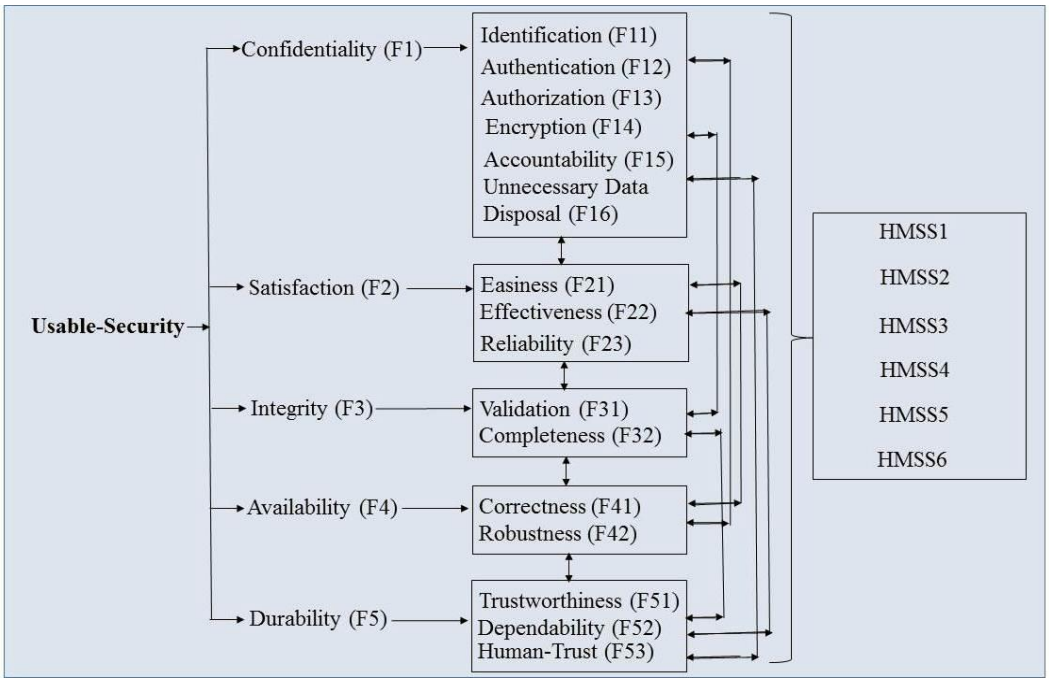


Fig. 2. Usable-Security Attributes

In this paper, we have designed the high-level hierarchy diagram for the proposed MCDM based issue in context of usable security evaluation, which can be seen in **Fig. 2**. According to this diagram, we have identified the total 16 sub-factors at the second Tier of this MCDM based hierarchy. All these sub-factors are sequentially defined in **Table 1**.

Table 1. Different Sub-factors of Usable security

Sub-factor	Description	Reference
Identification	Identification process takes place when a person, system or method assumes an identity (such as with a username). It is interpretation of one's identity where even the user or almost any other element is not recognized. *It describes, who I am in general.*	[3]
Authentication	Authentication is the method of identifying if, in essence, anyone or anything is who or what they claim themselves to be. Authentication technique provides device network access by verifying to see whether passwords are available to a participant or user.	[13, 14]
Authorization	Authorization is a mechanism by which the application's resources are given permissions. In the principle of authentication, it determines the individual's resource control domain.	[13, 14]
Encryption	Encryption is a mechanism by which plaintext or unencrypted data is translated into ciphertext, also called the coded form, to preserve or secure privacy of digital information.	[15]
Accountability	The responsibility of an individual's activities and choices is established by accountability. In other terms, the individuals is responsible for his/her actions; thus attributing accountability.	[14]
Unnecessary Data Disposal	It indicates avoidable data disposal in which data is withdrawn or deleted adequately if the information is no longer needed so that it will not be retrieved back or abused in future.	[1]
Easiness	Easiness represents the situation or quality that is easy to obtain or to do something to accomplish an objective. In other terms, we might conclude that ease is the extent to which we know how easy or user-friendly a service or program is.	[16]
Effectiveness	The extent upon which expectations are met and to what level targeted issues are resolved.	[3]
Reliability	Reliability guarantees efficiency or accuracy of performance with time as needed. ISO defined reliability as "*property of consistent intended behavior and results".*	[14, 17]
Validation	Validation is the test used to determine whether the output of the program is up to standard or, in other terms, the output has stringent expectations. This is the method of testing product validation.	[5]
Completeness	Completeness is the capacity of a monitoring system to show that errors are present. When a system is dismissed, then there are flaws in the system.	[18]

Correctness	From the software engineering point of view, correctness ca n be described as conformity to the requirements that dictate how users are int eracting with the application, as well as how the application will respond when it is used accurately.	[5]
Robustness	Robustness is the capability of a software system to manage failures during performing operation, and also to manage error data.	[3]
Trustworthines s	Trustworthiness is a sort of confirmation that application would therefore perform as anticipated.	[14]
Dependability	Dependability is the capability to deliver products in a time-period which can also assure solid defense. This may also include processes designed to enhance and establish a software product or process's reliability.	[14]
Human Trust	Human trust is a concept used in software engineering and security to define as an agreed dependency on the software application capacity, power, or reality. It is represented as a commitment to rely on the software system on which a person has trust.	[14]

4. Hybrid Methodology

The present study employs the ANP-TOPSIS which is a highly proficient technique of MCMD and is used in several research methods for delivering Usable Security Services in different technological sectors. Fuzzy-ANP has been integrated in the ANP network to measure the weights of the factors and their interconnectedness. Thereafter, TOPSIS is used to classify the replacements. These strategies have been explicated in the subsequent section.

4.1 Fuzzy Logic

The term '*Fuzzy'* refers to things which aren't obvious or ambiguous. Almost always, in real life scenarios also people have conflicting opinions and seldom agree on a certain assertion to be *either right or wrong.* Fuzzy logic addresses such indecisiveness by offering several options between an *absolute true or false*. Fuzzy logic includes several logical values but these values are really an indicator's true values or a concern between 0 and 1. In 1965, Lofti Zadeh developed this conceptualization which is based on the Fuzzy Set Theory. This methodology shows the consequences that cannot be provided by computer systems but are close to the selection of human-generated considerations. Just two choices (0 and 1) occur in the Boolean method, where 1 signifies the exact value of truth and 0 signifies the exact false value. Yet there are several possible scenarios between the 0 and 1 inside the fuzzy method, which can be partially wrong and partially right. Fuzzy logic is a popular and strong mathematical method that is used to tackle and manage uncertain and inaccurate information about decisions shown in **Fig. 3** [19].

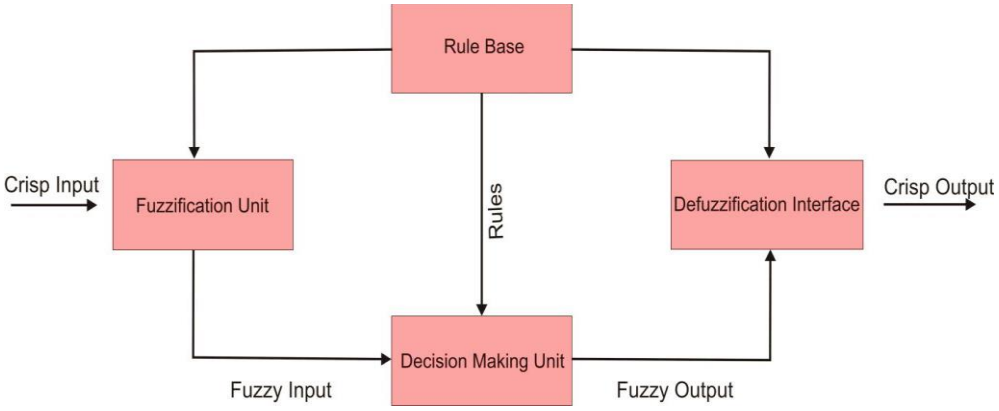


Fig. 3. Basic Block of Fuzzy Logic System

4.2 Analytic Network Process (ANP)

ANP mechanism is a popular structured multi-criteria decision making (MCDM) analysis technique which is used in decision taking challenges to select the optimum solution across all alternative solutions. The ANP is a generalized form of the AHP [20]. T.L. Saaty developed the method of analytical hierarchy [21]. The Analytic hierarchy method assumes that the hierarchical criteria are autonomous, so the potential relations between the criteria are not measured [22]. This was not just an assumption. Therefore, In order to address problems with reliance on parameters or alternatives, Saaty implemented ANP to overcome the constraints in using AHP [13, 22, 23].The Analytical network process is a network structure instead of a hierarchy [20] as it encompasses the interactions and dependency between the major issue factors and assesses its overall impact on the network. The hierarchical structure is substituted by a network structure because of the response approach utilized by ANP.

