Journal of Information Systems Engineering and Management
2025, 10(25s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Evaluating the Impact of Security Risks through Fuzzy AHP-TOPSIS Method

Mohd Shabbir[1, 2], Rakesh Kumar Yadav[3], Mohd Waris Khan[4,*]
[1]*Ph.D candidate, Department of Computer Science and Engineering, Maharishi University of Information Technology, Lucknow, India*
[2]*Assistant Professor, Integral University, Lucknow, India*
[3]*Associate Professor, Department of Computer Science and Engineering, Maharishi University of Information Technology, Lucknow, India*
[4] *Assistant Professor, Department of Computer Application, Integral University, Lucknow, 226026, India*
**Corresponding Author:* wariskhan070@gmail.com

ARTICLE INFO

Received: 21 Dec 2024

Revised: 12 Feb 2025

Accepted: 25 Feb 2025

ABSTRACT

The increasing demand for big data and the depletion of security in data become a critical threat in the digital world. Selecting appropriate information and developing a secure application is a critical task in the software development life cycle (SDLC). This paper shows how the multi-criteria decision-making (MCDM) technique may be used to select appropriate risk factors and define the criteria for the development of software. The proposed model is the integration of two MCDM approaches, i.e., AHP and TOPSIS that are used to calculate the ideal criteria. The appropriate criteria are determined by analyzing risk variables during the requirement engineering stage of the SDLC and their impact on risk attributes. Through the integration of AHP with TOPSIS, an effective pair-wise comparison process and ranking of criteria for optimal and secure software are evaluated in this model. The study presents a novel perspective on the MCDM technique. Furthermore, the security risk's influence on the requirements engineering process was quantified. Practitioners can apply the findings and conclusions to enhance software usability and security.

Keywords: Confidentiality, integrity, authentication, non-repudiation.

INTRODUCTION

The Today, all over the world, all the projects are digital, and most organizations depend on the digital world. Digitalization makes user tasks more inventive and organized for individuals and enterprises [1]. In terms of software deployment, there has been a significant rise. Although computers and digital technology enhance the quality of work, they can cause extensive losses and threats at various levels of organizational procedures. It improves our working conditions, but there are some security concerns, which make it a top priority for security specialists to address systematically [2]. The dependency on digitalization resulted in new threats, which is a sad fact of life [3]. The risks cannot be perfectly eliminated, but software developers can reduce the risks to some extent. Software security refers to addressing security at each SDLC phase, resulting in software that can perform the required action in case of an attack [4, 5]. In SDLC, the first and most significant area is requirements engineering. If the errors made at the SDLC phase are not identified in the earlier phase, they can be pretty expensive. Various kinds of risks that arise at this phase that are not easily considered and handled will fail the software [6]. The size of a project significantly impacts its level of risk and complexity during development. Accurately specifying requirements early on can reduce issues in subsequent stages, ultimately lowering software development and maintenance costs while ensuring customers receive the system they desire. This paper emphasizes the use of risk management tools and techniques to address risks early in the Software Development Life Cycle (SDLC). These tools provide structured methods to identify and prioritize risk factors, helping to mitigate potential challenges effectively [7, 8].

One of the methodologies is AHP (Analytical Hierarchy Process), which is widely used for decision-making and analyzing risk. AHP is gaining popularity in different fields, analyzing complex circumstances and providing sound decisions [9]. It facilitates an effective solution for multi-criteria decision-making when the sample size is small [10]. The multi-criteria decision analysis provides a number of strategies and techniques for resolving conflicts between different aspects of a concerned security problem [11, 12]. AHP solves the problem by structuring a hierarchy of levels that are interdependent from the higher level to the lower level [13, 14]. On the other hand, the

TOPSIS method finds the best viable critical criteria that are the closest to the ideal positive solution and the farthest from the ideal negative solution [15, 16].

This paper used the integrated approach of TOPSIS and AHP to manage the risk and find the optimal solution for the risk-free development of software. The weights of each criterion are computed using the AHP approach, and the rank of the criteria is determined using TOPSIS. An AHP-TOPSIS methodology is best for risk evaluation and mitigation because risks can be identified from the analysis collected in the form of factors that affect the performance of development. So, AHP is used to figure out how much each criterion matters, and TOPSIS is used to figure out which option is best.

The key contribution of this research work:

1. The study integrates AHP and TOPSIS methodologies to effectively manage risks and ensure risk-free software development.
2. Fuzzy AHP TOPSIS is utilized to rank the criteria based on their significance and identify the optimal solution.
3. The AHP-TOPSIS approach is highlighted as an effective methodology for evaluating and mitigating risks in software development.
4. Risks are identified and assessed through the analysis of factors influencing development performance, facilitating informed decision-making.

The remainder of the paper is organized as follows: Section 2 discusses the requirement for engineering security attributes. Section 3 presents the methodology, in which the complete work flow is explained. In Section 4, data analysis and the results are shown. The discussion is done in Section 5, and the paper is concluded in Section 6.

SECURITY ASSESSMENT OF REQUIREMENT ENGINEERING

Requirement engineering phase is the first and foremost important phase of SDLC and information field. It is essential for effective and rapid development of software. The requirements engineering phases provides exact need of customers to the developers and assist in decision making to improve the development. Consequently, any variation and change negatively affect the whole process. Thus, security of software is the censorious factor that must be scrutinize earlier.

Confidentiality

Confidentiality refers a condition where user's data and resources disclosed by unauthorized access. Confidential information of any stakeholder is very crucial and loss of this information makes total system failure. Confidential information only available to authorized persons. Requirement engineering is the step in SDLC which will highly confidential to access [17].

Authentication

Authentication commonly referred s validation of user and their data. In the process of authentication the identity of user is validate and all the data of user is matched with the stored data. Authentication is a very important process in requirement engineering to validate the information given by a stakeholder, which will help to develop a system faster and meet the stakeholder requirements with quality [18].

Authorization

Authorization is the process that gives permission to access the system. This will be done when identification, validation, and authentication have been completed [19].

