Computers, Materials & Continua
DOI:10.32604/cmc.2022.024903
Article

Tech Science Press

Sustainable-Security Assessment Through a Multi Perspective Benchmarking Framework

Ahmed Saeed Alfakeeh[1], Abdulmohsen Almalawi[2], Fawaz Jaber Alsolami[2], Yoosef B. Abushark[2], Asif Irshad Khan[2,*], Adel Aboud S. Bahaddad[1], Md Mottahir Alam[3], Alka Agrawal[4], Rajeev Kumar[5] and Raees Ahmad Khan[4]

[1]Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[2]Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[3]Department of Electrical and Computer Engineering, Faculty of Engineering, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[4]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow-226025, Uttar Pradesh, India
[5]Department of Computer Science and Engineering, Babu Banarasi Das University, Lucknow-226028, Uttar Pradesh, India
*Corresponding Author: Asif Irshad Khan. Email: aikhan@kau.edu.sa
Received: 03 November 2021; Accepted: 07 December 2021

Abstract: The current cyber-attack environment has put even the most protected systems at risk as the hackers are now modifying technologies to exploit even the tiniest of weaknesses and infiltrate networks. In this situation, it's critical to design and construct software that is both secure and long-lasting. While security is the most well-defined aspect of health information software systems, it is equally significant to prioritise sustainability because any health information software system will be more effective if it provides both security and sustainability to the customers at the same time. In this league, it is crucial to determine those characteristics in the systems that can help in the accurate assessment of the sustainable-security of the health information software during the development stage. This research work employed the Fuzzy Analytic Network Process (Fuzzy ANP) to estimate the impact of the overall sustainable-security of health information software systems and their characteristics in order to achieve a high level of sustainable-security. Furthermore, the study validates the efficacy of the Fuzzy ANP procedure by testing it on five different versions of a health information software system through Fuzzy Technique for Order of Preference by Similarity to Ideal Solutions (Fuzzy TOPSIS). Despite the sensitivity of the health information software systems, this study employed multiple versions of health information software system. When compared with the existing procedures for testing the sustainable-security of health information software systems, the outcomes were conclusive and significantly more effective. Besides saving time and resources, the mechanism suggested in this research work aims to establish

an outline that software practitioners can follow to enhance the sustainable-security of health information software systems.

Keywords: Sustainable-security; sustainable health information software systems; analytic network process; fuzzy logic

1 Introduction

The primary goal of all the developers is to secure health information software systems from harmful assaults in long-term situations. While the establishment, identification, and estimation procedures can achieve security objectives, maintaining sustainability in the same measure necessitates the use of highly effective strategies at an early stage in the development procedure of health information software systems [1]. Furthermore, the goals of secure software systems must always be in line with the requirements of the consumer. However, the consumer of the systems is often the poor link, unknowingly inviting attacks. This call for procedures capable of eradicating potential vulnerabilities at all levels. Thus, it's critical to enlist and validate the best practices for estimating the long-term viability and security of a health information software system. Such a framework of established mechanisms would be a credible and accurate reference for the developers. Furthermore, following these principles early in the development life cycle would help in enhancing the sustainable-security of healthcare information systems.

The evolution of security and sustainability in the online application of all healthcare related operations occurred in the preceding few years of the twentieth century [2]. According to a survey [3], there has been a noticeable enhancement in developers' attempts to upgrade their overall security mechanisms to include sustainability at the early stage of health information software system development. However, designing this software is a difficult duty that may entail failures. Some of the reports on the failure of the security of the health information software systems need a mention in this context. To quote a few examples of the same, a report cited that significant data, including the names, phone numbers, and addresses of 1157 scholars, was leaked. According to another report, attackers attempted to breach the health information software systems more than 70 times during an institution's entrance exams [4]. These outcomes demonstrate a growing need for sustainable-security, particularly in the health information software systems for an organization due to the large quantity of sensitive data involved, the loss of which could affect thousands.

Security experts are always working on strategies to improvise upon the health information software systems' sustainable-security and its overall security [5]. The major purpose of security is to prevent unwanted access, whereas sustainability focuses on maintaining uninterrupted consumer services [3]. The sustainable-security of the healthcare systems is estimated as a machine-related problem rather than an age or industry-related problem [6]. Hence, the company's focus is on maintaining sustainable-security, i.e., ensuring continuous security procedures till the health information software systems are employed. While the experts have attempted to estimate the sustainable-security of the software by using various procedures [4], the majority of the research done in this field does not address practical difficulties [3]. "Software sustainability, as segment of its consistency and associated to non-functional criteria," as Agrawal et al., put it, "is a means of strengthening security for health information software systems" [5].

Sustainability and security features are vital for developing a maintainable security of the health information software systems [7–9]. The main aspects that affect the sustainability and security of health information software systems are confidentiality, integrity, availability, and energy consumption, as well as software-based resource management, perdurability. Each of these are included in security and sustainability characteristics [10–13]. The importance of these features in maximising the health information software system's sustainable-security cannot be overstated. Furthermore, no evaluation can be completed without taking into account the aforementioned features. The evaluations based on these indices would be more efficient and trustworthy. In the same row, it is critical to recognise that estimating sustainable-security is an issue of decision-making because each organisation adopts its own procedures and regulations, thus involving the process of taking judicious decisions for analyzing the security of its software systems [14–19].

The majority of research done to date hasn't employed the characteristics of both sustainable-security for assessing the efficacy of the health information software systems. As an outcome, an additional operational approach for evaluating the health information software systems' sustainable-security is required, allowing specialists to discern between preferences of qualities. Designing a health information software system with security-sustainability for an organisation is a multi-step decision-making procedure involving several people. The Multi-Criteria Decision-Making (MCDM) procedure is important in merging the judgement of various experts into a single frame [20–26]. The MCDM is a set of procedures to address issues relating to sustainable and renewable energy, according to Calabrese et al. [6]. The researchers analyzed the restrictions for implementing sustainable and green technologies using the Fuzzy ANP-TOPSIS procedure. This procedure encompasses a range of quite varied procedures. Furthermore, Fuzzy MCDM is a well-known approach for estimating, predicting, and resolving flaws from several perspectives. The evaluation facilitates any selection that identifies the options while ensuring sustainable-security of healthcare systems.

The rest of the document is built in the same way: Following the introduction in the first unit, the second unit discusses some of the relevant work in the areas of MCDM, sustainability, and security in the linked work section. A hierarchy that acknowledges the characteristics that affect sustainability and security must be constructed. In this context, the third section of the study is dedicated to sustainable-security and the hierarchy of its qualities. The Fuzzy ANP-TOPSIS is employed to compute the health information software system's sustainable-security. Authors have used the Fuzzy ANP-TOPSIS technique in the current research work to estimate the sustainable-security; as explained in the procedure section. The fifth section of the study includes data processing, sensitivity analysis, and final outcomes on six versions of the hospital's software. The overall findings will assist the security designers in adding sustainable-security into health information software systems during the development procedure. In the sixth section, the outcomes are compared with the earlier research investigations done in this regard. Finally, in sections seven and eight, respectively, the discussion and conclusion are listed. Main contributions of this study are as follows:

- To carry out the in-depth study of health information software systems' sustainable-security, i.e., in health information software systems' perspective, security and sustainability impacts are analyzed in terms of weakness and strength.
- To conduct implementations through Fuzzy ANP to estimate the most noteworthy features of health information software systems sustainable-security.
- The performance of the health information software system's sustainable-security has been estimated on six different healthcare systems by using Fuzzy TOPSIS.
- To show the efficacy of our proposed clarification by accompanying sensitivity analysis on the estimated outcomes.

- Comparisons between the estimated outcomes in the present research work and the earlier techniques have been done to highlight on the profits of the current contributions.

2 Literature Review

Sustainable-security focuses on safe end-user health information software systems services, which have already become a top priority for every industry; nonetheless, there is still much more to be done in this area. A research involving 4000 specialists was conducted by the Global Executive Report on Sustainability [6]. According to the study, 65% of the defendants agreed that the goals of sustainability obliged them to use health information software systems security models that were freely accessible, regardless of whether the programme was protected or not. Evidently, health information software systems security is commonly overlooked, despite the fact that it is critical during the design phase. The majority of security specialists rely on simple network architecture and rudimentary frameworks [7], thus jeopardizing the data of the consumers. There should be no loophole or possibilities of errors in either security or sustainability while designing health information software systems for an organisation where data, time, and large assets are at risk. Hence to eliminate vulnerabilities, the examination of sustainable-security of the institutional health information software systems architecture becomes essential. In reality, the impact of sustainability on design characteristics should be quantified. The following are some of the most important research sources that we referred to during our research:

Calabrese et al. [6] talk about both sustainability and security in their work on responsible software engineering. The authors also explore numerous aspects of responsible software engineering, including design for sustainability. This paper proposes ethical standards for software engineering.

Agrawal et al. [5] evaluated the sustainable-security of healthcare systems using a multi-criteria decision-making tactics based on fuzzy logic in 2020. Four key parameters of confidentiality, integrity, availability, and longevity were identified and estimated to determine the results. The outcomes were compared to those of other multi-criteria decision-making procedures.

Calero et al. [7] wrote a paper in 2019 related to the sustainable-security of health information software systems. The paper was divided into three sections including economic viability, environmental, and human, respectively. According to the authors, perdurability as a sustainability quality, as well as coupling and cohesion of design elements are crucial characteristics that have a major impact on the security of health information software systems.

Calero et al. [8] proposed a library of health information software systems sustainability designs to aid the developers in creating a long-lasting health information software systems that meets the expectations of consumers. The evaluations of current and prior studies linked to sustainable health information software systems were employed to compile this catalogue. An outline was also presented in this effort, which featured a set of sustainability targets in terms of quality and security. According to a report, the availability and durability of sustainability features, as well as the encapsulation, heredity, and abstraction of design traits, are important qualities that have a major impact on sustainability.