4.3 TOPSIS Method

The Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) was developed by Hwang & Yoon. It is a procedure for evaluating the effectiveness of alternative solutions with the help of the resemblance with the optimal solution. The TOPSIS approach is the second most prevalent method among MCDM methods. Dozens of researchers have implemented TOPSIS to handle easy and hard issues in various areas to tackle exclusive challenges. TOPSIS procedure 's implementation is an advanced approach. Hence, most of its application scenarios to overcome multiple issues represent the overall trends and developments of all MCDM approaches to solve relatively complex assignments [24]. The strongest ideal solution, as per this technique, would be something which is very close to the positive-ideal solution (PIS), and the furthest from the negative-ideal solution (NIS). The resolution of PIS is one that greatly increases the conditions for profit and reduces the standards for costs. The NIS increases the cost criteria and also greatly reduces the profit conditions [25-28]. In short, this is composed of all highest ratings points achievable of criteria, and the NIS comprises of all the lowest ratings points achievable of criteria. TOPSIS is a value-based method, and therefore its basic principle relates to the distance measured from the NIS as well as the PIS. The technique estimates the ranges with the help of the Euclidean n-dimensional length as per the total count of the issue criteria. The TOPSIS technique can also be easily integrated with other decision-making techniques with multi-criteria to calculate the alternative's performance by using different criteria. The findings are consistent with the TOPSIS and hybrid approach. The

following **Fig. 4** shows the functional flow of hybrid fuzzy ANP-TOPSIS method used in this research study to accomplish the objective.

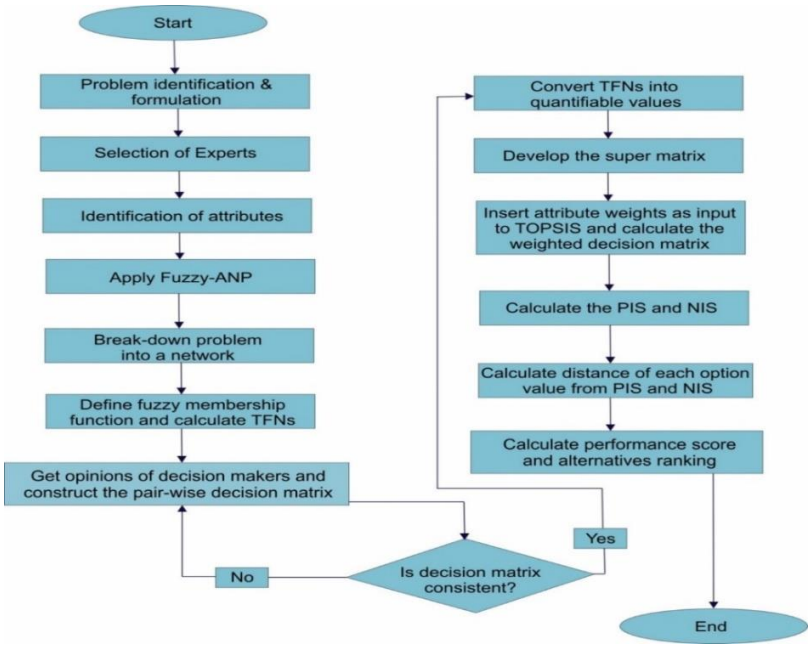


Fig. 4. Functional diagram of the hybrid fuzzy ANP-TOPSIS methodology

4.4 Hybrid Fuzzy-ANP-TOPSIS

In this paper, we have designed a combination of Fuzzy-ANP-TOPSIS technique to get more accurate and comprehensive outcomes. The step-by - step weighting and ratings operation through the support of Fuzzy ANP-TOPSIS has been explained below:

Step1: Researchers transformed the linguistic variables into precise numeric standards, and thereafter, into triangular fuzzy numbers. TFN is considered to act as a component and resides between 0 and 1 [3, 4]. TFN can be represented as (k, l, m), where (k = l = m) and k, l, m are variables implying the lowest, middle, and the highest value in the TFN. Furthermore, if its membership function is provided in (1) and (2), a fuzzy number N on F is designated the Triangular Fuzzy Number (TFN) and that can be seen in **Fig. 5**.

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

$$\mu_A(x) = \begin{cases} \frac{x-k}{l-k}, & k \le x \le l \\ \frac{m-x}{m-s}, & l \le x \le m \\ 0, & x > m \quad Otherwise \end{cases} \tag{2}$$

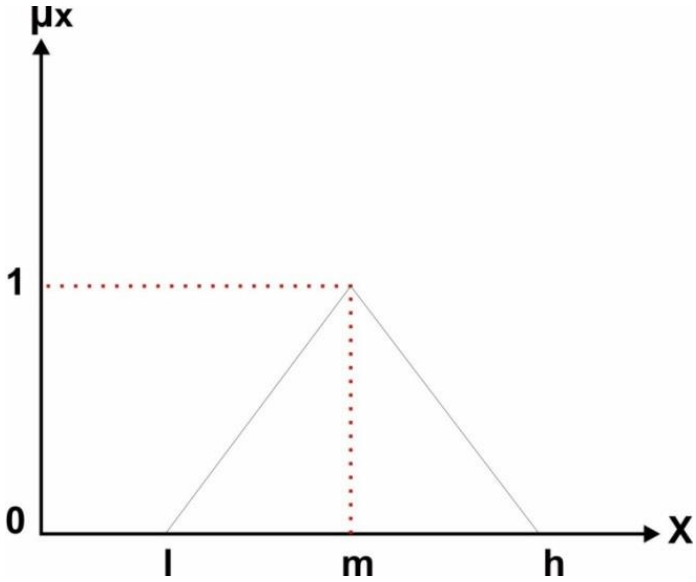


Fig. 5. Triangular Fuzzy Number

Professionals and experts allocated ratings according to the scale as shown in **Fig. 2** to the parameters influencing the values in a quantifiable manner.