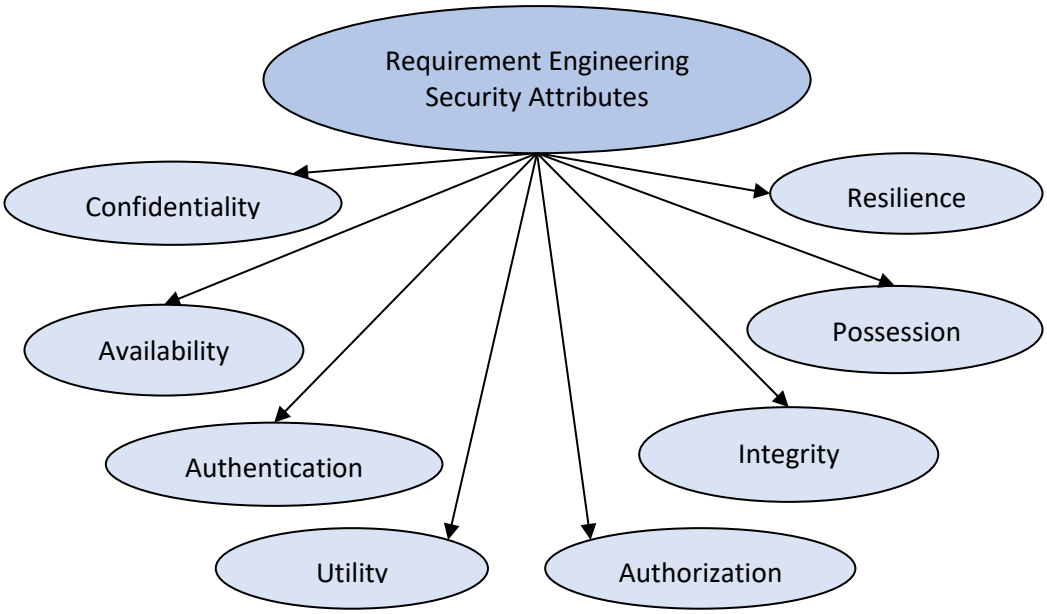

Figure 1. Security attributes of requirement engineering

Availability

Availability refer as, when the data is easily available when it requires. In the case of requirement engineering the data should be available to developer. Availability of data is depends also on, how easily it will available in the case of power failure, software failure and up gradation and hardware failure [20].

Utility

Utility refers to the usefulness of old data. In the case of requirement engineering, according to the customer requirements, sometimes old data is require or sometimes not. This is called as utility. The utility of old data depends on the customer's current requirements. The availability and utility have slight difference as data is available is called availability but it is no longer useful represents its utility.

Integrity

Integrity refers to the accuracy of data. The major security factor of requirement engineering is to achieve complete and correct information from stakeholder. The data or information which collects from the user should not change or altered in between the processing and development of software [21].

Possession

Possession means the ownership. The ownership of data should be maintained from the staring. It demonstrates data control. Ownership of data in terms of requirement engineering is determined by the requirement. If ownership lost then original data may be corrupted and whole system goes towards failure.

Resilience

The term "resilience" relates to the testing of a requirement engineering system's resistance to attacks. Resilience is maintained in the requirement engineering system through the use of OTP and encryption. By considering all dangerous scenarios in the system, resilience is vital for protecting the entire software and development process from attacks.

The information sector relies heavily on software. Security should be a top priority while designing software utilizing the SDLC. These security attributes helps to design the guidelines of development that are used as major criteria to minimize the risk factors at an early step of SDLC i.e. Requirement Engineering.

METHODS

Security issues in requirement engineering are a serious concern for many authors. Identifying and mitigating risk factors from the software development process through the AHP-TOPSIS technique; used to achieve the goal of a

highly secure system and the satisfaction of customers [22]. To achieve this objective MCDM is used in this research. This methodology section of Fuzzy AHP-TOPSIS is separately explained with mathematical identities as shown in **figure 2.** There is a sequence of steps is followed for the assessment of security [23]. The methodology contains the 3 sections-

- In the first section a model is proposed for determining the criteria from risk factors in the requirement engineering phase of SDLC [24].
- In the second section Fuzzy AHP method used to evaluate the weights of each criterion.
- Finally, the rank of the alternatives is determined using Fuzzy TOPSIS [25].