Kumar et al. [9] developed a sensitive procedure for detecting and mitigating denial of service attacks on cloud-based services based on a rate limit tactic with minimum overhead. The relationship between security, stability, and sustainability was discussed in the essay, which is essential for the twenty-first century. Researchers combined three areas of research: security, sustainability, and health. They also came up with an innovative way for determining availability.

A study on the role of health information software systems in sustainable architectural design was published in 2013 by Calero et al., and team [10]. The authors of this paper chose to focus on specific sustainability opportunities in order to propose research approaches that would emphasise the issue of architectural sustainability. The researchers also mentioned that it was only recently decided to incorporate sustainability in software design as a research theme.

Calero et al. [11] expanded an edge computing procedure for mobile that is built on a security configuration based on fuzzy theory in 2019. A security intermediary was added in the paper, which was comparable to typical security capabilities. To achieve numerous optimal potentials and the finest order of the needed security facilities, the researchers presented a procedure based on a Fuzzy Inference Scheme (FIS). Because of FIS, the findings demonstrated effective performance.

Kumar et al. [12] proposed the idea of combining sustainable software design and development. Divergent viewpoints and programmes on design for longevity were also discussed in the report. Li et al. [13] discussed the possibility of using Facebook to promote public healthcare related information and enhance services in 2017. The work looked at the advantages and disadvantages of adopting such a forum as a tactic for healthcare initiatives in perspective of public. According to the findings, Facebook is a right potential resource for supporting software 2.0 e-health services, and that security and sustainability attributes interact or are interlinked.

Luthra et al. [14] focussed the most important software risk that must be estimated in advance for to developing an appropriate risk management and deliberate mitigation plan of risk. The research work outlined some of the most significant concerns from a long-term security standpoint, as well as a map that depicted the rigorousness of each attribute, such as integrity, availability, and confidentiality. To estimate, mitigate, and enhance sustainable security, the study employed linear programming and fuzzy optimization procedures.

Mardani et al. [15] looked at 54 studies in 2015 that had used multiple MCDM procedures. The studies were divided into different categories based on procedures, years of publication, and two categories: renewable and sustainable strength. Finally, the scholars highlighted that the number of submissions had increased from preceding years, and that new MCDM approaches, such as Fuzzy ANP-TOPSIS, Fuzzy ANP-VIKOR, and others, had been identified.

While much has been written about sustainability in the past, we discovered that the recommended security and sustainability estimation procedures in the existing references lacked a configuration for evaluating sustainability with preferable design qualities. The proposed plan in this study will be a watershed moment in sustainability study by achieving higher environmental security in the health information software systems for a hospital. During the creation of a health information software system, a quantitative evaluation of sustainable-security is required. In addition, the goal of this research is to evaluate the security of six modified versions of locally produced healthcare institutional software. For our study, we analysed the security of the software being used in Sanjay Gandhi Postgraduate Institute of Medical Sciences, Lucknow, India. The Fuzzy ANP procedure, as outlined in the next section, was utilised to estimate the sustainable-security of the health information software.

3 Sustainable-Security of Health Information Software Systems

Managing security of healthcare systems is a procedure for preventing malicious assaults from a variety of hostile goals and clients [23–26]. With the rapid growth of health information software systems, security as a key feature in a sustainable environment is becoming increasingly diverse

[27–29]. Mikhailov's intent on health information software systems security is applicable in this situation [30]. A stable health information software systems, according to the study, entails developing a health information software systems to make it safe and secure, ensuring that the health information software systems remains reliable, and educating health information software systems engineers and end-users on how to design secure health information software system [20]. Adapting environmentally friendly procedures to create existing goods and services sustainable and viable is now a commercial and social requirement [21]. The concept of balancing sustainability and security as a bottom line concept for health information software systems security is not commonly acknowledged. Additionally, numerous practitioners argue that reliability cannot be negotiated while dealing with the security of healthcare systems.

One of the most credible approaches to create efficient and stable health information software systems is to estimate and maintain CIA in a secure environment during health information software systems development [22]. Because of the significance of sustainable-security in health information software systems nowadays, everyone must ensure security. Security monitoring, on the other hand, necessitates a high level of sophistication, which renders solutions less scalable, complex, and reusable. This is a major worry for lengthier health information software systems services, and it is harming long-term software. Sustainability, according to Penzenstadler et al., must be considered high quality amongst the other essential criteria such as security, performance, reliability, and durability [23]. Because of the enhancing number of security risks, money theft, and personal frauds, sustainable-security is becoming a top priority [24]. Organizations that develop health information software systems nowadays must concentrate on both security and sustainability.

As a leading technology company, Robillard, M. P., defines longevity as "the quantity of how strong a system is to secure a product and meet its set duties" [25]. Furthermore, sustainable software has a negligible impact on culture, economics, human beings, and climate as a result of diverse types of development and implementation, and has a beneficial impact on the environment through its use [26]. "Sustainable software development," as Sahu, K., & Srivastava, R. K., put it, "seeks to meet the needs of consumers while protecting the natural systems and the environment" [28]. Recognizing the qualities that contribute to both can help define the link between security and sustainability. In addition, Fig. 1 depicts a hierarchy of sustainable-security attributes.

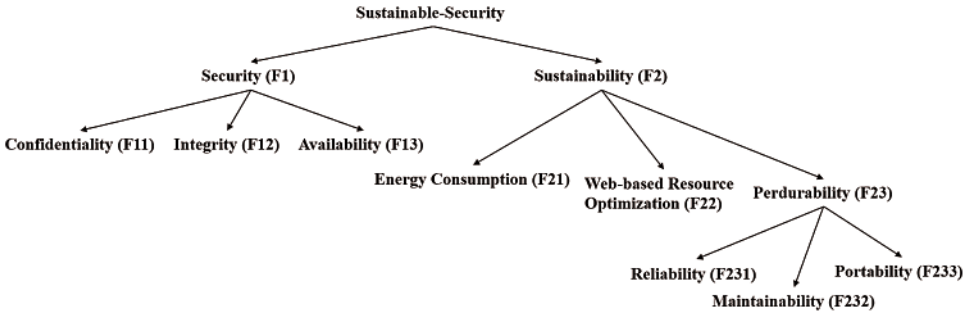

Figure 1: A tree of sustainable-security characteristics

Fig. 1 depicts how the health information software system's sustainable-security is affected by availability, and integrity, confidentiality, and energy consumption, as well as perdurability and software-based resource optimization. Collaboration between characteristics can enhance sustainable-security [29]. Therefore, while determining the sustainable-security of the health information software

systems, the above features will be considered. The following are definitions and interpretations of sustainable-security characteristics:

Security (F1): Security of health information software system is an important feature that protects the healthcare related systems from destructive attacks and various hazards engineered by the hackers and malicious information, ensuring that the software continues to function effectively in the face of potential threats. Security is also necessary for facilitating giving secrecy, authentication, and availability [29]. These characteristics, on the other hand, must be combined with the concept of sustainability.

Sustainability (F2): Sustainability is defined as meeting the current demands of the customer without jeopardising the capability of future generations to meet their own needs [30]. Security of health information software system that is built sustainably could aid in reaching life's sustainability goals. Furthermore, security technologies have a greater impact on our day-to-day life. Thus, combining security and sustainability will provide the world with secure and sustainable health information software system.

Confidentiality (F11): Confidentiality can be characterised in terms of security as guaranteeing that sensitive information can only be used by the individuals who are authorized to access the same while also confirming the data of the intended consumer [31]. Furthermore, confidentiality is a characteristic that impacts security and is linked to sustainable-security. Hence, it has an impact on sustainable-security in several ways.

Integrity (F12): Maintaining the reliability of the information is what integrity is all about [32]. Maintaining integrity enhances the sustainable-security. Therefore, it is incorporated as a well-informed quality of sustainable-security. Integrity plays a crucial part in achieving sustainable-security. The quantitative estimation of sustainable-security will aid in ensuring the long-term viability of secure health information software system.

Availability (F13): Availability confirms that knowledge is accessible to permitted consumers in a sustainable environment. If the hackers are not permitted to compromise on integrity and confidentiality, they can try to bring down the server [33] and make the data unavailable for a short period of time. This has a negative impact on the sustainable-security of health information software system. Thus, availability must be considered while evaluating sustainable-security.

Energy Consumption (F21): In sustainable-security, energy consumption refers to the degree to which the quantity of energy is required by a healthcare system to fulfill its security activities for meeting the security standards [34]. When considering sustainable-security, this is an important sustainability concept to consider.

Software-based Resource Optimization (F22): Software-based resource management is a set of prototypes and strategies for aligning existing resources, such as equipment, money, and human resources, with the organization's security standards in order to accomplish well-known security and sustainability objectives. The term "resource optimization" refers to accomplishing the preferred outcomes within the budget and set time while using the fewest resources possible [35].

Perdurability (F23): It is the idea of creating adaptable, recyclable, and long-lasting, sustainable information security products, i.e., those characteristics that allow data to subsist for a long time while maintaining its quality-related functioning [36,37]. Perdurability is a feature of sustainability, but it also has an impact on security. This makes it a crucial feature in the context of sustainable-security in healthcare systems perspective.

Reliability (F231): The degree to which sustainable-security of health information software system functions safely in a specific sustainable environment for a set amount of time is characterized as reliability [5]. In every scenario, reliability is either 1 or 0. Hence, reliable sustainability is entirely dependent on sustainable-security.

Maintainability (F232): The degree of effectiveness and efficiency with which the intended creators can update the health information software system to preserve sustainability is maintainability [6]. It's the degree to which healthcare system has been corrected or comprehended. Maintainability is a health information software system notion that can also be employed to gauge sustainable-security.