Table 2. Linguistic-terms with their equivalent TFNs

Saaty Scale Definition	**Fuzzy Triangle Scale**	
1	Equally significant	(1 ,1, 1)
3	Weakly significant	(2 ,3, 4)
5	Fairly significant	(4 ,5, 6)
7	Strongly significant	(6 ,7, 8)
9	Absolutely significant	(9 ,9, 9)
2 4 6 8	Intermittent values between two adjacent scales	(1 ,2, 3) (3 ,4, 5) (5 ,6, 7) (7 ,8, 9)

Transformation from numerical data to Triangular Fuzzy Number is achieved using (3-6) [26] and represented as (k_{ij}, l_{ij}, m_{ij}) where, k_{ij} denotes lower-value, l_{ij}denotes middle-value and m_{ij}denotes upper-value. Moreover, TFN [ɳij] is defined as following:

$$\eta_{ij} = (k_{ij}, l_{ij}, m_{ij}) \tag{3}$$

where, $k_{ij} \leq l_{ij} \leq m_{ij}$

$$k_{ij} = min(J_{ijd}) \tag{4}$$

$$l_{ij} = (J_{ij1}, J_{ij2}, J_{ij3})^{\frac{1}{x}} \tag{5}$$

$$\text{And } m_{ij} = max(J_{ijd}) \tag{6}$$

Relative significance of the standards amongst two factors is presented by J_{ijk} in the above specified equations; and assumed by experts' or decision makers' choices. At this point, a pair of features is judged by specialists and is characterized by i and j. The evaluation of TFN (η_{ij}) is founded on the geometric mean of specialists' views for a specific comparative assessment. Furthermore, (7) to (9) refer to combined triangular fuzzy number standards. Considering that N1 and N2 are two TFNs, N1= (k_1, l_1, m_1) and N2= (k_2, l_2, m_2), the operating guidelines on them are as follows:

$$(k_1, l_1, m_1) + (k_2, l_2, m_2) = (k_1 + k_2,\ l_1 + l_2,\ m_1 + m_2) \tag{7}$$

$$(k_1, l_1, m_1) \times (k_2, l_2, m_2) = (k_1 * k_2,\ l_1 * l_2,\ m_1 * m_2) \tag{8}$$

$$(k_1, l_1, m_1)^{-1} = (\frac{1}{k_1}, \frac{1}{l_1}, \frac{1}{m_1}) \tag{9}$$

Step2: The matrix for a comparative analysis is constructed in pairs with the responses gathered from the specialists as well as the decision makers. The estimated Consistency Index (CI) in (10) would be:

$$CI = (\gamma_{max} - n)/(n-1) \tag{10}$$

Where, CI: Consistency Index and n: number of compared components.

The statement would be further estimated by the Random Index (RI) for the Consistency Ratio (CR):

$$CR = CI/RI \tag{11}$$

If CR < 0.1 then generated matrix is reasonably consistent.

In this equation, RI expresses random index. Random index is generated from Saaty [29]

Step 3: Through the support of defuzzification procedure, the TFN standards are converted into computable form after accomplishing a properly consistent matrix. The method of defuzzification instigated in this study is derived from [3, 4] as created in (12-14), mostly termed as the *alpha-cut.*

$$\mu_{\alpha,\beta}(\eta_{ij}) = [\beta.\eta\alpha(k_{ij}) + (1-\beta).\eta\alpha(m_{ij})] \tag{12}$$

where, $0 \leq \alpha \leq 1$ and $0 \leq \beta \leq 1$
such that,

$$\eta\alpha(k_{ij}) = (l_{ij} - k_{ij}).\alpha + k_{ij} \tag{13}$$

$$\eta\alpha(m_{ij}) = m_{ij} - (m_{ij} - l_{ij}).\alpha \tag{14}$$

On behalf of the predilection of the specialists, α and β are used in the above equations. Also, α and β values vary between 0 and 1.

Step4: In this phase, the supermatrix is formed which is the consequence of the primary concern matrix from the pair-wise comparison among the groups which include objective, factors, sub-factors, and alternative solutions.

Step5: Assessing TOPSIS involves output rating over any normalized variable in each alternative. The formula for this step is as follows:

$$X_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}} \tag{15}$$

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

The Normalized Weighted-Decision Matrix will then be calculated. This would be done with the help of following equation.

$$D_{ij} = w_i X_{ij} \tag{16}$$

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

Step 6: Assessment of positive-ideal solution (PIS)Z^+ matrix and negative-ideal solution (NIS)Z^-matrix.

$$Z^+ = e_1^+, e_2^+, e_3^+ \ldots\ldots e_n^+$$

$$Z^- = e_1^-, e_2^-, e_3^- \ldots\ldots e_n^- \tag{17}$$

Where, e_j^+ is Max $e_{ij,}$ if j is the benefit factor, and Max $e_{ij,}$ if j is a cost factor; e_{j^-} is Min e_{ij} if $j^{'}$ is benefit factor and Min $e_{ij,}$ if j is a cost factor.

Step 7: Next step is recognizing the range of each value with reference to positive- ideal solution (PIS) and negative-ideal solution (NIS):

Positive ideal solution:

$$w_i^+ = \sqrt{\sum_{j=1}^{m} (e_i^+ - e_{ij})^2} \; ; i = 1,2,3 \ldots . m \tag{18}$$

Negative ideal solution:

$$w_i^- = \sqrt{\sum_{j=1}^{m} (e_{ij} - e_i^-)^2} \; ; \quad where, i = 1,2,3 \ldots . m \tag{19}$$

where s_j^+describes the range to the positive-ideal solution (PIS) for i option. s_i^- is the distance from the negative-ideal solution (NIS). Computing the preference significance for every alternative (E_i)

$$E = \frac{w_i^-}{w_i^- - w_i^+} \tag{20}$$

where, i= 1, 2, 3….m

The above described processes will be accompanied with various alternatives to test accessible- protection by using Fuzzy ANP TOPSIS method. The subsequent section conveys a case study which provides the quantitative evaluation to accomplish usable security.

5. Data Analysis and Results

Measuring quantifiable usable-security is complicated as well as demanding as the usable-security assessment is reasonably a quantifiable entity [3]. Moreover in their efforts to design a more usable system, the developers often abandon the emphasis on fundamentals. Businesses and professionals in the current years have been demanding more powerful software security. Thus, the ranking of usable-security factors throughout software development life cycle plays a major role in creating safe as well as functional software systems. In this league, utilizing hybrid fuzzy-ANP-TOPSIS approach, in this study proved to be a significant usable-security assessment of HMS software. Five parameters at Tier-1 including confidentiality, satisfaction, integrity, availability and durability defined by F1, F2, F3, F4 and F5, correspondingly, were estimated for the determination of usable-security significance. As already defined, the usability-security at tier two, confidentiality elements are expressed as F11, F12, F13, F14, F15, F16, satisfaction elements are represented as F21, F22 and F23, integrity elements as F31, and F32, availability elements as F41, F42 and durability attributes as F51, F52, F53 presented in the following table. Usable-security evaluation incorporating Fuzzy-ANP-TOPSIS was evaluated by using all the equations from (1-20), as described in the following:

With the support of **Table 2** and (1-9), the researchers in this work interpreted the textual-terms into numerical values and afterwards integrated triangular fuzzy numeral values. Again with support of (3-6), the crisp estimated standards were converted into fuzzy TFN. Therefore, the Tier-1 comparative analysis matrixes are computed pair-wise and can be seen in **Table 3**. After which, the consistency index as well as the Random Index (RI) were calculated with the help of (10, 11). For such pair-wise assessments, the random index (RI) of the matrix is below 0.1, where it demonstrates that the matrix is consistent in a pair-wise comparison. For defuzifying a matrix of pair-sided measurement at tier two, the formulation provided in (12-14) has used the alpha cut procedures, with results presented in **Table 4**. Similarly, different other pair-wise matrix comparative assessment matrixes were determined for Tier 2 sub-factors as well as findings were systematically taken from all of these respective matrixes and a weighted super matrix was developed by representing and criteria (attribute) weight with regard to its comparable, as seen in **Table 5**, and attribute rankings are also presented in the same table as per their weight.