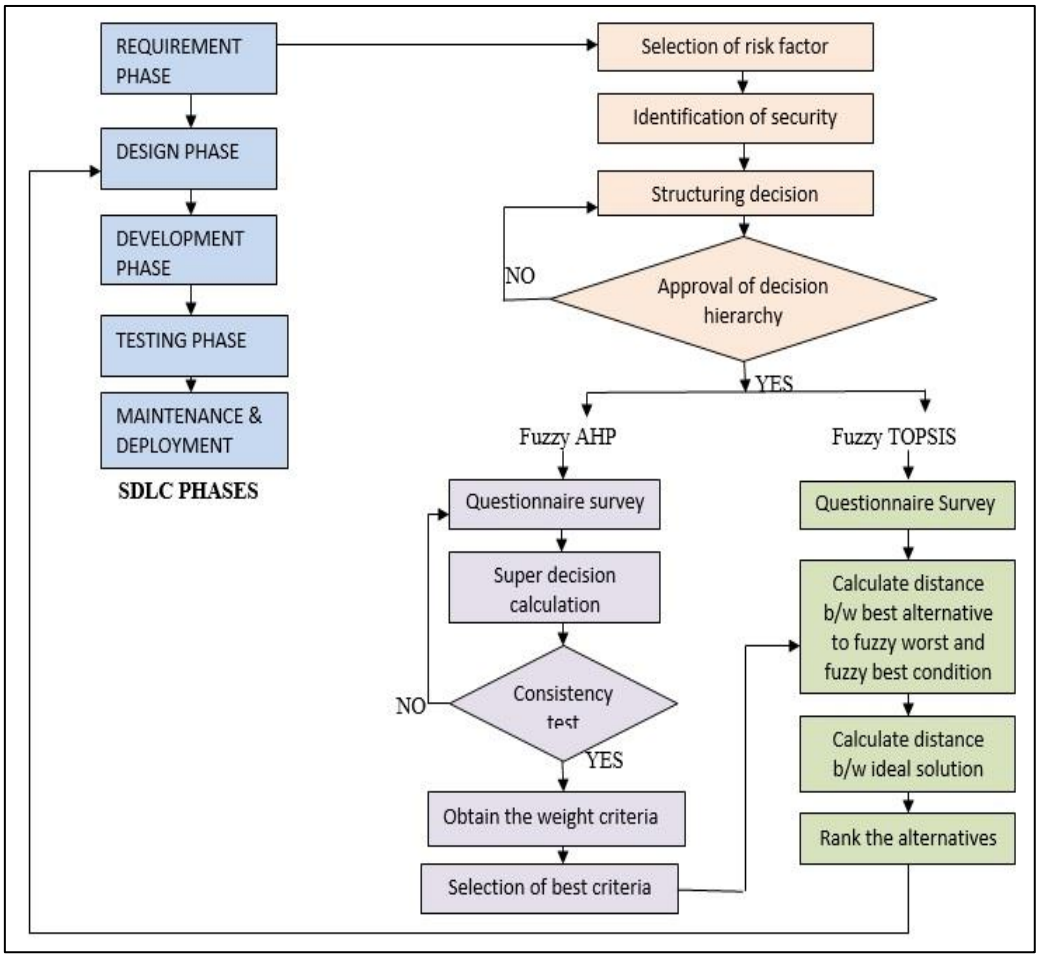

Figure 2. Proposed framework for secure development of software

Proposed Model

SDLC cycle have 5 phases in the series of software development. In this research work consider the requirement engineering phase and list down the risk factors and from these risk factors determine the criteria for security. This model is best for identifying risk factors and reduces the risks at early stage of SDLC which will save resources and time both. The steps which are followed in this model are described below-

- Gathering requirement from the customers and stakeholder and build software requirement specification (SRS) document.
- Follow all the four basic activities of requirement engineering i.e. requirement elicitation, specification, validation and documentation.
- From these activities select the risk factors.
- Then List down all the criteria.
- Build a decision hierarchy.
- After completing the decision hierarchy go for the Fuzzy AHP-TOPSIS merger methodology.
- Calculate the weights of criteria and select best criteria among them [26].

- Then calculate distance between best alternatives to fuzzy worst and fuzzy best solution.
- In the last step calculate the rank of alternatives.
- And according to rank of alternatives prioritize the process and go for the next phase of SDLC.

Fuzzy AHP

Fuzzy Analytical hierarchy process (AHP) is a widely used method for decision making problems. Fuzzy AHP approach is used to calculate weights of criteria which are collected from risk factors. Fuzzy AHP organize the problems in a hierarchical structure from higher level to lower level which are interconnected with each other [27]. The hierarchical structure divided into 3 majorly levels. Top level represents the objective and goal. Middle level shows the criteria and related sub-criteria and last level represents the alternatives which are analogous with criteria and its sub-criteria. The next step is to determine the Triangular fuzzy number (TFN) from the hierarchical structure after it has been built. Then, the triangular fuzzy values are used to build a comparison matrix.

Chang [28] and Cheng [29] employed triangular fuzzy membership values for pair wise comparison by using FAHP algorithm for calculating naval tactical system. Chang employed triangular fuzzy membership values for pair wise comparison matrices [28] and Cheng employed FAHP algorithm for naval tactical system [29]. In this paper triangular fuzzy membership (TFN) values are used to calculate the fuzzy weights. TFN values are lies between 0 and 1 as similar to fuzzy values [30]. In the **table 1** linguistic values are split into strongly important equally important, fairly important, absolute important, and weakly important etc. the membership functions of theses linguistic values are calculated as using (1, 2) mathematical identities.

$$\mu_{a(x)=a\to[0,1]} \quad \text{..... (1)}$$

$$\mu_{a(x)=\left\{\frac{x}{Q-P}-\frac{P}{Q-P}\,x\in[P,Q]\frac{P}{Q-R}-\frac{u}{Q-R}\,x\in[Q,R]\right\}} \quad \text{..... (2)}$$

P, Q, and R are equally assigned for triangular membership function as lower, middle and upper value respectively. The TFN values are represented in **figure 3**.

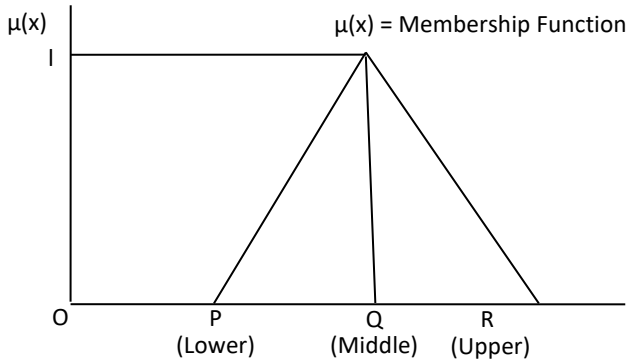

Figure 3. Triangular Membership Function (TFN)

Figure 3 shows the triangular membership functions in a graphical way. Experts assigned some of the numerical values to all the linguistic values as shown in **table 1.**

Table 1. TFN represented in Linguistic Terms

Security Assessment Scale	Linguistic Terms	Membership Function (TFN's)
1	Equally Important	(1,1,1)
2	Immediate Values	(1,2,3)
4	Between two	(3,4,5)
6	Adjacent	(5,6,7)
8	Scales	(7,8,9)