Portability (F233): Portability can be explained as the degree of efficiency and efficacy with which health information software system and its security may be moved from one software product to another [7]. In sustainable-security, the efficacy of shifting security applications from one location to another is measured as portability.

Developers in the fields of computer sustainability and security must learn to work with shared-environment ideas [8]. This is due to the fact that security and sustainability may coexist together. Despite the fact that several strategies for merging the two have been devised, each procedure has its own set of limits and benefits [9]. Sustainability in security must be incorporated into sustainable-security at the very beginning of development and must be maintained before security services are put in place [10–13]. All the ambiguities that exist between sustainability and security appear to be due to sustainability. The sustainable-security evaluation proposed in this work considers the weights and constraints of both the procedures and proposes a way to achieve increased levels of sustainability while maintaining security.

4 Methodology

The framework within which a researcher does research is known as research methodology [17,18]. The research methodology used in this research work to estimate the sustainable-security of healthcare systems is based on fuzzy ANP-TOPSIS technique, a popular MCDM tactic. The weights of the characteristics and their dependencies on every ANP network are estimated using Fuzzy-ANP. In the end, the TOPSIS approach is used to rank the alternates. The following is a detailed explanation of these techniques.

Fuzzy-Analytic Network Process (F-ANP): Srivastava et al. [33] created the term "fuzzy logic," which is an enhanced variant of classical logic based on fuzzy-set theory. All hesitations in an issue where determining the solution is difficult, or are considered to be either entirely true or completely false can be resolved by fuzzy logic. To handle and address imprecise and uncertain data in decision-making situations, it considers 1 and 0 as two extreme cases of truth and denotes various cases in between 1 and 0 [14,15]. In decision-making difficulties, the ANP is a multi-criteria decision analysis technique. It's a broadening of the AHP [17]. T.L. Saaty developed the Analytic Hierarchy Process (AHP) approach for MCDM problems, but due to the limitation of not evaluating probable relationships among the criteria [27], T.L. Saaty later presented ANP to overcome the constraint of AHP [26]. To answer issues with dependencies, ANP depicts the dependencies among criteria or options [17,18]. Because dependencies and interactions among the problem's features are portrayed in a network, AHP is signified by a hierarchy, whereas ANP is showed by a network [17]. The overall impact of these dependencies on the network is also determined by ANP. ANP also uses loops to describe interdependencies between elements of the same cluster, as well as feedback between clusters in the same network [18]. The fuzzy-ANP approach combines fuzzy logic and ANP to manage imprecise data and improve the precision and accuracy of the outcomes.

Fuzzy-TOPSIS Method: F-TOPSIS was discussed by Kumar et al., to tackle MCDM problems using a multi-criteria decision analysis technique [18–21]. TOPSIS has been determined to be the greatest approach belong to multi-criteria decision making techniques for addressing the rank reversal problem, defining that when a non-optimal alternative is discovered, the alternative ranking can be modified [22–25]. TOPSIS' key notion is that the best alternative among all competing alternatives should be the furthest away from PIS and the furthest away from NIS [26–28]. PIS maximizes benefit criteria while minimising cost criteria, whereas NIS maximizes cost criteria while minimising benefit criteria [29–31]. TOPSIS is the most well-known method for MCDM problem alternative rankings. The authors of this paper apply a fuzzy-ANP TOPSIS hybrid technique to evaluate the sustainable-security of health information software systems, resulting in precise, accurate, and efficient results. The Fuzzy ANP-TOPSIS approach's step-by-step technique for analysing weightage and ranking is outlined below, and Fig. 2 depicts an overview of the study's total work.

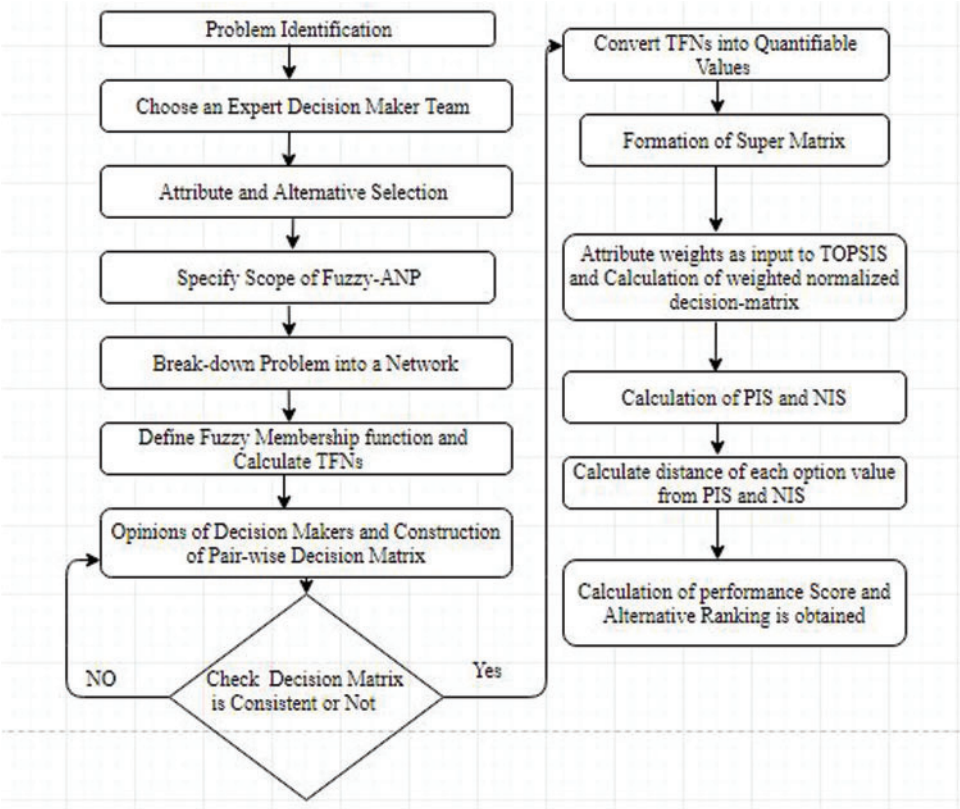

Figure 2: Flow chart of fuzzy ANP-TOPSIS tactic

Triangular Fuzzy Numbers were created after language concepts were translated into crisp numeric values (TFN). TFN can be written as (c1, c2, c3), where (c1 c2 c3) and c1, c2, c3 are parameters representing the TFN's smallest, middle, and biggest values, respectively. Assume A is a fuzzy number, and its membership function can be well-defined as shown in Fig. 3 [26] using Eqs. (1) and (2).

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

$$\mu_A(x) = \begin{cases} \dfrac{x - \mathrm{c1}}{\mathrm{c2} - c1}, & c1 \le x \le c2 \\ \dfrac{c3 - x}{c3 - c2}, & c2 \le x \le c3 \\ 0, & x > c3 \quad \textit{Otherwise} \end{cases} \tag{2}$$

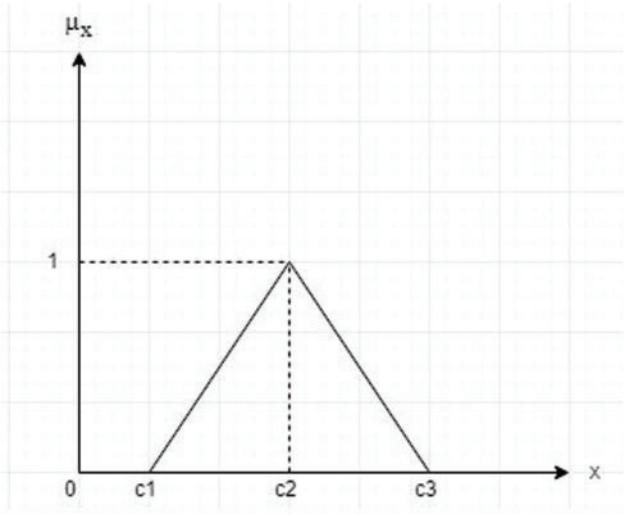

Figure 3: Triangular fuzzy number

Experts and practitioners use the fundamental scale (Tab. 1), known as the Saaty Scale [27], to give language terms to the criteria first, followed by their quantitative values. Numeric values are afterwards transformed into fuzzy numbers.

Table 1: Fuzzy triangular scale

Numeric Value	Fuzzy Triangular Scale (Saaty Scale)	
1	Equally important	(1, 1, 1)
3	Weakly important	(2, 3, 4)
5	Fairly important	(4, 5, 6)
7	Strongly important	(6, 7, 8)
9	Absolutely important	(9, 9, 9)
2	Intermittent values between two	(1, 2, 3)
4	adjacent scales	(3, 4, 5)
6		(5, 6, 7)
8		(7, 8, 9)

Eqs. (3)–(6) are used to determine the triangular fuzzy number, which is written as (c1ij, c2ij, c3ij), where c1ij signifies low importance, c2ij signifies intermediate importance, and c3ij signifies high

importance. TFN [η ij] is further definite as follows:

$$\eta_{ij} = (c1_{ij},\ c2_{ij},\ c3_{ij}) \tag{3}$$

Where, $c1_{ij} \le c2_{ij} \le c3_{ij}$

$$c1_{ij} = min(J_{ijd}) \tag{4}$$

$$c2_{ij} = (J_{ij1}, J_{ij2}, J_{ij3})^{\frac{1}{x}} \tag{5}$$

and $$c3_{ij} = max(J_{ijd}) \tag{6}$$

Jijk denotes the relative significance of the values between the two features indicated in the equations above, as determined by practitioner judgement. Where I and j indicate a pair of expert-selected qualities. The geometric mean of practitioner views for a given comparison is used to calculate TFN (η ij). Eqs. (7)–(9) also aid in the aggregation of triangular fuzzy number values. A1 and A2 are two TFNs, with A1 equaling (c11, c21, c31) and A2 equaling (c11, c21, c31) (c12, c22, c32). The following are the operating guidelines for them:

$$(c1_1,\ c2_1,\ c3_1) + (c1_2,\ c2_2,\ c3_2) = (c1_1 + c1_2,\ \ c2_1 + c2_2,\ c3_1 + c3_2) \tag{7}$$

$$(c1_1,\ c2_1,\ c3_1) \times (c1_2,\ c2_2,\ c3_2) = (c1_1 * c1_2,\ \ c2_1 * c2_2,\ c3_1 * c3_2) \tag{8}$$

$$(c1_1,\ c2_1,\ c3_1)^{-1} = \left(\frac{1}{c3_1}, \frac{1}{c2_1}, \frac{1}{c1_1}\right) \tag{9}$$

The responses from the decision makers are used to create a pair-wise comparison matrix. The CI is deliberated using the formula in Eq. (10), which is as follows:

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

where CI stands for Consistency Index and t denotes the number of pieces to be compared. The following is a random index-based estimate of the Consistency Ratio (CR) (Eq. (11)):

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

If CR is less than 0.1, the produced matrix is fairly consistent. The random index is abbreviated as RI. Saaty [26] is the source of the random index.