Table 3. Fuzzy Pair-wise Comparison Matrix at Tier I

	F1	F2	F3	F4	F5
F1	1.0000,1.0000,1.0000	1.0000, 1.5200, 1.9300	0.4900, 0.6400, 1.0000	0.4200, 0.5700, 1.0000	0.2200, 0.2900, 0.4200
F2	0.5180,0.6570, 1.0000	1.0000,1.0000,1.0000	0.5700, 0.6700 0.8000	0.3100, 0.3900, 0.5600	0.2700, 0.3500, 0.5200
F3	1.0000, 1.5600, 2.0400	1.2500, 1.4900, 1.7500	1.0000,1.0000,1.0000	1.0000, 1.3200, 1.5500	0.3000, 0.4400, 0.8000
F4	1.0000, 1.7500, 2.3800	1.7800, 2.5600, 3.2200	0.6405, 0.7500, 1.0000	1.0000,1.0000,1.0000	0.5400, 0.9100, 1.5800
F5	2.3800, 3.4400, 4.5400	1.9200, 2.8500, 3.7000	1.2500, 2.2700, 3.3300	0.6320, 1.0980, 1.8500	1.0000,1.0000,1.0000

Table 4. Integrated Fuzzy Pair-wise Comparison Matrix at Tier II

	Eigen Vectors	Normalized Fuzzy Weights	Defuzzified Weights
F1	0.2350, 0.2550, 0.2660	0.0760, 0.0870, 0.1080	0.0950
F2	0.5280, 0.5350, 0.5480	0.1700, 0.1800, 0.2230	0.2290
F3	0.4020, 0.4104, 0.4280	0.1300, 0.1400, 0.1740	0.2340
F4	0.2320, 0.2400, 0.2690	0.0750, 0.0800, 0.1090	0.3230
F5	0.2770, 0.2840, 0.2890	0.0510, 0.0570, 0.0640	0.1190

Table 5. Weighted Super Matrix

	Goal	F11	F12	F13	F14	F15	F16	F21	F22	F23	F31	F32	F41	F42	F51	F52	F53
Goal	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
F11	0.1000	0.0000	0.2300	0.2000	0.0000	0.3800	0.5000	0.0000	0.0000	0.0000	0.6000	0.4000	0.0000	0.0000	0.0000	0.0000	0.6000
F12	0.1000	0.2300	0.0000	0.2000	0.0000	0.3900	0.3100	0.0000	0.0000	0.0000	0.2500	0.2500	0.0000	0.0000	0.0000	0.0000	0.2500
F13	0.1000	0.2000	0.2600	0.0000	0.0000	0.0000	0.0000	1.0000	1.0000	0.8200	0.0000	0.2000	0.6900	0.7000	1.0000	0.8200	0.0000
F14	0.0500	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.4000	0.0000	0.0000	0.0000
F15	0.1000	0.2900	0.2400	0.0000	0.0000	0.0000	0.1900	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
F16	0.0000	0.0800	0.0800	0.0700	0.0000	0.2300	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
F21	0.1000	0.0000	0.0000	0.0900	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
F22	0.1000	0.0000	0.0000	0.0800	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
F23	0.0300	0.0000	0.0000	0.0500	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.3100	0.0000	0.0000	0.0000	0.0000
F31	0.0800	0.1400	0.2000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.1500	0.0000	0.0000	0.0000	0.0000	0.0000
F32	0.0600	0.0600	0.0400	0.1200	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.1500	0.0000	0.0000	0.0000	0.0000	0.0000	0.1500
F41	0.0800	0.0000	0.0000	0.1500	0.0000	0.0000	0.0000	0.0000	0.0000	0.1800	0.0000	0.0000	0.0000	0.0000	0.0000	0.1800	0.0000
F42	0.0200	0.0000	0.0000	0.0300	1.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
F51	0.0000	0.0800	0.0800	0.0700	0.0000	0.2300	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
F52	0.1000	0.0000	0.0000	0.0900	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
F53	0.1000	0.0000	0.0000	0.0800	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000

After collecting the weights of variables with the support of Fuzzy-ANP procedure, TOPSIS system demonstrates the weights of variables as input as well as provides ranking for each alternative solutions. TOPSIS requires performance rating over any standardized variable in each alternative choice; for this kind of (15) is being used standardized decision-matrix is developed for m requirements and n alternatives, as well as its final production outcomes are presented in **Table 6**. Therefore, each standardized decision-matrix cell quantity is generally regarded as the normalized presentation value and is multiplied by weights of each set of criteria and a fuzzy weighted standardized decision-matrix was calculated using (16) and also its actual output findings are presented in **Table 7**. Next, the PIS (positive-ideal solution) Z+ matrix and NIS (negative-ideal solution) Z- matrix are calculated with the help of (17) to evaluate PIS and NIS, as well as findings are described in **Table 8**. Afterwards, the range from the PIS matrix as well as NIS matrix of the each option value is determined by applying formula 18 and 19, and outcome data represented in **Table 9**. Ultimately, the success score of parameter was determined by using (20), and the ratings of the alternatives' was calculated based on the estimated performance rating, as seen in **Table 10** and **Fig. 6**. Alternatives are

ranked as: *HMSS1*, *HMSS4*, *HMSS2*, *HMSS3*, *HMSS6*, *and HMSS5*, respectively. HMSS1 is considered to deliver the best usability-security, while the HMSS5 is found to be the worst.

Table 6. Weights of Criteria

First Tier Factors	Second Tier Factors	Local Weights	Final Weights	Percentage	Rank
F1	F11	0.1040	0.0110	1.10 %	16
	F12	0.0750	0.0070	7.00 %	6
	F13	0.1590	0.0150	1.50 %	15
	F14	0.1850	0.0180	1.80 %	14
	F15	0.2370	0.0230	2.30 %	11
	F16	0.2410	0.0230	2.30 %	12
F2	F21	0.1830	0.0420	4.20 %	10
	F22	0.2240	0.0520	5.20 %	7
	F23	0.5930	0.1360	13.60 %	3
F3	F31	0.3120	0.0730	7.30 %	5
	F32	0.6880	0.1610	16.10 %	2
F4	F41	0.3840	0.1240	12.40 %	4
	F42	0.6160	0.1990	19.90 %	1
F5	F51	0.3610	0.0430	4.30 %	9
	F52	0.3870	0.0460	4.60 %	8
	F53	0.2520	0.0230	2.30 %	13