3	Weakly important	(2,3,4)
5	Fairly important	(4,5,6)
7	Strongly important	(6,7,8)
9	Absolutely important	(9,9,9)

Now, we convert numerical data into TFN using (3, 4, 5, 6) mathematical identities. Øij [TFN] calculated as

$$\text{Øij} = (P_{ij}, Q_{ij}, R_{ij}) \quad \text{..... (3)}$$

Where $P_{ij} \leq Q_{ij} \leq R_{ij}$

$$P_{ij} = \min (J_{ijd}) \quad \text{..... (4)}$$

$$Q_{ij} = (J_{ij1}, J_{ij2,} J_{ij3})^{\frac{1}{x}} \quad \text{..... (5)}$$

$$\text{and } R_{ij} = \max(J_{ijd}) \quad \text{..... (6)}$$

To evaluate the geometric mean, we are using two methods by multiplying and adding two different fuzzy numbers using (7-9) mathematical identities. Let two TFNs M1 and M2, $M1 = (P_1, Q_1, R_1)$ and $M2 = (P_2, Q_2, R_2)$

$$(P_1, Q_1, R_1) + (P_2, Q_2, R_2) = (P_1 + P_2,\ Q_1 + Q_2\ , R_1 + R_2) \quad \text{..... (7)}$$

$$(P_1, Q_1, R_1) \times (P_2, Q_2, R_2) = (P_1 \times P_2,\ Q_1 \times Q_2\ , R_1 \times R_2) \quad \text{..... (8)}$$

$$(P_1, Q_1, R_1)\text{-}1 = (1/R_1, 1/Q_1, 1/P_1) \quad \text{..... (9)}$$

The column and row elements are divided into two halves to calculate the pair wise n*n comparison matrices using the (10) mathematical identity.

The column and row elements are divided into two halves to calculate the pair wise n*n comparison matrices using the (10) mathematical identity

$$\tilde{A}^d = [\tilde{B}^d_{11} \tilde{B}^d_{12} \ldots . \tilde{B}^d_{1n} \tilde{B}^d_{21} \tilde{B}^d_{22} \ldots . \tilde{B}^d_{2n} \ldots \ldots \tilde{B}^d_{n1} B^d_{n2} \ldots \tilde{B}^d_{nn}] \quad \text{..... (10)}$$

Where $\tilde{B}^k_{ij}$ shows the d^{th} experts which give importance to the i^{th} fact over the j fact. If two experts are presents then the average of each expert is calculated by the (11) mathematical identity

$$\tilde{B}_{ij} = \sum_{d=1}^{d} \tilde{B}^d_{ij} \quad \text{..... (11)}$$

Next, using the (12) mathematical identity, take the average of all given factors in a hierarchy and update the comparative metrics.

$$\tilde{A} = [\tilde{B}_{11} \ldots . \tilde{B}_{1n} \ldots \ldots . \tilde{B} \ldots . \tilde{B}_{nn}] \quad \text{..... (12)}$$

Calculate the fuzzy geometric mean and fuzzy weights of each factor after updating the comparison metrics by using (13) mathematical identity

$$\tilde{O}_i = (\prod_{j=1}^{n} \tilde{B}_{ij})^{\frac{1}{n}},\ i = 1,2,3 \ldots\ldots n \quad \text{..... (13)}$$

Now, add all the geometric mean and calculate the fuzzy weight

$$\tilde{M}_i = \tilde{O}_i * (\tilde{O}_1 + \tilde{O}_2 + \tilde{O}_3 \ldots . . + O_n)^{-1} \quad \text{..... (14)}$$

Now, calculate fuzzy average weight by (15) mathematical identity

$$N_i = \frac{\tilde{M}_1 + \tilde{M}_2 \ldots\ldots\ldots + \tilde{M}_n}{n} \quad \text{..... (15)}$$

In the next step normalize the fuzzy weights using (16) mathematical identity

$$Qw_i = \frac{N_i}{N_1 + N_2 + \cdots\ldots\ldots + N_n} \quad \text{..... (16)}$$

In the last step defuzzification method is used to defuzzify the fuzzy weights by using center of area (COA) to calculate best non- fuzzy performance (BNP) by (17) mathematical identity

$$\mathrm{BNPwD1} = \frac{[(\mathrm{RB1}-\mathrm{PB1})+(\mathrm{QB1}-\mathrm{PB1})]}{3} + \mathrm{PB1} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (17)$$

Fuzzy TOPSIS

Fuzzy AHP-TOPSIS methodology has sequence of steps. Start with the first step which employed fuzzy AHP methodology using mathematical identities from (1 to 16). In the second step construct the fuzzy design matrix by using (18) mathematical identity and decides the ratings of the alternatives with respect to criteria of security which is shown in **table 2.**

Table 2. Linguistic Scale for Rating

Linguistic Scale for Rating	Triangular Fuzzy Scale (TFN's)
Very Poor (VP)	(0,1,3)
Poor (P)	(1,3,5)
Fair (F)	(3,5,7)
Good (G)	(5,7,9)
Very good (VG)	(7,9,10)

$$\tilde{A} = \begin{bmatrix} \tilde{x}_{11} & \cdots & \tilde{x}_{1n} \\ \vdots & \ddots & \vdots \\ \tilde{x}_{m1} & \cdots & \tilde{x}_{mn} \end{bmatrix} \ldots\ldots\ldots\ldots\ldots (18)$$

Where rows represents $P_1 \ldots \ldots \ldots . . P_m$ and column represents $R_1 \ldots \ldots \ldots R_n$

In the (19) mathematical identity fuzzy decision matrix is simplified and standardized which is represented as $\tilde{F}$.

$$\tilde{F} = [\tilde{F}_{ij}]_{m*n} \ldots\ldots\ldots\ldots\ldots\ldots (19)$$

Standardization of fuzzy decision matrix is done by (20) mathematical identity.

$$\tilde{F}_{ij} = \left(\frac{P_{ij}}{R_j^+}, \frac{Q_{ij}}{R_j^+}, \frac{R_{ij}}{R_j^+}\right), R_j^+ = \max\{R_{ij}, i = 1, 2, 3, \ldots n\} \ldots (20)$$

Now, the weighted fuzzy standardize matrix ($\widetilde{ST}$) is calculated by using (21) mathematical identity.

$$\widetilde{ST} = \left[\widetilde{st}_{ij}\right]_{m*n} \ i = 1, 2 \ldots m; j = 1,2,3, \ldots n \ldots\ldots (21)$$

Where $\widetilde{st}_{ij} = \tilde{F}_{ij} \times \tilde{M}_{ij}$, in the next step calculate the fuzzy positive ideal solution (FIPS) and fuzzy negative ideal solution (FINS). Both the best and worst case such as FIPSI^+ (supreme) and FINSI^- (worst) respectively is calculated by using (22, 23) mathematical identity.