TFN values are turned to measurable values using the defuzzification process after generating a generally consistent matrix. The alpha-cut approach, as described in Eqs. (12)–(14), is the defuzzification method used in this study, which is based on [17,28].

$$\mu_{\alpha,\beta}(\eta_{ij}) = [\beta.\eta\alpha(c1_{ij}) + (1-\beta).\ \eta\alpha(c3_{ij})] \tag{12}$$

where, $0 \le \alpha \le 1$ and $0 \le \beta \le 1$

Such that,

$$\eta\alpha(c1_{ij}) = (c2_{ij} - c3_{ij}).\alpha + c1_{ij} \tag{13}$$

$$\eta\alpha(c3_{ij}) = c3_{ij} - (c3_{ij} - c2_{ij}).\alpha \tag{14}$$

For practitioners' preferences, α and β are employed in the above equations, also α and β values vary between 0 and 1.

This stage involves constructing the super-matrix, which is the outcome of the priority vector derived through paired group comparisons, and includes goals, characteristics, sub-characteristics, and alternatives. The usual form of super matrix [18] is shown Eq. (15).

$$W = \begin{array}{c} \\ \\ C_1 \\ \\ \\ \\ C_n \\ \\ \end{array} \begin{array}{c} \begin{array}{c} e_{11} \\ e_{11} \\ \vdots \\ e_{1m_1} \\ \\ \vdots \\ e_{n1} \\ e_{n2} \\ \vdots \\ e_{nm_n} \end{array} \\ \begin{bmatrix} W_{11} & W_{12} & \dots & W_{1n} \\ W_{21} & W_{22} & \dots & W_{2n} \\ \vdots & \vdots & \dots & \vdots \\ W_{n1} & W_{n2} & \dots & W_{nm} \end{bmatrix} \end{array} \tag{15}$$

where Cn is the nth cluster, emn denotes the mth element of the nth cluster, and Wij denotes the principal eigenvector.

TOPSIS uses Eq. (16) to normalise the entire decision matrix in order to determine the performance rating of each alternative over each normalised characteristic through Tab. 2.

$$X_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}} \tag{16}$$

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

Table 2: Rating scale

Linguistic Variables	Corresponding TFN
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)

Next, the assessment of the Normalized Weighted-Decision Matrix is implemented through Eq. (17).

$$M_{ij} = w_i X_{ij} \tag{17}$$

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

Assessment of negative-ideal solution I_ matrix and positive-ideal solution I+ matrix are performed through Eq. (18).

$$I^+ = z_1^+, z_2^+, z_3^+ \ldots..z_n^+$$

$$I^- = z_1^-, z_2^-, z_3^- \ldots..z_n^- \tag{18}$$

where, max zij if j is an advantage and Min zij if j is a cost characteristic, or Min zij if j is an advantage and Min zij if j is a cost feature.

The following step is to calculate the distance between each option value and the negative-ideal solutions and positive-ideal solutions Eqs. (19) and (20):

Positive ideal solution:

$$D_i^+ = \sqrt{\sum_{j=1}^{m} (z_i^+ - z_{ij})^2}\ ; i = 1, 2, 3 \ldots.m \tag{19}$$

Negative ideal solution:

$$D_i^- = \sqrt{\sum_{j=1}^{m} (z_{ij} - z_i^-)^2}\ ; \quad where,\ i = 1, 2, 3 \ldots.m \tag{20}$$

where the distance from one is option to the positive-ideal solution and is the distance from one option to the negative-ideal solution. Calculating the value of each alternative's performance (Pi) (Eq. (21)).

$$P = \frac{D_i^-}{D_i^- - D_i^+} \tag{21}$$

where, i= 1, 2, 3 . . . .m

Using the Fuzzy-ANP TOPSIS technique with a varying number of options, the above-defined step-by-step process will be performed to estimate the sustainable-security of healthcare systems. The following part conducts a case study and provides a numerical analysis.

5 Numerical Analysis and Outcomes

Because sustainable-security assessment is primarily a qualitative metric, quantifying the sustainable-security of health information software systems is a complex and difficult task. Prioritizing quality features during the development process of health information software systems is critical for building secure and long-lasting software products. Using fuzzy ANP-TOPSIS, this research work presents a tactic for estimating the sustainable-security security of healthcare systems. Two level 1 criteria, namely security and sustainability, are represented as F1 and F2, respectively, for determining the sustainable-security of health information software systems. Confidentiality, integrity, and availability are symbolized as F11, F12, and F13, respectively, in terms of sustainable-security of health information software systems at level 2. Energy consumption, software-based resource

optimization, and perdurability are symbolized as F21, F22, and F23, respectively, in terms of sustainable-security of health information software systems at level 2. The features of perdurability in terms of level-3 sustainable security include reliability, maintainability, and portability, which are represented as F231, F232, and F233, respectively. The following Eqs. (1)–(21) were used to estimate the sustainable-security of health information software systems using Fuzzy-ANP-TOPSIS:

Authors obtained the numeric values from linguistic values and then accumulated triangular fuzzy numbers using the standard Saaty scale shown in Tab. 1 and Eqs. (1)–(9). To transform the crisp numerical values into fuzzy TFN numbers, Eqs. (3)–(6) were used. The level-1 criteria pair-wise comparison matrixes are then calculated and shown in Tab. 1. After that, the consistency index and random index were calculated using Eqs. (10)–(11). The pair-wise comparison matrix's random index is less than 0.1, indicating that our pair-wise matrix is consistent. Further, Eqs. (7)–(9) are employed for intermediate operations on fuzzy numbers, such as multiplication, reciprocal, and addition. These intermediate operations are not presented in the current research work because they would exceed the study's page limit. In addition, local weights and normalised values of level-1 characteristics are displayed in Tab. 3. Local pair-wise comparison matrices for sub-characteristics of detecting attacks, resisting attacks, reacting and recovering from attacks at level-2 have been deliberated and displayed in Tabs. 4–6, respectively, using the same operations and Eqs. (1)–(11) as for level-1 characteristics. The alpha cut method was used to defuzzify pair-wise comparison matrices, and the normalised values and defuzzified local weights of these sub-characteristics are displayed in Tabs. 7–10, respectively, using Eqs. (12)–(14).

Table 3: Fuzzified form of aggregated pair-wise comparison matrix at level 1

	F1	F2
Security (F1)	1.00000, 1.00000, 1.00000	1.68000, 1.37100, 1.02140
Sustainability (F2)	0.98100, 0.73410, 0.59000	1.00000, 1.00000, 1.00000

Table 4: For security fuzzified form of aggregated pair-wise comparison matrix at level 2

	F11	F12	F13
Confidentiality (F11)	1.00000, 1.00000, 1.00000	1.71000, 1.89000, 2.08000	2.46000, 3.5000, 4.52000
Integrity (F12)	0.48000, 0.53000, 0.58000	1.00000, 1.00000, 1.00000	2.81000, 3.27000, 3.78000
Availability (F13)	0.22000, 0.29000, 0.41000	0.26000, 0.31000, 0.36000	1.00000, 1.00000, 1.00000

An unweighted super-matrix is created using the significances derived from the numerous pair-wise comparisons. The unweighted super matrix is generated using Eq. (15), and the results are displayed in Tab. 11. The weighted super-matrix is then calculated by converting all column sums to unity ([18,26], with the results displayed in Tab. 12. The limit super-matrix is then calculated using a weighted super matrix, with the results displayed in Tab. 13. In addition, global characteristic weights are calculated, and the results are displayed in Tab. 14 with characteristic ranking.