Table 7. Fuzzy decision matrix of alternatives with respect to usable-security

	HMSS-1	HMSS-2	HMSS-3	HMSS-4	HMSS-5	HMSS-6
F11	5.1200, 7.1400, 8.7200	3.1500, 5.1500, 6.9100	2.8200, 4.6400, 6.6400	1.5500, 3.1800, 5.1800	1.4500, 3.1800, 5.1800	2.4500, 4.2700, 6.2700
F12	4.2800, 6.3700, 8.3700	2.4500, 4.4500, 6.4500	2.9100, 4.6400, 6.5500	1.4500, 3.0000, 4.9100	1.1800, 2.8200, 4.8200	2.0900, 3.7300, 5.7300
F13	4.2700, 6.2700, 8.1400	2.8200, 4.8200, 6.8200	3.1800, 5.1800, 7.1000	1.4500, 3.0700, 4.9100	0.8200, 2.2700, 4.2070	3.0000, 4.8200, 6.8200
F14	5.3600, 7.3600, 9.1200	3.7300, 5.7300, 7.5500	2.4500, 4.4500, 6.4500	0.9100, 2.4500, 4.4500	2.4500, 4.2700, 6.2700	3.9100, 5.9100, 7.8020
F15	4.6400, 6.6400, 8.5500	3.0000, 5.0000, 7.1400	2.1800, 4.0900, 6.1400	2.8200, 4.6400, 6.6400	1.9010, 3.7030, 5.7300	2.5500, 4.4500, 6.4500
F16	3.1200, 5.0000, 7.1400	2.4500, 4.4500, 6.4500	3.5500, 5.5500, 7.4500	1.8200, 3.7300, 5.7300	1.6400, 3.5500, 5.5500	3.9100, 5.9100, 7.9100
F21	5.3600, 7.3600, 9.0900	2.6400, 4.6400, 6.6400	2.9000, 4.8000, 6.7000	2.8200, 4.6400, 6.6400	2.5500, 4.4500, 6.4500	3.1800, 5.1800, 7.0900
F22	5.1200, 7.1400, 8.7200	3.1500, 5.1500, 6.9100	2.8200, 4.6400, 6.6400	1.5500, 3.1800, 5.1800	1.4500, 3.1800, 5.1800	2.4500, 4.2700, 6.2700
F23	4.2800, 6.3700, 8.3700	2.4500, 4.4500, 6.4500	2.9100, 4.6400, 6.5500	1.4500, 3.0000, 4.9100	1.1800, 2.8200, 4.8200	2.0900, 3.7300, 5.7300
F31	4.2700, 6.2700, 8.1400	2.8200, 4.8200, 6.8200	3.1800, 5.1800, 7.1000	1.4500, 3.0700, 4.9100	0.8200, 2.2700, 4.2070	3.0000, 4.8200, 6.8200
F32	5.3600, 7.3600, 9.1200	3.7300, 5.7300, 7.5500	2.4500, 4.4500, 6.4500	0.9100, 2.4500, 4.4500	2.4500, 4.2700, 6.2700	3.9100, 5.9100, 7.8020
F41	4.6400, 6.6400, 8.5500	3.0000, 5.0000, 7.1400	2.1800, 4.0900, 6.1400	2.8200, 4.6400, 6.6400	1.9010, 3.7030, 5.7300	2.5500, 4.4500, 6.4500
F42	3.1200, 5.0000, 7.1400	2.4500, 4.4500, 6.4500	3.5500, 5.5500, 7.4500	1.8200, 3.7300, 5.7300	1.6400, 3.5500, 5.5500	3.9100, 5.9100, 7.9100
F51	5.3600, 7.3600, 9.0900	2.6400, 4.6400, 6.6400	2.9000, 4.8000, 6.7000	2.8200, 4.6400, 6.6400	2.5500, 4.4500, 6.4500	3.1800, 5.1800, 7.0900
F52	5.1200, 7.1400, 8.7200	3.1500, 5.1500, 6.9100	2.8200, 4.6400, 6.6400	1.5500, 3.1800, 5.1800	1.4500, 3.1800, 5.1800	2.4500, 4.2700, 6.2700
F53	4.2800, 6.3700, 8.3700	2.4500, 4.4500, 6.4500	2.9100, 4.6400, 6.5500	1.4500, 3.0000, 4.9100	1.1800, 2.8200, 4.8200	2.0900, 3.7300, 5.7300

Table 8. Fuzzy positive and negative ideal solutions

	Fuzzy Positive Ideal Solution (FPIS)	Fuzzy Negative Ideal Solution (FNIS)
F11	0.0113, 0.0131, 0.0152	0.0061, 0.0080, 0.0100
F12	0.0124, 0.0121, 0.0132	0.0052, 0.0060, 0.0070
F13	0.0132, 0.0147, 0.0170	0.0084, 0.0110, 0.0130
F14	0.0454, 0.0577, 0.0690	0.0224, 0.0290, 0.0360
F15	0.0932, 0.1092, 0.1251	0.0414, 0.0570, 0.0690
F16	0.0512, 0.0612, 0.0730	0.0263, 0.0370, 0.0480
F21	0.0113, 0.0131, 0.0152	0.0061, 0.0080, 0.0100
F22	0.0124, 0.0121, 0.0132	0.0052, 0.0060, 0.0070
F23	0.0132, 0.0147, 0.0170	0.0084, 0.0110, 0.0130
F31	0.0454, 0.0577, 0.0690	0.0224, 0.0290, 0.0360
F32	0.0371, 0.0440, 0.0520	0.0221, 0.0300, 0.0380
F41	0.0512, 0.0612, 0.0730	0.0263, 0.0370, 0.0480
F42	0.0113, 0.0131, 0.0152	0.0061, 0.0080, 0.0100
F51	0.0124, 0.0121, 0.0132	0.0052, 0.0060, 0.0070
F52	0.0132, 0.0147, 0.0170	0.0084, 0.0110, 0.0130
F53	0.0454, 0.0577, 0.0690	0.0224, 0.0290, 0.0360

Table 9. Distance between alternatives and ideal solutions

	Positive						Negative					
	HMSS-1	HMSS-2	HMSS-3	HMSS-4	HMSS-5	HMSS-6	HMSS-1	HMSS-2	HMSS-3	HMSS-4	HMSS-5	HMSS-6
d11	0.0000	0.0344	0.0429	0.0035	0.0743	0.0604	0.2313	0.2044	0.2010	0.2289	0.1812	0.1892
d12	0.0000	0.0271	0.0349	0.0185	0.0664	0.0627	0.1878	0.1719	0.1617	0.1737	0.1424	0.1438
d13	0.0151	0.0299	0.0191	0.0003	0.0491	0.0457	0.1677	0.1616	0.1642	0.1779	0.1456	0.1474
d14	0.0074	0.0027	0.0003	0.0004	0.0006	0.0004	0.0032	0.0032	0.0031	0.0033	0.0029	0.0028
d15	0.0000	0.0284	0.0288	0.0138	0.0493	0.0521	0.1202	0.0998	0.0980	0.1091	0.0804	0.0826
d16	0.0068	0.0071	0.0154	0.0008	0.0154	0.0245	0.0680	0.0701	0.0619	0.0732	0.0619	0.0566
d21	0.0000	0.0017	0.0028	0.0009	0.0045	0.0035	0.0156	0.0148	0.0136	0.0154	0.0126	0.0132
d22	0.0000	0.0038	0.0004	0.0013	0.0048	0.0056	0.0129	0.0114	0.0126	0.0119	0.0095	0.0085
d23	0.0000	0.0042	0.0015	0.0008	0.0044	0.0045	0.0183	0.0166	0.0172	0.0177	0.0156	0.0154
d31	0.0000	0.0071	0.0108	0.0057	0.0284	0.0252	0.0657	0.0592	0.0568	0.0607	0.0426	0.0445
d32	0.0058	0.0007	0.0112	0.0022	0.0145	0.0112	0.0499	0.0536	0.0458	0.0519	0.0439	0.0458
d41	0.0028	0.0047	0.0012	0.0000	0.0082	0.0104	0.0268	0.0260	0.0284	0.0290	0.0231	0.0217
d42	0.0000	0.0018	0.0011	0.0003	0.0031	0.0026	0.0091	0.0079	0.0082	0.0088	0.0069	0.0072
d51	0.0068	0.0037	0.0145	0.0000	0.0145	0.0244	0.0683	0.0701	0.0619	0.0732	0.0619	0.0566
d52	0.0000	0.0011	0.0028	0.0009	0.0045	0.0035	0.0156	0.0148	0.0136	0.0150	0.0126	0.0132
d53	0.0000	0.0025	0.0004	0.0013	0.0048	0.0056	0.0129	0.0110	0.0126	0.0119	0.0095	0.0085
dt	0.0298	0.1308	0.1705	0.0469	0.3227	0.3082	0.9757	0.9001	0.8723	0.9610	0.7684	0.7788

Table 10. Relative Closeness of the Alternatives

Alternatives	HMSS-1	HMSS-2	HMSS-3	HMSS-4	HMSS-5	HMSS-6
Relative Closeness (RCi)	0.9246	0.9855	0.9846	0.8955	0.7255	0.6959
Ranks	3	1	2	4	5	6