$$I^+ = (\tilde{t}_1^*, \ldots \ldots \ldots \tilde{t}_j^*, \ldots \ldots \ldots \tilde{t}_n^*) \ldots\ldots\ldots\ldots\ldots (22)$$

$$I^- = (\tilde{t}_1^*, \ldots \ldots \ldots \tilde{t}_j^*, \ldots \ldots \ldots \tilde{t}_n^*) \ldots\ldots\ldots\ldots\ldots (23)$$

Where $\tilde{t}_1^*$=(1, 1, 1) × $\tilde{M}_{ij}$=($L\tilde{M}_I, M\tilde{M}_I, H\tilde{M}_i$) and $\widetilde{st}_{ij}$ =(0, 0, 0), j=1, 2, 3...n. Now the area compensation technique is used to calculate the distance for each alternative from I^+ and I^- which is represented as $\tilde{D}_i^+$ and $\tilde{D}_i^-$ respectively by (24 and 25) mathematical identities.

$$\tilde{D}_i^+ = \sum_{j=1}^{n} D\left(\widetilde{st}_{ij}, \widetilde{st}_{ij}\right) i = 1, 2, \ldots m; j = 1,2,3 \ldots n \ \ldots\ldots (24)$$

$$\tilde{D}_i^- = \sum_{j=1}^{n} D\left(\widetilde{st}_{ij}, \widetilde{st}_{ij}\right) i = 1, 2, \ldots . . m; j = 1,2,3 \ldots . n \ldots\ldots (25)$$

In the last step further options is developed to find the desired level of each factor by using the (26) mathematical identity and calculate the most close coefficients ($\widetilde{CoC}_i$) .

$$\widetilde{CoC}_i = \frac{\tilde{K}_i^-}{K_i^+ + \tilde{K}_i^-} = 1 - \frac{\tilde{K}_i^-}{\tilde{K}_i^+ + K_i^-}, i = 1, 2, \dots, m \quad \text{..... (26)}$$

Where $\frac{\tilde{K}_i^-}{K_i^+ + \tilde{K}_i^-}$=fuzzy degree satisfaction (in the i^{th} alternative) and $\frac{\tilde{K}_i^-}{\tilde{K}_i^+ + K_i^-}$= fuzzy degree gap (in the i^{th} alternative).

DATA ANALYSIS AND RESULTS

As security is a highly resolute matter in the digital world. So qualitative and quantitative both evaluation is required to assess security in early phase of software development life cycle. Qualitative analysis has done by many authors, but quantitative analysis is typical to done for security. In recent years, all organizations and businesses have demanded software with low risk, excellent quality, and a quick delivery schedule. The fuzzy AHP-TOPSIS methodology is used in this study to investigate security risks in requirement engineering.

The attributes of security in information technology have been explained in **figure 1.** In the methodology section from (1-26) mathematical identities are explained which are used for calculating requirement engineering bases security assessment using Fuzzy AHP-TOPSIS approach [31]. After that fuzzification is performed in which numerical values are obtained from linguistic values. And these numerical values are used to build pair wise comparison matrix.

This study's objective is to build a model based on a hybrid MCDM strategy for security attributes. **Table 3** shows the seven design attributes and their weights. DP1, DP2, DP3, DP4, DP4, DP5, DP6, and DP7 are represented as design properties such as coupling, cohesion, polymorphism, encapsulation, inheritance, abstraction, and design size respectively. These all seven properties are gathered and a questionnaire is prepared on these properties which are viewed by experts. And based on their different reviews and comments the impact values are calculated.

Table 3. Attributes and 7 Security Risks

Seven Design Attributes	Attributes Weights						
DP1	1.00000, 1.00000, 1.00000	1.00000, 1.51570, 1.93310	0.48960, 0.63720, 1.00000	0.41502, 0.57043, 1.00000	0.22015, 0.28071, 0.41502	0.30146, 0.40610, 0.80705	0.60575, 1.10653, 1.60883
DP2	-	1.00000, 1.00000, 1.00000	0.57430, 0.66570, 0.80220	0.3039, 0.3936, 0.5661	0.20679, 0.30521, 0.50176	0.16063, 0.19609, 0.25031	0.30930, 0.50743, 1.00564
DP3	-	-	1.00000, 1.00000, 1.00000	1.00000, 1.31950, 1.55180	0.30009, 0.43052, 0.80207	0.80027, 0.87005, 1.00000	1.26019, 1.82050, 2.43034
DP4	-	-	-	1.00000, 1.00000, 1.00000	0.53860, 0.91403, 1.58360	0.60083, 1.05092, 1.68029	0.75003, 1.34065, 1.96011
DP5	-	-	-	-	1.00000, 1.00000, 1.00000	0.41052, 0.63072, 1.17091	0.94650, 1.10905, 1.24057
DP6	-	-	-	-	-	1.00000, 1.00000, 1.00000	1.88081, 2.50508, 3.10697
DP7	-	-	-	-	-	-	1.00000, 1.00000, 1.00000

Table 4 shows the local weight which are calculated through fuzzy AHP for obtaining better accuracy. **Table 5** shows the logistic values on the behalf of quantitative values for all the design properties. Then normalize the fuzzy matrix by using TOPSIS analysis which is given in **table 6** and **table 7** and construct a final decision matrix. And finally the normalized values are used to calculate the ranks of attributes.

Table 4. Local weight of attributes through fuzzy method

Seven Design Attributes	Local Weights							Weights
DP1	1.00000	1.49120	0.69100	0.64100	0.30270	0.52680	1.16910	**0.17330**
DP2	0.67006	1.00000	0.67070	0.41403	0.37204	0.20033	0.64095	**0.19970**
DP3	1.44070	1.47071	1.00000	1.29077	0.49305	0.85200	1.83064	**0.10310**
DP4	1.56000	2.41037	0.7706	1.00000	0.96036	1.10204	1.35011	**0.12710**
DP5	3.30036	2.60853	2.0263	1.00378	1.00000	0.71702	1.10208	**0.14140**
DP6	1.89082	4.91808	1.17370	0.90710	1.39430	1.00000	2.38520	**0.17890**
DP7	0.85054	1.53907	0.54450	0.74010	0.90679	0.41925	1.00000	**0.07650**