Table 5: For sustainability fuzzified form of aggregated pair-wise comparison matrix at level 2

	F21	F22	F23
Energy Consumption (F21)	1.00000, 1.00000, 1.00000	1.72010, 1.41000, 1.14300	2.31100, 1.74500, 1.27500
Software based Resource Optimization (F22)	0.88100, 0.70100, 0.60200	1.00000, 1.00000, 1.00000	1.68000, 1.37100, 1.02140
Perdurability (F23)	0.80200, 0.60400, 0.40300	0.98100, 0.73410, 0.59000	1.00000, 1.00000, 1.00000

Table 6: For perdurability fuzzified form of aggregated pair-wise comparison matrix at level 3

	F231	F232	F233
Reliability (F231)	1.00000, 1.00000, 1.00000	1.64000, 1.92000, 2.20000	2.42000, 3.06000, 3.70000
Maintainability (F232)	0.45000, 0.52000, 0.61000	1.00000, 1.00000, 1.00000	1.52000, 1.94000, 2.48000
Portability (F233)	0.27000, 0.33000, 0.41000	0.40000, 0.52000, 0.66000	1.00000, 1.00000, 1.00000

Table 7: Local weights of level-1 characteristics

	Normalizing value	Local weights
Security (F1)	0.32535, 0.44565, 0.63525	0.43060
Sustainability (F2)	0.22554, 0.32568, 0.43556	0.56940

Table 8: Local weights of level-1 characteristics

	Normalizing value	Local weights
Confidentiality (F11)	0.07854, 0.13254, 0.25547	0.17785
Integrity (F12)	0.03565, 0.07546, 0.11568	0.31550
Availability (F13)	0.04988, 0.07564, 0.15585	0.50615

Table 9: Local weights of level-1 characteristics

	Normalizing value	Local weights
Energy Consumption (F21)	0.13457, 0.21565, 0.33547	0.17885
Software based Resource Optimization (F22)	0.04584, 0.07547, 0.11564	0.31885
Perdurability (F23)	0.06569, 0.09659, 0.14657	0.50230

Table 10: Local weights of level-1 characteristics

	Normalizing value	Local weights
Reliability (F231)	0.14547, 0.17548, 0.21568	0.16175
Maintainability (F232)	0.16569, 0.19569, 0.24574	0.31195
Portability (F233)	0.15547, 0.16567, 0.23569	0.52640

Table 11: Unweighted super matrix

	Goal	F1	F2	F11	F12	F13	F21	F22	F23	F231	F232	F233
Goal	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000
F1	0.25300	0.49100	0.35400	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000
F2	0.37900	0.44900	0.32100	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000
F11	0.00000	0.19600	0.00000	0.18100	0.13300	0.16800	0.13300	0.16800	0.17300	0.21000	0.16800	0.16800
F12	0.00000	0.16300	0.00000	0.18100	0.13300	0.16800	0.19200	0.21000	0.16800	0.17300	0.20100	0.20100
F13	0.00000	0.13400	0.00000	0.17800	0.20100	0.18400	0.18100	0.13300	0.16800	0.19200	0.21000	0.16800
F21	0.00000	0.00000	0.22700	0.13300	0.16800	0.17800	0.18600	0.15300	0.13300	0.19000	0.19200	0.21000
F22	0.00000	0.00000	0.29400	0.18600	0.15300	0.13300	0.19000	0.19200	0.21000	0.16800	0.17300	0.19000
F23	0.00000	0.00000	0.18100	0.16800	0.18100	0.13300	0.19000	0.19200	0.21000	0.16800	0.17300	0.19600
F231	0.00000	0.00000	0.18100	0.16800	0.18100	0.13300	0.19000	0.19200	0.21000	0.16800	0.17300	0.18700
F232	0.00000	0.00000	0.17800	0.18400	0.17800	0.20100	0.18200	0.19200	0.17000	0.18400	0.19600	0.20400
F233	0.00000	0.00000	0.13300	0.17800	0.13300	0.16800	0.18400	0.19600	0.18200	0.20100	0.20100	0.19000

Table 12: Weighted super matrix

	Goal	F1	F2	F11	F12	F13	F21	F22	F23	F231	F232	F233
Goal	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000
F1	0.25300	0.49100	0.35400	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000
F2	0.37900	0.44900	0.32100	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000
F11	0.00000	0.19600	0.00000	0.03400	0.03400	0.03900	0.03300	0.03300	0.03700	0.03500	0.04000	0.03400
F12	0.00000	0.16003	0.00000	0.05900	0.05900	0.05700	0.05900	0.05300	0.05200	0.05100	0.05500	0.05900
F13	0.00000	0.13400	0.00000	0.04600	0.04600	0.05400	0.05600	0.04500	0.05500	0.05600	0.05800	0.05000
F21	0.00000	0.00000	0.22700	0.05400	0.05300	0.04400	0.05000	0.04600	0.04800	0.04400	0.04500	0.04500
F22	0.00000	0.00000	0.29400	0.04900	0.04900	0.04000	0.04400	0.04900	0.04800	0.04000	0.04700	0.04800
F23	0.00000	0.00000	0.19100	0.05800	0.05700	0.04300	0.04200	0.05300	0.04600	0.04200	0.04600	0.04300
F231	0.00000	0.00000	0.00000	0.03700	0.03600	0.04900	0.04300	0.04800	0.04400	0.03800	0.04300	0.05200
F232	0.00000	0.00000	0.00000	0.04500	0.04500	0.05000	0.04400	0.04800	0.05600	0.05000	0.04500	0.05400
F233	0.00000	0.00000	0.00000	0.05500	0.05400	0.04900	0.04300	0.04200	0.04200	0.04300	0.04400	0.04200

Table 13: Limit super matrix

	Goal	F1	F2	F11	F12	F13	F21	F22	F23	F231	F232	F233
Goal	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000	0.00000
F1	0.25300	0.25300	0.25300	0.25300	0.25300	0.25300	0.25300	0.25300	0.25300	0.25300	0.25300	0.25300
F2	0.37900	0.37900	0.37900	0.37900	0.37900	0.37900	0.37900	0.379 00	0.37900	0.37900	0.37900	0.37900
F11	0.05785	0.05785	0.05785	0.05785	0.05785	0.05785	0.05785	0.05785	0.05785	0.05785	0.05785	0.05785
F12	0.07178	0.07178	0.07178	0.07178	0.07178	0.07178	0.07178	0.07178	0.07178	0.07178	0.07178	0.07178
F13	0.06556	0.06556	0.06556	0.06556	0.06556	0.06556	0.06556	0.06556	0.06556	0.06556	0.06556	0.06556
F21	0.03902	0.03902	0.03902	0.03902	0.03902	0.03902	0.06556	0.06556	0.06556	0.06556	0.06556	0.06556
F22	0.01369	0.01369	0.01369	0.06556	0.06556	0.06556	0.03902	0.03902	0.03902	0.03902	0.03902	0.03902
F23	0.08779	0.08779	0.08779	0.03902	0.03902	0.03902	0.03902	0.03902	0.03902	0.03902	0.08779	0.08779
F231	0.03954	0.03954	0.03954	0.06556	0.06556	0.06556	0.06556	0.06556	0.06556	0.06556	0.03954	0.03954
F232	0.08988	0.08988	0.08988	0.03902	0.03902	0.03902	0.03902	0.03902	0.03902	0.03902	0.08988	0.08988
F233	0.07478	0.07478	0.07478	0.07478	0.07478	0.07478	0.07478	0.07478	0.07478	0.07478	0.07478	0.07478

Table 14: Global weights through the hierarchy

Characteristics	Global weights	Percentage	Ranks
F11	0.0565	5.65%	8
F12	0.0978	9.78%	6
F13	0.1654	16.54%	3
F21	0.1254	12.54%	4
F22	0.2047	20.47%	1
F231	0.0587	5.87%	7
F232	0.1105	11.05%	5
F233	0.1810	18.10%	2

Authors took inputs on the technological data of six healthcare system projects as given in Tab. 15 using Tab. 2 from the methodology section. The fuzzy-TOPSIS tactic uses the final weights of characteristics acquired by fuzzy-ANP as inputs to produce a rank for respectively alternative. For this, Eq. (16) is used, and a normalised decision-matrix is created for 8 criteria and 6 options, as shown in Tab. 15. Then, using Eq. (17), each cell value (known as normalised value) of the normalised decision-matrix is multiplied by the weights of each criterion, yielding a fuzzy weighted normalised decision-matrix, as shown in Tab. 16. The Fuzzy Negative-Ideal Solution (NIS) and Fuzzy Positive-Ideal Solution (PIS) are then calculated using Eq. (18). The distance of respectively option value from the NIS and PIS is then evaluated using Eqs. (19) and (20) and is shown in Tab. 17 under the column names D-I and D+I. Lastly, using Eq. (21), the performance value of respectively criterion was computed, and the ranking of alternatives was determined based on the derived performance score, which is also shown in Tab. 17 and Fig. 4. According to the findings of this present research work, Alternative-1 has the finest security tactic in terms of security methods among the 6 competitors.

Table 15: Subjective cognition results of evaluators in linguistic terms

	Alternative-1	Alternative-2	Alternative-3	Alternative-4	Alternative-5	Alternative-6
F11	4.10000, 5.40000, 6.60000	2.50000, 3.90000, 5.50000	3.90000, 5.70000, 7.40000	4.10000, 5.40000, 6.60000	2.50000, 3.90000, 5.50000	3.90000, 5.70000, 7.40000
F12	4.10000, 5.60000, 7.00000	5.20000, 6.70000, 7.90000	4.10000, 5.40000, 6.60000	2.50000, 3.90000, 5.50000	4.10000, 5.40000, 6.60000	2.50000, 3.90000, 5.50000
F13	2.80000, 4.10000, 5.60000	2.90000, 4.40000, 600000	4.10000, 5.60000, 7.00000	5.20000, 6.70000, 7.90000	4.10000, 5.60000, 7.00000	5.20000, 6.70000, 7.90000
F21	2.80000, 3.90000, 5.10000	4.10000, 5.40000, 6.60000	2.50000, 3.90000, 5.50000	3.90000, 5.70000, 7.40000	5.00000, 6.60000, 7.80000	2.90000, 4.40000, 600000
F22	3.90000, 5.50000, 6.90000	4.10000, 5.60000, 7.00000	5.20000, 6.70000, 7.90000	2.80000, 3.70000, 4.90000	4.10000, 5.40000, 6.60000	2.50000, 3.90000, 5.50000
F231	4.10000, 5.40000, 6.60000	2.50000, 3.90000, 5.50000	3.90000, 5.70000, 7.40000	5.00000, 6.60000, 7.80000	4.10000, 5.40000, 6.60000	2.50000, 3.90000, 5.50000
F232	4.10000, 5.60000, 7.00000	5.20000, 6.70000, 7.90000	2.80000, 3.70000, 4.90000	4.10000, 5.60000, 7.00000	4.10000, 5.60000, 7.00000	5.20000, 6.70000, 7.90000
F233	2.80000, 4.10000, 5.60000	2.90000, 4.40000, 600000	1.90000, 2.90000, 4.30000	3.50000, 5.10000, 6.60000	2.80000, 4.10000, 5.60000	2.90000, 4.40000, 600000