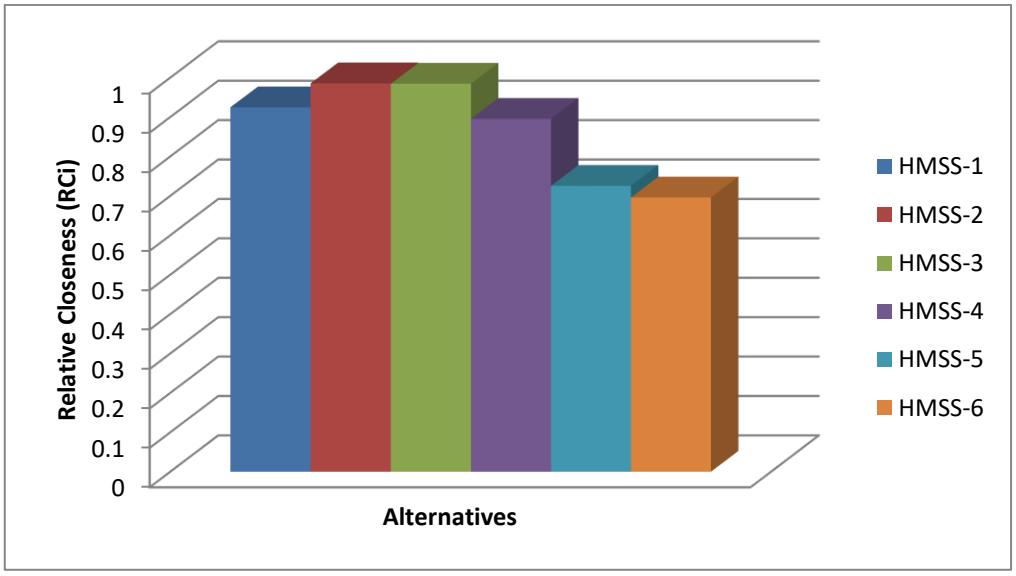


Fig. 6. Graphical Illustration of the Relative Closeness (RCi) for specified Alternatives

The sensitivity evaluation is achieved by changing the variables that affect the accuracy of the study obtained. During this statistical analysis, sensitivity assessment on resulted weights (variables) was performed. After this (2nd) stage 16 variables were taken all through this research study so as to check the sensitivities with the support of 16 experiments. From each experiment the rate of satisfaction (CC-i) was accomplished by considering weight adjustments within each variable, while the weight of the other entire variable remained constant by both the Fuzzy-ANP-TOPSIS technique. Projected effects are given in **Table 11** and **Fig. 7**.

Table 11. Sensitivity Analysis

Experiments	Weights/Alternatives		HMSS1	HMSS2	HMSS3	HMSS4	HMSS5	HMSS6
	Original Weights	Satisfaction Degree (CC-i)	0.9246	0.9855	0.9846	0.8955	0.7255	0.6959
Exp. 1	F11		0.9439	0.8322	0.8179	0.9415	0.6673	0.6496
ExP.2	F12		0.9713	0.8657	0.8451	0.9684	0.6978	0.7180
Exp. 3	F13		0.9725	0.8752	0.8487	0.9785	0.7258	0.7285
Exp. 4	F14		0.9657	0.8658	0.8487	0.9687	0.6987	0.7189
Exp. 5	F15		0.9056	0.7845	0.7831	0.8982	0.6309	0.6559
Exp.6	F16		0.9784	0.8711	0.8129	0.9211	0.6891	0.7145
Exp. 7	F21		0.9724	0.8708	0.8597	0.9742	0.7037	0.7194
Exp. 8	F22		0.9501	0.8608	0.8467	0.9627	0.6942	0.7189
Exp. 9	F23		0.9537	0.8553	0.8537	0.9567	0.6897	0.7174
Exp. 10	F31		0.9627	0.6778	0.8411	0.9468	0.6989	0.7084
Exp. 11	F32		0.9239	0.8232	0.8079	0.9315	0.6573	0.6796
Exp. 12	F41		0.8766	0.7742	0.7631	0.8882	0.6109	0.6359
Exp. 13	F42		0.9684	0.8611	0.8529	0.9811	0.6991	0.7246
Exp. 14	F51		0.9530	0.8728	0.8507	0.9667	0.7060	0.7095
Exp. 15	F52		0.9783	0.8908	0.8469	0.9711	0.6917	0.7285
Exp. 16	F53		0.9280	0.8338	0.8107	0.9234	0.6567	0.6702

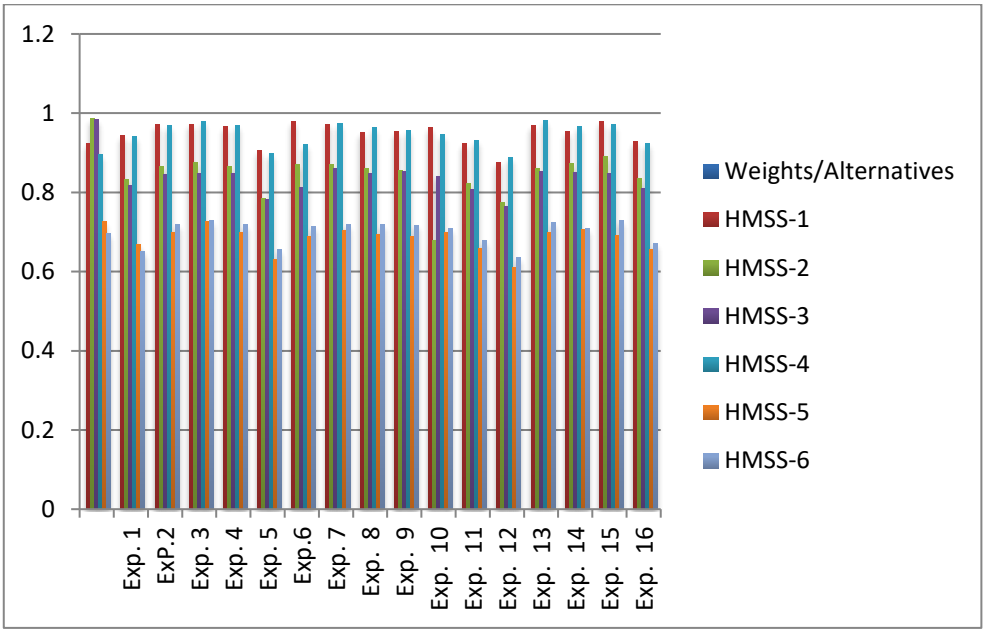


Fig. 7. Graph of Sensitivity Analysis

6. Discussion

Security is progressively going to be a big major consideration when designing real-time convergent software frequently used in commercial enterprise and academic organizations [30, 31]. Complex nature of the software application is increasing correspondingly along with its relevance in daily life. Nonetheless, insufficiency of available security architecture is the main reason for the increase in the instances of data security breaches. Given the considerable spending on security methods and techniques, there's also been a significant growth in the number of cyber-attacks. As per HIPPA data breach estimates (2018-2019), there had been 2,546 security breaches in the healthcare industry between 2009 and 2018 and each breach involved more than 500 records. These breaches ultimately resulted in theft / exposure of more than 189 million health-care records. Such a scenario necessitates the need for high quality usable-security software applications.

This research article proposed to calculate the software system's usability-security. For this reason, an instance of study was directed on six different hospital management systems in Varanasi, Uttar Pradesh, India. The study mainly used five usable-security attributes at Tier 1 and 16 at Tier 2 with six significant alternative solutions, specifically: HMSS1, HMSS2, HMSS3, HMSS4, HMSS5, and HMSS6. The findings obtained would be very beneficial for the professionals in designing and developing security-critical software products with usable-security, particularly in the healthcare industry. Numerous security alternatives are described that individually assess security and usability, however these models that incorporate security and usability into one sequence that include FANP, TOPSIS and several other decision-making multi-criteria, are very limited in number. The authors of this article have employed the MCDM integrated system of fuzzy-ANP TOPSIS to quantify usable security application, as fuzzy-ANP, unlike fuzzy-AHP, represents attribute and alternative specific suggestions [32,

33]. Because of this, it represents the actual issues meticulously and provides better results [13, 20, 22, 23] as well as fuzzy logic identifies and covers the ambiguous and incomplete data really well in decision problems [7]. In addition, TOPSIS seems to be extremely effective in scoring alternative solutions, and enhances the selection of the most appropriate alternative amongst all the reasonable alternatives [25-28]. The current study consequently incorporates the combination of fuzzy-ANP TOPSIS to accomplish maximum efficiency, especially in comparison to other MCMD techniques. Finally, this research showed that alternative (HMSS5) offers maximum security, including maximum customer satisfaction amongst the other six alternative solutions. The findings along with the advantages and disadvantages of the study are:

Pros:

- Usable-security assessment of several web applications centered on hospital management system will help the engineers in achieving the target of full consumer satisfaction by producing high-quality web-applications.
- The obtained outcome derived from this research analysis by using hybrid Fuzzy ANP-TOPSIS may be useful for software professionals when it comes to classifying different characteristics and choosing usable-security-design throughout quality software application production. This would lead to the production of quality software and web based application software which requires enduring usability-security.
- Usable-security is a serious issue in the present scenario but it still gets neglected. This Study would be a decisive orientation for the software developers for deep understanding of usable-security design.