Table 5. Subjective cognition results evaluators in linguistic terms

	A1	A2	A3	A4	A5	A6
DP1	5.12000, 7.14000, 8.72000	3.15000, 5.15000, 6.90010	4.27000, 6.27000, 8.14000	2.80020, 4.82000, 6.80020	3.18000, 5.18000, 7.10000	1.45000, 3.07000, 4.91000
DP2	4.28000, 6.30070, 8.30070	2.45000, 4.00450, 6.40050	5.36000, 7.36000, 9.12000	3.73000, 5.70030, 7.50050	2.45000, 4.40050, 6.40050	0.90010, 2.45000, 4.40000
DP3	4.27000, 6.27000, 8.14000	2.80020, 4.82000, 6.80020	4.64000, 6.60040, 8.50050	3.00000, 5.00000, 7.14000	2.18000, 4.00090, 6.14000	4.64000, 6.60040, 8.50050
DP4	5.36000, 7.36000, 9.12000	3.73000, 5.70030, 7.50050	2.45000, 4.40050, 6.40050	0.90010, 2.45000, 4.40000	3.73000, 5.70030, 7.50050	2.45000, 4.40050, 6.40050
DP5	4.64000, 6.60040, 8.50050	3.00000, 5.00000, 7.14000	2.18000, 4.00090, 6.14000	2.82000, 4.60040, 6.64000	3.00000, 5.00000, 7.14000	2.18000, 4.00090, 6.14000
DP6	3.12000, 5.00000, 7.14000	2.40050, 4.40050, 6.45000	3.50050, 5.50050, 7.45000	1.82000, 3.73000, 5.73000	2.40050, 4.40050, 6.45000	3.50050, 5.50050, 7.45000
DP7	5.36000, 7.36000, 9.09000	2.64000, 4.64000, 6.64000	2.90000, 4.80000, 6.70000	2.80020, 4.64000, 6.64000	2.64000, 4.64000, 6.64000	3.10080, 5.10080, 7.09000

Table 6. The Normalized Fuzzy Decision Matrix

Properties/ Alternatives		A1	A2	A3	A4	A5	A6
Coupling	DP1	0.56000, 0.78000, 0.90050	0.41000, 0.68000, 0.91000	0.30070, 0.62000, 0.89000	0.23000, 0.40070, 0.78000	0.39000, 0.62000, 0.80070	0.20010, 0.45000, 0.73000

Cohesion	DP2	0.46000, 0.60090, 0.00910	0.32000, 0.58000, 0.85000	0.39000, 0.62000, 0.80070	0.20010, 0.45000, 0.73000	0.42000, 0.69000, 0.95000	0.20010, 0.46000, 0.73000
Polymorphism	DP3	0.46000, 0.60080, 0.80090	0.37000, 0.60030, 0.90000	0.42000, 0.69000, 0.95000	0.20010, 0.46000, 0.73000	0.32000, 0.59000, 0.86000	0.13000, 0.36000, 0.67000
Encapsulation	DP4	0.50080, 0.80000, 1.00000	0.49000, 0.75000, 1.00000	0.32000, 0.59000, 0.86000	0.13000, 0.36000, 0.67000	0.29000, 0.54000, 0.82000	0.40020, 0.60090, 1.00000
Inheritance	DP5	0.50000, 0.70020, 0.93000	0.00390, 0.60060, 0.94000	0.29000, 0.54000, 0.82000	0.40020, 0.60090, 1.00000	0.47000, 0.74000, 1.00000	0.27000, 0.50060, 0.86000
Abstraction	DP6	0.30040, 0.54000, 0.78000	0.32000, 0.50080, 0.85000	0.47000, 0.74000, 1.00000	0.27000, 0.50060, 0.86000	0.32000, 0.50080, 0.85000	0.47000, 0.74000, 1.00000
Design-Size	DP7	0.58000, 0.80000, 0.99000	0.30040, 0.60010, 0.87000	0.38000, 0.64000, 0.89000	0.42000, 0.60090, 1.00000	0.50000, 0.70020, 0.93000	0.00390, 0.60060, 0.94000

Table 7. Weighted Normalized Fuzzy Decision Matrix

Properties/ Alternatives		A1	A2	A3	A4	A5	A6
Coupling	DP1	0.00076, 0.0013, 0.10079	0.05006, 0.11004, 0.17200	0.05001, 0.10004, 0.16008	0.03100, 0.07800, 0.14700	0.03000, 0.08002, 0.15100	0.00036, 0.07002, 0.16200
Cohesion	DP2	0.04002, 0.00080, 0.16900	0.02009, 0.00067, 0.15800	0.00036, 0.07002, 0.16200	0.01009, 0.05002, 0.13500	0.01600, 0.05000, 0.13700	0.05004, 0.10020, 0.26000
Polymorphism	DP3	0.05009, 0.10018, 0.24000	0.04007, 0.10009, 0.24300	0.05004, 0.10020, 0.26000	0.02007, 0.08000, 0.19700	0.015004, 0.0006, 0.17800	0.04003, 0.09600, 0.19600
Encapsulation	DP4	0.07007, 0.13001, 0.23000	0.06005, 0.10023, 0.22800	0.04003, 0.09600, 0.19600	0.01007, 0.05900, 0.15200	0.04009, 0.10008, 0.22100	0.04000, 0.09005, 0.24200
Inheritance	DP5	0.07000, 0.12006, 0.27005	0.00054, 0.11006, 0.27800	0.04000, 0.09005, 0.24200	0.05009, 0.12001, 0.29600	0.04001, 0.10000, 0.20060	0.02007, 0.08000, 0.19700
Abstraction	DP6	0.00044, 0.08008, 0.18002	0.04001, 0.09005, 0.19800	0.06001, 0.12001, 0.23300	0.03400, 0.09001, 0.20000	0.000032, 0.00089, 0.20000	0.01007, 0.05900, 0.15200
Design-Size	DP7	0.10073, 0.18000, 0.34000	0.10002, 0.10037, 0.29900	0.11004, 0.14400, 0.30600	0.12500, 0.15005, 0.34400	0.11006, 0.15007, 0.34400	0.05009, 0.12001, 0.29600

These all calculations are done on one project and impact of attribute is calculated and ranks are prioritized. Similarly work has been done on 6 different-different projects and result is represented in below **table 8** as the degree of satisfaction.