Table 16: The weighted normalized fuzzy-decision matrix

	Alternative-1	Alternative-2	Alternative-3	Alternative-4	Alternative-5	Alternative-6
F11	0.0160000, 0.0250000, 0.0350000	0.0130000, 0.0190000, 0.0240000	0.0180000, 0.0240000, 0.0280000	0.0340000, 0.0490000, 0.0650000	0.0110000, 0.0160000, 0.0220000	0.0350000, 0.0530000, 0.0700000
F12	0.0330000, 0.0430000, 0.0510000	0.0090000, 0.0120000, 0.0160000	0.0160000, 0.0250000, 0.0350000	0.0130000, 0.0190000, 0.0240000	0.0180000, 0.0240000, 0.0280000	0.0340000, 0.0490000, 0.0650000
F13	0.0190000, 0.0280000, 0.0390000	0.0060000, 0.0090000, 0.0140000	0.0330000, 0.0430000, 0.0510000	0.0090000, 0.0120000, 0.0160000	0.0150000, 0.0200000, 0.0250000	0.0500000, 0.0600000, 0.0680000

(Continued)

Table 16: Continued

	Alternative-1	Alternative-2	Alternative-3	Alternative-4	Alternative-5	Alternative-6
F21	0.0220000, 0.0300000, 0.0390000	0.0360000, 0.0490000, 0.0620000	0.0190000, 0.0280000, 0.0390000	0.0060000, 0.0090000, 0.0140000	0.0130000, 0.0190000, 0.0240000	0.0520000, 0.0670000, 0.0790000
F22	0.0160000, 0.0250000, 0.0350000	0.0130000, 0.0190000, 0.0240000	0.0160000, 0.0250000, 0.0350000	0.0130000, 0.0190000, 0.0240000	0.0180000, 0.0240000, 0.0280000	0.0340000, 0.0490000, 0.0650000
F231	0.0330000, 0.0430000, 0.0510000	0.0090000, 0.0120000, 0.0160000	0.0330000, 0.0430000, 0.0510000	0.0090000, 0.0120000, 0.0160000	0.0150000, 0.0200000, 0.0250000	0.0500000, 0.0600000, 0.0680000
F232	0.0190000, 0.0280000, 0.0390000	0.0060000, 0.0090000, 0.0140000	0.0190000, 0.0280000, 0.0390000	0.0060000, 0.0090000, 0.0140000	0.0130000, 0.0190000, 0.0240000	0.0520000, 0.0670000, 0.0790000
F233	0.0310000, 0.0430000, 0.0550000	0.0190000, 0.0320000, 0.0470000	0.0210000, 0.0310000, 0.0410000	0.0120000, 0.0170000, 0.0220000	0.0180000, 0.0240000, 0.0280000	0.0260000, 0.0380000, 0.0530000

Table 17: Closeness coefficients of various alternatives

Alternatives	D + i	D − i	Performance score (Pi)	Rank
Alternative 1	0.24758142	0.13154451	0.54257143	1
Alternative 2	0.25679145	0.14958216	0.48695789	4
Alternative 3	0.22256759	0.15274324	0.41274745	6
Alternative 4	0.22547145	0.15465216	0.41763452	5
Alternative 5	0.18556253	0.18167142	0.48854251	3
Alternative 6	0.16859215	0.19957211	0.54168452	2

As a result, the rating of each characteristic in each alternative varies depending on its functioning and the needs of the consumer. Furthermore, a combined estimate of attribute weights and attribute ratings is created as follows to evaluate the influence of sustainable-security of health information software systems throughout the hierarchy. The findings demonstrate that, out of all the options, *the Alternative 1* has the greatest influence on the sustainable-security of health information software systems.

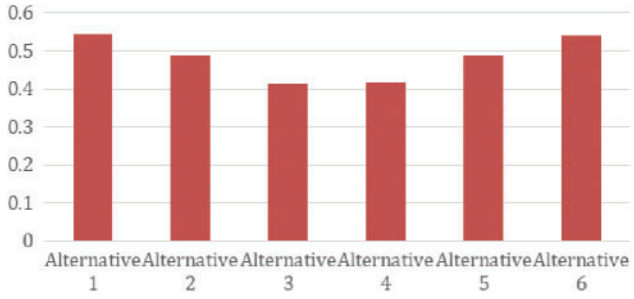

Figure 4: Graphical representation of performance score

6 Sensitivity Analysis

The "Sensitivity Analysis" [26,27] approach is employed to define how the values of independent variables will affect a certain variable under a specified set of expectations. Sensitivity analysis evaluates the effect in a project's basic values and is based on one or more input variables that are kept within certain limitations. The authors used the values of and as 0.5 and 0.5, respectively, throughout the defuzzification technique in this study. These two numbers range from 0 to 1, with a lower value indicating more ambiguity in the participants' decision-making. Because values are dependent on environmental hesitations, the 0.5 value for and is employed to reflect a symmetrical environment. This specifies that the participants are neither overly optimistic nor overly pessimistic about their choices. Those ideals would have a direct impact on sustainable-security.

The values of and can be re-adjusted to suggest assured judgments if the experts participating in the estimate have domain competence. Furthermore, the sets are all 81 (9 × 9), such as (0.1, 0.1), (0.1, 0.2), (0.2, 0.1), (0.1, 0.3), (0.3, 0.1), and so on. Examining the impact of values against the concluding outcomes can improve the procedure's accuracy even more. As a result, more research is needed to accurately predict the values of and. To assess for changes in the outcomes, the authors used Ex1 (0.5, 0.1), Ex2 (0.5, 0.3), Ex3 (0.5, 0.7), Ex4 (0.5, 0.9), Ex0 (0.1, 0.5), Ex6 (0.3, 0.5), Ex7 (0.7, 0.5), and Ex8 (0.9, 0.5) as studies. Furthermore, the value of α is constant while the value of β is in variance for Ex1, Ex2, Ex3, and Ex4. Whereas the value for Ex5, Ex6, Ex7, and Ex8 is constant and changes. Furthermore, for Ex0, the values of and are constant (0.5, 0.5). The results are shown in Tab. 18 and Fig. 5.

Table 18: Variations in the final outcomes

	Ex1	Ex2	Ex3	Ex4	Ex0	Ex5	Ex6	Ex7	Ex8
(Preferences of Participants) α	0.5	0.5	0.5	0.5	0.5	0.1	0.3	0.7	0.9
(Risk Tolerance of Participants) β	0.1	0.3	0.7	0.9	0.5	0.5	0.5	0.5	0.5

(Continued)

Table 18: Continued

	Ex1	Ex2	Ex3	Ex4	Ex0	Ex5	Ex6	Ex7	Ex8
Alternatives									
Alternative 1	0.532 541240	0.555 636233	0.542 111541	0.540 011223	0.542 571430	0.536 526582	0.556 526533	0.569 658745	0.532 236552
Alternative 2	0.485 455574	0.485 699872	0.486 598556	0.480 124574	0.486 957890	0.478 596554	0.496 587457	0.502 236589	0.465 584744
Alternative 3	0.414 555874	0.456 522354	0.412 326542	0.405 654744	0.412 747450	0.406 535299	0.425 699887	0.436 369754	0.396 658745
Alternative 4	0.419 658577	0.417 898878	0.417 256324	0.406 365493	0.417 634520	0.405 657485	0.427 788998	0.436 622001	0.396 655874
Alternative 5	0.487 745844	0.485 653622	0.452 541122	0.479 653558	0.488 542510	0.478 896525	0.496 585479	0.496 558745	0.465 523987
Alternative 6	0.545 655655	0.541 133662	0.545 522333	0.536 365252	0.541 684520	0.536 365859	0.556 988565	0.545 568579	0.523 699878

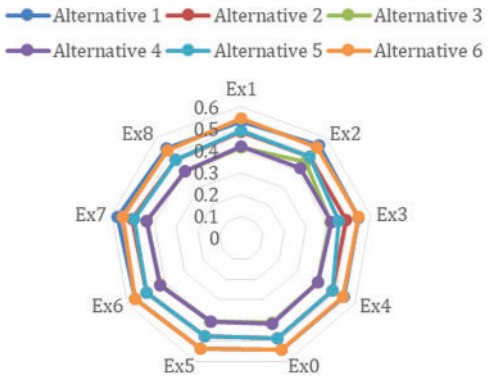

Figure 5: Variation in outcomes

Variability in outcomes is shown in Tab. 18 and Fig. 5 due to the values. The findings from the values (as 0.5) suggested that a symmetrical environment in terms of practitioner judgments could provide the best outcomes. After reviewing the outcomes of the sensitivity analysis, it was concluded that the values of the overall sustainable-security of health information software systems do not vary significantly. The importance of health information software systems sustainable-security is positively influenced by participants' expectations and risk perceptions.

7 Comparing the Outcomes with Other Methodologies

With the same data, different procedures produce different results (Srivastava et al., 2010). The majority of practitioners use one or more procedures to check the accuracy of the outcomes achieved using the projected method [5–8]. Following the Fuzzy ANP-TOPSIS process's implementation, this segment employs four further procedures to demonstrate the accuracy of the overall assessments and results. Classical-ANP-TOPSIS process [9], Classical AHP-TOPSIS process [12], Fuzzy AHP-TOPSIS process [15], and Fuzzy AHP-Average Weighted process [17–19] were among the ANP and AHP based procedures used by the authors. Furthermore, estimation in the ANP procedure is accomplished through ratio-scale pair-wise judgments [21–23]. It's also used to assess decisions based on practitioners' first impressions. This is one of the most important MCDM procedures

for defining unstructured problems during the development of health information software systems [25–27]. Furthermore, fuzzy set theory has played an important role in accepting uncertainty and inconsistent judgments, such as the nature of human decision investigation, which was not adequately addressed in previous ANP [29–31].