Delimits:

- Recognition and selection of attributes is not ideal or definitive for usable-security evaluation. Findings may vary depending on the numbers of characteristics which might raise or lower the rate of different factors.
- Hybrid fuzzy-ANP TOPSIS is one of the prevalent approaches that we have used for usable-security assessment; however, there could be greater MCDM strategies for handling complex MCMD issues.

7. Conclusion

In today's world, estimating the usable-security of security-critical software product is a must. If a software firm has inadequate security, no one would ever buy its software product. There have always been new requirements, and if they aren't a concern, one can be sure there would be a few angry clients demanding that the product in question performs on their demands for protection. The present research includes an effective hybrid F-ANP TOPSIS procedure to assess the usability-security of different web applications for the prevalent hospital management system. This study implemented the powerful hybrid Fuzzy-ANP TOPSIS approach which is the most appropriate method for evaluating any MCDM problem with various factors as well as alternative solutions, including certain usable-security assessment. Furthermore, it measures several recognized usable-security factors, and defines usable-security for several healthcare based web applications. The absolute final ranking of alternative solutions by using TOPSIS was verified for available security of different healthcare based web applications alternatives such as HMSS1, HMSS4, HMSS2, HMSS3, HMSS6, and HMSS5, respectively. As per the results, the alternative (HMSS1) offered high user satisfaction with ideal security. Inspection of usable-security of different web-based HMS

(hospital management systems) application software attempted in this study will support the practitioners in building high quality products with usable-security.

Acknowledgement

The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by grant code 19-COM-1-01-0015.

References

[1] M. T. J. Ansari and D. Pandey, "Risks, Security, and Privacy for HIV/AIDS Data: Big Data Perspective," *Big Data Analytics in HIV/AIDS Research*, pp. 117-139, 2018. Article (CrossRef Link)

[2] Healthcare Data Breach Statistics, 2020. Article (CrossRef Link)

[3] A. Agrawal, M. Alenezi, S. A. Khan, R. Kumar, and R. A. Khan, "Multi-Level Fuzzy System for Usable-Security Assessment," *Journal of King Saud University-Computer and Information Sciences*, 2019. Article (CrossRef Link)

[4] F. A. Al-Zahrani, "Evaluating the Usable-Security of Healthcare Software through Unified Technique of Fuzzy Logic, ANP and TOPSIS," *IEEE Access*, vol. 8, no. 7, pp. 109905-109916, 2020. Article (CrossRef Link)

[5] M. T. J. Ansari, D. Pandey, and M. Alenezi, "STORE: Security Threat Oriented Requirements Engineering Methodology," *Journal of King Saud University-Computer and Information Sciences*, Article in Press, 2018. Article (CrossRef Link)

[6] T. J. Ross, Fuzzy Logic with Engineering Applications, Third Edition, John Wiley & Sons, 2010. Article (CrossRef Link)

[7] M. Zarour, Md. T. J. Ansari, M. Alenezi, A. K. Sarkar, M. Faizan, A. Agrawal, R. Kumar, and R. A. Khan, "Evaluating the Impact of Blockchain Models for Secure and Trustworthy Electronic Healthcare Records," *IEEE Access*, vol. 8, no. 8, pp. 157959-157973, 2020. Article (CrossRef Link)

[8] B. Roy and S. K. Misra, "An Integrated Fuzzy ANP and TOPSIS Methodology for Software Selection under MCDM Perspective," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 6, no. 1, pp. 492-501, 2018. Article (CrossRef Link)

[9] K. C. Park, J. W. Shin, and B. G. Lee, "Analysis of Authentication Methods for Smartphone Banking Service using ANP," *KSII Transactions on Internet and Information Systems*, vol. 8, no. 6, pp. 2087-2103, 2014. Article (CrossRef Link)

[10] P. Biswas, S. Pramanik, and B. C. Giri, "TOPSIS Method for Multi-Attribute Group Decision-Making under Single-Valued Neutrosophic Environment," *Neural Computing and Applications*, vol. 27, pp. 727-737, 2016. Article (CrossRef Link)

[11] R. R. Kumar, S. Mishra, and C. Kumar, "Prioritizing the Solution of Cloud Service Selection using Integrated MCDM Methods under Fuzzy Environment," *The Journal of Supercomputing*, vol. 73, pp. 4652-4682, 2017. Article (CrossRef Link)

[12] M. Hassenzahl, "Hedonic, Emotional, and Experiential Perspectives on Product Quality," *Encyclopedia of Human Cmputer Interaction*, pp. 266-272, 2006. Article (CrossRef Link)

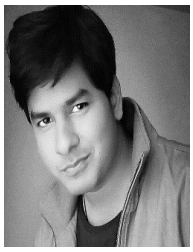
[13] K. Sahu and R. K. Srivastava, "Soft Computing Approach for Prediction of Software Reliability," *ICIC Express Letter*, vol. 12, no. 12, pp. 1213-1222, 2018. Article (CrossRef Link)

[14] A. Agrawal, M. Zarour, M. Alenezi, R. Kumar, and R. A. Khan, "Security Durability Assessment through Fuzzy Analytic Hierarchy Process," *PeerJ Computer Science*, vol. 5, 2019. Article (CrossRef Link)

[15] G. Kapil, A. Agrawal, A. Attaallah, A. Algarni, R. Kumar, and R. A. Khan, "Attribute based Honey Encryption Algorithm for Securing Big Data: Hadoop Distributed File System Perspective," *PeerJ Computer Science*, vol. 6, 2020. Article (CrossRef Link)