Table 8. Closeness coefficient to the aspired level among the different alternatives

Alternatives		d+i	d-i	Gap Degree of CC+i	Satisfaction Degree of CC-i
Project 1	A1	1.254875	1.335553	0.51556	0.482484
Project 2	A2	0.697854	0.84550	0.54557	0.455484
Project 3	A3	0.785745	1.48554	0.65554	0.345746
Project 4	A4	2.1675847	1.48554	0.40557	**0.6987593**
Project 5	A5	2.0045895	1.53556	0.43554	0.5587466
Project 6	A6	0.4457885	0.39550	0.46555	0.6584535

DISCUSSION

In this Paper, the MCDM methodology was acknowledged to calculate the prioritization of security attributes corresponding to its weighted values. A model is proposed to evaluate the impact and their priority. **Table 8** shows the degree of satisfaction which evaluated after calculation of AHP and TOPSIS that sets priority. This table is achieved by the mathematical statement (22 to 26). The highest degree of satisfaction shows the highest priority which means it has highest impact on the model which is shown in below graph and it has to be critically handled when we developing a software.

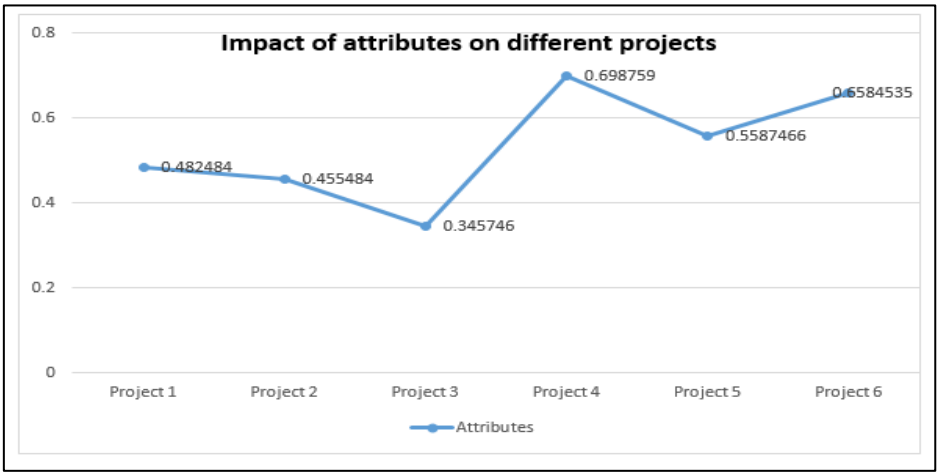

Figure 4. Impact of attributes

From the above figure it has been concluded that A4 attribute has highest impact on project and A3 has lowest impact. According to these results risks are handled and secure software is developed. The opinion on all the 7 security attributes has been gathered through the experts by the questionnaire. The experts came from software industries and academics field of research who perfectly understands the present scenario of security. By utilizing these opinions weights are calculated using hybrid methodology and its mathematical formulas and rankings are given to each attributes. Hence to develop secure software these attributes and their priorities should be considered carefully. The findings of this study is discussed below-

- Using requirement engineering to assess security will allow developers to focus on customer satisfaction.
- The fuzzy AHP-TOPSIS method and their mathematical statements, quantitative evaluation has been done which will help in setting the priorities and calculating rank of each attributes.
- On the basis of rank of the security attributes the impact factor can be measure which will minimize and handled critically while developing the software.

- These ranks and impact factor helps to develop guidelines for developing to check their software prior to launch in the market and develop highly secure software.

CONCLUSIONS

This study provides a comprehensive evaluation of security risks in requirements engineering by analyzing seven software development projects. The findings reveal that a significant number of these systems are at high security risks, underscoring an urgent need for improved mitigation strategies. To prioritize and analyze the impact of these risks, the study introduces a novel hybrid approach combining the fuzzy AHP TOPSIS. This methodology, applied for the first time in the software and information systems domain, demonstrates its effectiveness in determining the severity and prioritization of security risks. The proposed fuzzy AHP-TOPSIS framework offers valuable insights into the hierarchical structure of risk factors and their comparative impact, paving the way for more informed decision-making in security risk management. Despite its contributions, the study acknowledges certain limitations, such as the exclusion of some factors and attributes, which provide scope for future exploration. This research opens new avenues for addressing unresolved issues in security risk assessment, offering a robust foundation for enhancing security measures in software development practices.

REFRENCES

[1] A.S. Alfakeeh, A. Almalawi, F.J. Alsolami, Y.B. Abushark, A.I. Khan, A.A.S. Bahaddad, A. Agarwal, R. Kumar and R.A. Khan "Hesitant fuzzy-sets based decision-making model for security risk assessment," Computers, Materials & Continua, vol.70, no.2, pp. 2297–2317, 2022.

[2] A.S. Alfakeeh, A. Almalawi, F.J. Alsolami, Y.B. Abushark, A.I. Khan, A.A.S. Bahaddad, A. Agarwal, R. Kumar and R.A. Khan "Hesitant fuzzy-sets based decision-making model for security risk assessment," Computers, Materials & Continua, vol.70, no.2, pp. 2297–2317, 2022.

[3] S.A. Ansar, M. Faizan and M.W. Khan, "A Review on Some Pertinent Software Security Risk Management Frameworks," International Journal of Innovative Research in Science Engineering and Technology, vol.9, pp. 58-62, 2020.

[4] Y.B. Abushark, A.I. Khan, F.J. Alsolami, A. Almalawi, M.M. Alam, A. Agarwal, R. kumar and R.A. Khan, "Usability evaluation through fuzzy AHP-Topsis approach: security requirement perspective," Computers, Materials & Continua, vol. 68, no.1, pp. 1203–1218, 2021.

[5] A. Alharbi, W. Alosaimi, H. Alyami, M. Nadeem, M. Faizan, A. Agarwal, R. Kumar and R.A. Khan, "Managing software security risks through an integrated computational method," Intelligent Automation & Soft Computing, vol. 28, no.1, pp. 179–194, 2021.