In addition, Fuzzy ANP-TOPSIS process allows for further comprehensive justifications of practitioners' confusing and undefined knowledge [32,33]. The number of experts is used in the Fuzzy ANP-TOPSIS procedure during combination, and the Fuzzy AHP-Average Weighted Procedure is employed only for simple average procedures of fuzzified values. Furthermore, Classical AHP-TOPSIS Process is a procedure for creating a gathering relationship procedure in one step. Furthermore, Fuzzy AHP-TOPSIS Process is a procedure based on fuzzy logic and tree structure that uses information gathering, analysis procedures, and forecasts to collect and revise practitioners' judgments [34,35]. The data is now collected in its purest form. Tab. 19 shows the differences in the impacts of sustainable-security, and Fig. 6 shows a graphical representation of the same.

Table 19: Comparisons between results

Alternatives/ Procedures	Fuzzy ANP-TOPSIS process	Classical ANP-TOPSIS process	Classical AHP-TOPSIS process	Fuzzy AHP-TOPSIS process	Fuzzy AHP-Average weighted Process
Alternative 1	0.542571430	0.554718730	0.542774584	0.542636365	0.554748574
Alternative 2	0.486957890	0.484474580	0.486563521	0.486564564	0.496585699
Alternative 3	0.412747450	0.425587440	0.412632635	0.412236232	0.425665877
Alternative 4	0.417634520	0.405524540	0.417252582	0.417254150	0.426398755
Alternative 5	0.488542510	0.485447460	0.488437856	0.488665522	0.496969633
Alternative 6	0.541684520	0.535555990	0.541555222	0.542555857	0.556632452

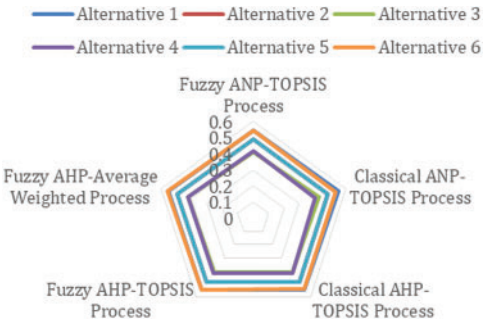

Figure 6: Graphical representation of differences between outcomes

The difference in the impacts of sustainable-security through diverse processes is minor, as indicated in Tab. 19. Pearson's correlation technique was used in this work for empirical testing [36]. This process is used to calculate the associated value of the main outcomes and other approaches' outcomes. Furthermore, the correlation coefficient depicts the degree of similarity between two outcomes. The proximity value ranges from 1 to +1 [37–39]. The value close to 1 specifies a weaker connection

between values, whereas the value close to + 1 specifies a stronger bond. Pearson correlations between outcomes are highly correlated.

The correlations show a strong link between the obtained outcomes. Also, the data show that the selected and detected features, as well as their contribution to positive sustainable-security, are important. Saaty T. L., just published an essay on the estimation of sustainable-security [38]. One of the three characteristics of security (CIA) chosen in this article was sustainability. Only one sustainability attribute was taken into consideration in that study, therefore these characteristics were not entirely balanced. Furthermore, Sahu et al. [40] point out that sustainable-security is fully dependent on its contributing qualities. According to Sahu et al. [41], features of sustainability and security play equal roles in preserving sustainable-security for a certain life-span.

8 Discussion

As health information software systems adapt to contemporary requirements, the unpredictability of health information software systems is also on the rise. According to Khan et al., piece, the tax data of millions of Bulgarians was taken, and the attacker gave the same stolen data to the international media outlets as proof of his crime [42]. Such instances call for the urgent need for well-designed health information software solutions. Alfakeeh et al., also asserted in his blog post that "sustainable software design satisfies its clients' current requirements without jeopardising the ability to meet those expectations in the future" [43]. As a result, the transformation of health information software systems into sustainable and secure software architecture is an essential prerequisite.

This research focuses on both security and sustainability aspects and proposes a classified construction that fundamentally underlines the noteworthy and contributing elements in the design of health information software systems for sustainable-security. The goal of this current research work is to evaluate the sustainable-security of health information software systems at an early stage during development process. Because evaluation is the most effective way to attain sustainable-security, this study includes security and sustainability qualities and puts them to the test [44,45]. The findings of the research, as cited in this study, will aid developers in strengthening the sustainable-security of health information software systems as it grows.

There are a variety of security models that quantify sustainable-security. However, employing Fuzzy-ANP and other MCDM techniques, a strategy or devoted framework that integrates sustainability and security in a single column is inherently more cost-effective [46,47]. The methodology described here would aid in determining the sustainable-security of health information software systems while also opening the road for improved economic and environmental sustainability to meet the consumers' expectations. In the present research work, we looked at nine sustainable-security criteria that might be incorporated during the construction of health information software systems.

The majority of the organisations distinguish between rapidly changing industry and regulatory demands to alter how security is controlled (essentially preserving CIA) and dependability is maintained only at some point in the procedure of developing health information software systems. The proposed study offers a quantitative assessment to enhance the sustainability and security of health information software systems. In the design phase of healthcare systems, the sustainable-security hierarchical structure aids in elucidating the connection between the features that lead to sustainable-security. The writers of this research gathered comments of the experts on the contributing security and sustainability aspects of three different health information software systems in order to write this

paper. Fuzzy ANP-TOPSIS is used to collect data from the experts, and the results are then double-checked using various ANP-based techniques. The study's findings and drawbacks are summarised below:-

- The characteristics used in this study are unique to each and every health information software system's security. As a result, the estimation would be valuable for all the developers.
- It is critical to strike a balance between sustainability and security qualities for achieving high sustainability. As a result of these findings, developers may be able to create a technique with important qualities that contribute to the sustainable-security of health information software systems.
- Determining sustainable-security will enhance economic, environmental, and social sustainability, thus adding to the customers' satisfaction.
- More essential characteristics for increasing the overall effectiveness of health information software systems are sustainability and longevity.
- Other ANP, AHP, and TOPSIS based processes have been demonstrated to generate less accurate results than MCDM procedures like Fuzzy ANP-TOPSIS. The results of the current investigation and the numerical analysis back this up.
- For statistical validation, the correlation coefficients are estimated. It is close to 1, indicating that the influence of the link between the Fuzzy ANP-TOPSIS outcomes and the outcomes from other ANP-based methods is minor.
- While Fuzzy ANP-TOPSIS produced better results in this study than ANP-based other methods, it is possible to achieve superior results using more traditional MCDM procedures, such as decision-making procedures based on fuzzy hesitant sets.
- This review yielded metric-based recommendations that can assist the practitioners in improving long-term security by utilising high-priority characteristics of concern.

The discussion has shown that evaluating sustainable-security is vital and critical in its own right. However, this approach may have some boundaries that can be addressed in future research. The following are the outcomes' limitations:

- The data for health information software systems was gathered from a small sample of people. The outcomes may alter if the data is gathered from a larger sample.
- Various sustainability and security qualities may exist in addition to those that are presented in this study. The number of elements that influence the outcome of the sustainable-security effect can vary.
- The methodology used in this research work is solely dependent on the opinions of 110 experts. As a result, a huge dataset can assist in producing more precise and dependable results.

9 Conclusion

For security specialists, well-organized sustainable-security engineering and its effective implementation in developing the health information software systems necessitates a specific security review technique. In this research work, the sustainability and security attributes of current research are identified, and the sustainability of health information software systems is investigated. This work uses the Fuzzy ANP-TOPSIS process for quantitative estimates, which are then confirmed using four different ANP-based approaches. Sustainability is the utmost important aspect of the nine key qualities for efficient and effective sustainable-security of health information software systems, according to all approaches. The current state of security for health information software systems is insufficient in comparison to the threat that the current attack environment provides to the systems. The fact

that development organisations have established a wide number of unsecure systems with numerous unsustainable vulnerabilities and applications is comical but compelling. The formulation of security rules that also focus on sustainability is a demand of our age. As a result, our study's sustainable-security assessment will aid the developers in developing secure and sustainable health information software systems.

Acknowledgement: This research work was funded by the Institutional Fund Projects under the Grant No. (IFPHI-287-611-2020). The authors are grateful for the technical and financial support rendered to them by the Ministry of Education and King Abdulaziz University, DSR, Jeddah, Saudi Arabia.

Funding Statement: Funding for this study was received from the Ministry of Education and Deanship of Scientific Research at King Abdulaziz University, Kingdom of Saudi Arabia under Grant No. IFPHI-287-611-2020.

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

References

[1] N. R. Alharbe, "A Fuzzy-delphi based decision-making process for measuring usable-security of web based smart hospital management system," *ICIC Express Letters*, vol. 14, no. 1, pp. 15–21, 2020.

[2] 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*, vol. 42, no. 6, pp. 1–18, 2019.

[3] T. Butler, "Compliance with institutional imperatives on environmental sustainability: Building theory on the role of green IS," *The Journal of Strategic Information Systems*, vol. 20, no. 1, pp. 6–26, 2011.

[4] A. Agrawal, M. Alenezi, R. Kumar and R. A. Khan, "Measuring the sustainable-security of web applications through a fuzzy-based integrated approach of AHP and TOPSIS," *IEEE Access*, vol. 7, no. 8, pp. 153936–153951, 2019.