[16] M. A. Aladwani, "The Development of Two Tools for Measuring the Easiness and Usefulness of Transactional Web Sites," *European Journal of Information Systems*, vol. 11, no. 3, pp. 223-234, 2002. Article (CrossRef Link)
[17] 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. 11, pp. 1770-1792, 2020. Article (CrossRef Link)
[18] R. P. Lourenço, "An Analysis of Open Government Portals: A Perspective of Transparency for Accountability," *Government Information Quarterly*, vol. 32, no. 3, pp. 323-332, 2015. Article (CrossRef Link)
[19] I. Nassar-Eddine, A. Obbadi, K. Et-Torabi, H. Mokhliss, A. Elamiri, R. Rmaily, Y. Errami, A. El Fajri, S. Sahnoun, and M. Agunaou, "A New Fuzzy Logic Architecture to Control the DC-Bus Voltage in Grid Connected Photovoltaic System," in *Proc. of 2019 International Conference of Computer Science and Renewable Energies*, pp. 1-7, 2019. Article (CrossRef Link)
[20] T. L. Saaty and L. G. Vargas, Decision Making with the Analytic Network Process, Springer, vol. 95, 2006. Article (CrossRef Link)
[21] T. L. Saaty, The Analytic Hierarchy Process, Agricultural Economics Review, New York, USA: McGraw Hill, 1980. Article (CrossRef Link)
[22] İ. Yüksel and M. Dağdeviren, "Using the Fuzzy Analytic Network Process (ANP) for Balanced Scorecard (BSC): A Case Study for a Manufacturing Firm," *Expert Systems with Applications*, vol. 37, no. 2, pp. 1270-1278, 2010. Article (CrossRef Link)
[23] M. C. Lee, H. W. Wang, and H. Y. Wang, "A Method of Performance Evaluation by Using the Analytic Network Process and Balanced Score Car," in *Proc. of 2007 International Conference on Convergence Information Technology*, pp. 235-240, 2007. Article (CrossRef Link)
[24] R. Kumar, M. Alenezi, M. T. J. Ansari, B. Gupta, A. Agrawal, and R. A. Khan, "Evaluating the Impact of Malware Analysis Techniques for Securing Web Applications through a Decision-Making Framework under Fuzzy Environment," *International Journal of Intelligent Engineering and Systems*, vol. 13, no. 6, pp. 94-109, 2020. Article (CrossRef Link)
[25] C. L. Hwang, Y. J. Lai, and T. Y. Liu, "A New Approach for Multiple Objective Decision Making," *Computers & Operations Research*, vol. 20, no. 8, pp. 889-899, 1993.
[26] J. W. Wang, C. H. Cheng, and K. C. Huang, "Fuzzy Hierarchical TOPSIS for Supplier Selection," *Applied Soft Computing*, vol. 9, no. 1, pp. 377-386, 2009. Article (CrossRef Link)
[27] A. Mohaghar, M. R. Fathi, A. Faghih, and M. M. Turkayesh, "An Integrated Approach of Fuzzy ANP and Fuzzy TOPSIS for R&D Project Selection: A Case Study," *Australian Journal of Basic and Applied Sciences*, vol. 6, no. 2, pp. 66-75, 2012. Article (CrossRef Link)
[28] M. N. Omar and A. R. Fayek, "A TOPSIS-based Approach for Prioritized Aggregation in Multi-Criteria Decision-Making Problems," *Journal of Multi-Criteria Decision Analysis*, vol. 23, no. 5-6, pp. 197-209, 2016. Article (CrossRef Link)
[29] M. T. J. Ansari, F. A. Al-Zahrani, D. Pandey, and A. Agrawal, "A Fuzzy TOPSIS based Analysis toward Selection of Effective Security Requirements Engineering Approach for Trustworthy Healthcare Software Development," *BMC Medical Informatics and Decision Making*, vol. 20, no. 1, pp. 1-13. Article (CrossRef Link)
[30] T. Xie and X. Qin, "Security-Aware Resource Allocation for Real-Time Parallel Jobs on Homogeneous and Heterogeneous Clusters," *IEEE Transactions on Parallel and Distributed Systems*, vol. 19, no. 5, pp. 682-697, 2008. Article (CrossRef Link)
[31] H. Chen, X. Zhu, G. Liu, and W. Pedrycz, "Uncertainty-Aware Online Scheduling for Real-Time Workflows in Cloud Service Environment," *IEEE Transactions on Services Computing*, 2018. Article (CrossRef Link)
[32] 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. Artcle (CrossRef Link)
[33] K. Sahu and R. K. Srivastava, "Revisiting Software Reliability," *Advances in Intelligent Systems and Computing*, vol. 808, pp. 221-235, 2019. Article (CrossRef Link)

Dr. Rajeev Kumar received the master's and Ph.D. degrees in information technology from Babasaheb Bhimrao Ambedkar University, Lucknow, India, in 2014 and 2019, respectively. He has more than five years of research and teaching experience. He is a young and energetic Researcher and holds two Major Projects (With PI) funded by University Grants Commission, New Delhi, and Council of Science & Technology, Uttar Pradesh (CST-UP), India. He is currently working as an Assistant Professor in the Department of Computer Application, Shri Ramswaroop Memorial University, Lucknow, Uttar Pradesh, India and as a Guest Faculty in the Department of Information Technology, Babasaheb Bhimrao Ambedkar University (A Central University), Lucknow, Uttar Pradesh, India. He has also published and presented articles in refereed journals and conferences. His research interest includes different areas of security engineering.



Dr. Md Tarique Jamal Ansari received a bachelor degree in Computer Application from University of Lucknow, India, in 2012, M.Sc. degree in Information Technology from BBA University, India, in 2015 and the Ph.D. degree in Information Technology from Department of Information Technology, BBA University, Lucknow, India in 2020. He is currently Assistant Professor with the Department of Computer Application, Integral University, Lucknow. His research interest includes Security Requirements Engineering, Software Engineering, Software Security, Blockchain, Cloud Security Engineering, Software Risk Management, Health informatics and Big Data. He is a University Gold Medalist for first rank during his Master's degree programme at BBA University, Lucknow, INDIA. He has significant contributions in international scientific journals. He is also a potential reviewer in several reputed journals.

Dr. Abdullah Baz received the B.Sc. degree in electrical and computer engineering from UQU, in 2002, the M.Sc. degree in electrical and computer engineering from KAU, in 2007, and the M.Sc. degree in communication and signal processing and the Ph.D. degree in computer system design from Newcastle University, in 2009 and 2014, respectively. He was a Vice-Dean, and then the Dean of the Deanship of Scientific Research with UQU, from 2014 to 2020. He is currently an Associate Professor with the Computer Engineering Department, a Vice-Dean of DFMEA, the General Director of the Decision Support Center, and the Consultant of the University Vice Chancellor with UQU. His research interests include data science, ML, AI, VLSI design, EDA/CAD tools, intelligent transportation, computer system and architecture, smart systems, smart health. Since 2015, he has been served as a Review Committee Member of the IEEE International Symposium on Circuits and Systems (ISCAS) and a member of the Technical Committee of the IEEE VLSI Systems and Applications. In 2017, IEEE has elevated him to the grade of IEEE Senior Member. He served as a Reviewer in a number of journals, including the IEEE Internet of Things, the IET Computer Vision, the Artificial Intelligence Review, IEEE Access, and the IET Circuits, Devices and Systems.

Dr. Hosam Alhakami received the B.Sc. degree in computer science from King Abdulaziz University, Saudi Arabia, in 2004, the M.Sc. degree in internet software systems from Birmingham University, Birmingham, U.K., in 2009, and the Ph.D. degree in software engineering from De Montfort University, in 2015. From 2004 to 2007, he worked with Software Development Industry, where he implemented several systems and solutions for a national academic institution. Dr. Alhakami was the Vice-Dean of the Deanship of Admission and Registration for Academic affairs with UQU, from 2015 to 2020. Currently, he is an Associate Professor of the computer science department with UQU. His research interests include algorithms, semantic web, and optimization techniques. He focuses on enhancing real-world matching systems using machine learning and data analytics in a context of supporting decision-making. In 2020, IEEE has elevated him to the grade of IEEE Senior Member.

Dr. Alka Agrawal has earned her Doctoral Degree from Babasaheb Bhimrao Ambedkar University, (A Central University), Vidya Vihar, Raibareli Road, Lucknow and she is currently working as an Assistant Professor in the same Department. Dr. Alka is a passionate researcher and has also published a number of research papers in national and international journals both. She has research/ teaching experience of more than 12 years. Her areas of research include Software Security, Software Vulnerability. She is currently working in the fields of Big Data Security, Genetic Algorithms and Software Security.

Prof. Raees Ahmad Khan (Member, IEEE) is currently working as a Professor & Head of the Department in the Department of Information Technology, Dean of School for Information Science & Technology, Babasaheb Bhimrao Ambedkar University, (A Central University), Vidya Vihar, Raibareli Road, Lucknow, India. Prof. Khan has more than 20 years of teaching & research experience. Prof. Khan has published more than 300 research publications with good impact factors in reputed International Journals and Conferences including IEEE, Springer, Elsevier, Inderscience, Hindawi, and IGI Global etc. He has published a number of National and International Books (Authored and Edited) (including Chinese Language). His research interests are in the different areas of Security Engineering and Computational Techniques.