[6] G. McGraw and B. Potter, "Software Security Testing [J]," IEEE Security & Privacy, vol.2, no.5, pp.81–85, 2004.

[7] J. Kaur, R.I. Khan, Y.B. Abushark, M.M. Alam, S.A. Khan A. Agarwal, R. Kumar and R.A. Khan, "Security Risk Assessment of Healthcare Web Application through Adaptive Neuro-Fuzzy Inference System: A Design Perspective," Risk ManagHealthc Policy, vol.13, pp. 355-371, 2020.

[8] G. Kotonya and I. Sommerville, "Requirements Engineering: Processes and Techniques," John Wiley & Sons, pp. 1-294, 1988.

[9] R. Fredriksen, M. Kristiansen, B. Gran, A.K. Stolen, T.A. Opperud and T. Dimitrakos, "The CORAS framework for a model-based risk management process," Proceedings of the 21st International Conference on Computer Safety, Reliability and Security (Safecomp 2002), LNCS 2434, pp. 94-105, Springer, 2002.

[10] M. Nazim, C. W. Mohammad, M. Sadiq, "A comparison between fuzzy AHP and fuzzy TOPSIS methods to software requirements selection," Alexandria Engineering Journal, Vol. 61, No. 12, pp. 10851-10870, 2022.

[11] Y. B. Abushark, A. I. Khan, F. J. Alsolami, A. Almalawi, M. M. Alam, A. Agrawal, R. Kumar, R. A. Khan, "Usability Evaluation Through Fuzzy AHP-TOPSIS Approach: Security Requirement Perspective," Computers, Materials and Continua, Vol.68, No.1, pp.1203-1218, 2021.

[12] K.Wang, Y. Hong, C. Li, "Fuzzy Risk Assessment Method for Airborne Network Security Based on AHP-TOPSIS," Computers, Materials and Continua, Vol. 80, No.1, pp. 1123-1142, 2024.

[13] A. Attaallah, K. al-Sulbi, A. Alasiry, M. Marzougui, S.A. Ansar, A. Agrawal, M.T.J. Ansari, R.A. Khan, "Fuzzy-Based Unified Decision-Making Technique to Evaluate Security Risks: A Healthcare Perspective," Mathematics, vol.11, no.11:2554, 2023.

[14] Y.C. Chou, H.Y. Yen, V.T. Dang and C-C. Sun, "Assessing the human resource in science and technology for Asian countries: Application of fuzzy AHP and fuzzy TOPSIS," Symmetry, vol.11, no.2, pp. 251-262, 2019.
[15] A. Agrawal, A.H. Seh, A. Baz, H. Alhakami, W. Alhakami, M. Baz, R. Kumar and R.A. Khan, "Software Security Estimation Using the Hybrid Fuzzy ANP-TOPSIS Approach: Design Tactics Perspective," Symmetry, vol. 12, pp.1-21, 2020.
[16] P. Gaunard and E. Dubois, "Bridging the Gap between Risk Analysis and Security Policies," In: Gritzalis, D., De Capitani di Vimercati, S., Samarati, P., Katsikas, S. (eds) Security and Privacy in the Age of Uncertainty, SEC, IFIP — The International Federation for Information Processing, Springer, Boston, MA, 2003, vol. 122.
[17] J.B. Bowles and C.E. Peláez, "Fuzzy logic prioritization of failures in a system failure mode, effects and criticality analysis," Reliab. Eng. Syst. Saf., vol.502, pp. 203–213, 1995.
[18] O. Gordieiev, V.S. Kharchenko and K. Vereshchak, "Usable security versus secure usability: An assessment of attributes interaction," In Proc. ICTERI, pp. 727-740, 2017.
[19] T.J. Ross, "Fuzzy Logic with Engineering Application," John Wiley & Sons, Ltd.: Hoboken, NJ, USA, 2010.
[20] J.J. Zhao and S.Y. Zhao, "Opportunities and threats: A security assessment of state e-government websites," Gov. Inf. Q., vol.27, pp. 49–56, 2010.
[21] W. Bai, D. Kim, M. Namara, Y. Qian, P.G. Kelley and M.L. Mazurek, "Balancing security and usability in encrypted email," IEEE Internet Comput., vol. 21, pp. 30–38, 2017.
[22] Confidentiality, Integrity, and Availability. Accessed: Dec.15, 2021. [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/Security/Information_Security_Basics/Confidentiality, Integrity, _and_Availability.
[23] J. Zeng, M. An and N.J. Smith, "Application of a fuzzy-based decision-making methodology to construction project risk assessment," Int. J. Proj. Manage, vol. 256, pp. 589–600, 2007.
[24] D.Y. Chang, "Applications of Extent Analysis Method on Fuzzy AHP," European Journal of Operational Research, vol.95, pp.649–655, 1996.
[25] K.K. Aggarwal and Y. Singh, "A book on software engineering," New Age International (P) Ltd, 2001.
[26] R.S. Pressman, "Software engineering: a practitioner's approach," Palgrave Macmillan, 2005.
[27] Y. Asnar and P. Giorgini, "Risk Analysis as part of the Requirements Engineering Process," Trento, Italy, Via Sommarive 14, March 2007.
[28] C.C. Lin, S.C.; Chen and Y.M. Chu, "Automatic price negotiation on the web: An agent-based web application using fuzzy expert system," Expert Systems with Applications, vol. 38, no. 5, pp. 5090-5100, 2011.
[29] D-Y. Chang, "Applications of the extent analysis method on fuzzy AHP," Eur J Oper Res, vol. 95, pp. 649–655, 1996.
[30] C-H. Cheng, "Evaluating naval tactical missile systems by fuzzy AHP based on the grade value of membership function," Eur J Oper Res, vol. 96, pp. 343–350, 1997.
[31] B.W. Boehm, "A spiral model of software development and enhancement," Computer, vol. 21, no. 5, pp. 61-72, 1988.
[32] R. Nagpal, D. Mehrotra, P.K. Bhatia and A. Sharma, "Rank University Websites Using Fuzzy AHP and Fuzzy TOPSIS Approach on Usability," IJIEEB, vol.7, no.1, pp.29-36, 2015.