[5] A. Agrawal, M. Alenezi, R. Kumar and R. A. Khan, "A unified fuzzy-based symmetrical multi-criteria decision-making method for evaluating sustainable-security of web applications," *Symmetry*, vol. 12, no. 3, pp. 1–18, 2020.

[6] A. Calabrese, R. Costa, N. Levialdi and T. Menichini, "Integrating sustainability into strategic decision-making: A fuzzy AHP method for the selection of relevant sustainability issues," *Technological Forecasting and Social Change*, vol. 139, no. 5, pp. 155–168, 2019.

[7] C. Calero and M. Piattini, "Puzzling out software sustainability," *Sustainable Computing: Informatics and Systems*, vol. 16, no. 6, pp. 117–124, 2019.

[8] C. Calero and M. Piattini, "Introduction to green in software engineering," *Green in Software Engineering*, vol. 5, no. 6, pp. 3–27, 2015.

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

[10] C. Calero, M. Moraga and M. F. Bertoa, "Towards a software product sustainability model," *Sustainable Software for Science: Practice and Experiences*, vol. 12, no. 3, pp. 1–18, 2020.

[11] C. Calero, I. G. R. Guzmán, M. A. Moraga and F. García, "Is software sustainability considered in the CSR of software industry?," *International Journal of Sustainable Development & World Ecology*, vol. 26, no. 5, pp. 439–459, 2019.

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

[13] G. Li, H. Zhou, B. Feng, G. Li, T. Li *et al.,* "Fuzzy theory based security service chaining for sustainable mobile-edge computing," *Mobile Information Systems*, vol. 42, no. 6, pp. 1–18, 2017.
[14] S. Luthra, S. Kumar, D. Garg and A. Haleem, "Barriers to renewable/sustainable energy technologies adoption: Indian perspective," *Renewable and Sustainable Energy Reviews*, vol. 41, no. 6, pp. 762–776, 2015.
[15] A. Mardani, A. Jusoh, E. Zavadskas, F. Cavallaro and Z. Khalifah, "Sustainable and renewable energy: An overview of the application of multiple criteria decision making techniques and approaches," *Sustainability*, vol. 7, no. 10, pp. 13947–13984, 2015.
[16] R. Kumar, S. A. Khan and R. A. Khan, "Durability challenges in software engineering," *CrossTalk*, vol. 42, no. 4, pp. 29–31, 2016.
[17] R. Kumar, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal *et al.,* "A Knowledge-based integrated system of hesitant fuzzy set, AHP and TOPSIS for evaluating security-durability of web applications," *IEEE Access*, vol. 8, no. 8, pp. 48870–48885, 2020.
[18] R. Kumar, M. Zarour, M. Alenezi, A. Agrawal and R. A. Khan, "Measuring security durability of software through fuzzy-based decision-making process," *International Journal of Computational Intelligence Systems*, vol. 12, no. 2, pp. 627–642, 2019.
[19] X. Mi, X. Wu, M. Tang, H. Liao, A. Albarakati *et al.,* "Hesitant fuzzy linguistic analytic hierarchical process with prioritization, consistency checking, and inconsistency repairing," *IEEE Access*, vol. 7, no. 6, pp. 44135–44149, 2019.
[20] H. Q. Nguyen, "*Testing Applications on the web: Test Planning for Internet-Based Systems*," Henderson, NV, USA: John Wiley & Sons, 2000. [Online]. Available: https://download.e-bookshelf.de/download/0000/5836/24/L-G-0000583624-0002361295.pdf.
[21] P. A. Owusu and S. A. Sarkodie, "A review of renewable energy sources, sustainability issues and climate change mitigation," *Cogent Engineering*, vol. 3, no. 1, pp. 1–14, 2016.
[22] S. Oyedeji, A. Seffah and B. Penzenstadler, "A catalogue supporting software sustainability design," *Sustainability*, vol. 10, no. 7, pp. 1–22, 2018.
[23] B. Penzenstadler, A. Raturi, D. Richardson and B. Tomlinson, "Safety, security, now sustainability: The non-functional requirement for the 21st century," *IEEE Software*, vol. 31, no. 3, pp. 40–47, 2014.
[24] Laerd Statistics. Pearson's product moment correlation. Statistical tutorials and software guides. Retrieved from https://statistics.laerd.com/statistical-guides/pearson-correlation-coefficient-statistical-guide.php. 2020.
[25] M. P. Robillard, "Sustainable software design," in *Proc. of the 2016 24th ACM SIGSOFT Int. Symposium on Foundations of Software Engineering*, New York, NY, United States, pp. 920–923, 2016.
[26] T. L. Saaty, "Decision making with the analytic hierarchy process," *International Journal of Services Sciences*, vol. 1, no. 1, pp. 83–98, 2008.
[27] T. L. Saaty, "How to make a decision: The analytic hierarchy process," *European Journal of Operational Research*, vol. 48, no. 1, pp. 9–26, 1990.
[28] K. Sahu, F. A. Alzahrani, R. K. Srivastava and R. Kumar, "Hesitant fuzzy sets based symmetrical framework of decision-making for estimating the durability of web application," *Symmetry*, vol. 12, no. 6, pp. 1770–1792, 2020.
[29] K. Sahu, F. A. Alzahrani, R. K. Srivastava and R. Kumar, "Evaluating the impact of prediction techniques: Software reliability perspective," *Computers, Materials & Continua*, vol. 67, no. 2, pp. 1471–1488, 2021.
[30] L. Mikhailov, "Deriving priorities from fuzzy pairwise comparison judgements," *Fuzzy Sets and Systems*, vol. 134, no. 3, pp. 365–385, 2003.
[31] K. Sahu and R. K. Srivastava, "Soft computing approach for prediction of software reliability," *ICIC Express Letters*, vol. 12, no. 12, pp. 1213–1222, 2018.
[32] I. Schieferdecker, "Responsible software engineering," *Future of Software Quality Assurance*, vol. 12, no. 6, pp. 137–146, 2020.
[33] P. R. Srivastava, A. P. Singh and K. V. Vageesh, "Assessment of software quality: A fuzzy multi criteria approach," *Evolution of Computation and Optimization Algorithms in Software Engineering: Applications and Techniques*, vol. 19, no. 5, pp. 200–219, 2010.

[34] W. Stallings, L. Brown, M. D. Bauer and A. K. Bhattacharjee, "Computer security: Principles and practice," *Computers, Materials & Continua*, vol. 65, no. 5, pp. 978–990, 2012.
[35] M. Stifel, "Securing The modern economy: Transforming cybersecurity through sustainability," Public Knowledge, 2018. [Online]. Available: https://www.publicknowledge.org/assets/uploads/documents/Securing_the_Modern_Economy--Transforming_Cybersecurity_Through_Sustainability_FINAL_4.18.18_PK.pdf.
[36] C. C. Venters, R. Capilla, S. Betz, B. Penzenstadler, T. Crick *et al.*, "Software sustainability: Research and practice from a software architecture viewpoint," *Journal of Systems and Software*, vol. 138, no. 2, pp. 174–188, 2018.
[37] C. Venters, C. Jay, L. Lau, M. K. Griffiths, V. Holmes *et al.,* "Software sustainability: the modern tower of babel," in *Proc. of the Third Int. Workshop on Requirements Engineering for Sustainable Systems Co-located with 22nd Int. Conf. on Requirements Engineering*, Karlskrona, Sweden, pp. 1–6, 2014. [Online]. Available: http://ceur-ws.org/Vol-1216/paper2.pdf.
[38] E. K. Zavadskas, K. Govindan, J. Antucheviciene and Z. Turskis, "Hybrid multiple criteria decision-making methods: A review of applications for sustainability issues," *Economic Research-Ekonomska Istraživanja*, vol. 29, no. 1, pp. 857–887, 2020.
[39] 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.
[40] K. Sahu and R. K. Srivastava, "Revisiting software reliability," *Advances in Intelligent Systems and Computing*, vol. 802, pp. 221–235, 2019..
[41] K. Sahu and R. K. Srivastava, "Predicting software bugs of newly and large datasets through a unified neuro-fuzzy approach: Reliability perspective," *Advances in Mathematics: Scientific Journal*, vol. 10, no. 1, pp. 543–555, 2021.
[42] A. I. Khan, A. Saad, F. J. Alsolami, Y. B. Abushark, A. Almalawi *et al.,* "Integrating blockchain technology into healthcare through an intelligent computing technique," *Computers, Materials & Continua*, vol. 70, no. 2, pp. 2835–2860, 2022.
[43] A. S. Alfakeeh, A. Almalawi, F. J. Alsolami, Y. B. Abushark, A. I. Khan *et al.,* "Hesitant fuzzy-sets based decision-making model for security risk assessment," *Computers, Materials & Continua*, vol. 70, no. 2, pp. 2297–2317, 2022.
[44] F. J. Alsolami, A. S. A. Alghamdi, A. I. Khan, Y. B. Abushark, A. Almalawi *et al.,* "Impact assessment of covid-19 pandemic through machine learning models," *Computers, Materials & Continua*, vol. 68, no. 3, pp. 2895–2912, 2021.
[45] Y. B. Abushark, A. I. Khan, F. J. Alsolami, A. Almalawi, M. M. Alam *et al.,* "Usability evaluation through fuzzy AHP-TOPSIS approach: Security requirement perspective," *Computers, Materials & Continua*, vol. 68, no. 1, pp. 1203–1218, 2021.
[46] J. Kaur, A. I. Khan, Y. B. Abushark, M. Alam, S. A. Khan *et al.,* "Security risk assessment of healthcare web application through adaptive neuro-fuzzy inference system: A design perspective," *Risk Management and Healthcare Policy*, vol. 13, no. 5, pp. 355–371, 2020.
[47] A. K. Pandey, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal *et al.,* "Key issues in healthcare data integrity: analysis recommendations," *IEEE Access*, vol. 8, no. 8, pp. 15847–15865, 2020.