IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 9, 2020, accepted July 17, 2020, date of publication July 21, 2020, date of current version August 4, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3010729

Evaluating the Security Impact of Healthcare Web Applications Through Fuzzy Based Hybrid Approach of Multi-Criteria Decision-Making Analysis

ALKA AGRAWAL[1], ABHISHEK KUMAR PANDEY[1], ABDULLAH BAZ[2], (Senior Member, IEEE), HOSAM ALHAKAMI[3], (Member, IEEE), WAJDI ALHAKAMI[4], RAJEEV KUMAR[1,5], AND RAEES AHMAD KHAN[1], (Member, IEEE)

[1]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow 226025, India
[2]Department of Computer Engineering, College of Computer and Information Systems, Umm Al-Qura University, Makkah 21421, Saudi Arabia
[3]Department of Computer Science, College of Computer and Information Systems, Umm Al-Qura University, Makkah 21421, Saudi Arabia
[4]Department of Information Technology, College of Computer Science and Technology, Taif University, Taif 26571, Saudi Arabia
[5]Department of Computer Application, Shri Ramswaroop Memorial University, Lucknow 225003, India

Corresponding author: Rajeev Kumar (rs0414@gmail.com)

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

ABSTRACT Continuous data breaches targeting the invaluable medical records have become a nemesis for the healthcare organizations. A secure and effective information security model in healthcare web applications can gain and enhance the respect as well as revenue of the healthcare organizations. For achieving this goal, a multi-criteria decision methodology can be a milestone. The authors have used a hybrid integrated Fuzzy Analytical Hierarchy Process-Technique for Order of Preference by Similarity to Ideal Solution (Fuzzy AHP-TOPSIS) method for evaluating various information security factors of a web application in order to provide effective and useful results for the developers and researchers. Furthermore, every calculation needs a validation and scientific proof in our case the study assesses the evaluated result on software of hospital from Varanasi, India. The results and ideology of this study will definitely help the practitioners in developing secure and effective information security within a web application. Moreover, the empirical analysis conducted in our research has attempted to etch a systematic path for the developers who can focus on the most prioritized factors for assured and concrete information security within a web application.

INDEX TERMS Information security, healthcare web applications, fuzzy AHP, fuzzy TOPSIS.

I. INTRODUCTION

Information security in healthcare web applications and the healthcare sector is the most pressing concern in the present context [1]. An article outsourced from *healthcaresecurity.com* provides a detailed explanation on the critical condition of healthcare web applications. The article also calls upon the immense need for pre-secured web applications [2].The previous 10 years were probably the most turbulent ones for the healthcare information security. According to the statistics, information disclosure in the healthcare industry has been one of the most efficient attacks in the last 10 years [3]. The experts cite that the security flaws of software and smart web portals of healthcare sector inadvertently provide an easy home ground for cyber-attacks. This type of situation has created a highly sensitive scenario for information security in healthcare web applications. The current smart health service scenario poses an enormous challenge for the developers and security practitioners who are now working on various security approaches and methodologies to provide a secure and *information-disclosure free* web application for healthcare [2]. However, providing assured information security in any web application is complex and a formidable task. While profiling this research study, the authors reviewed many healthcare data breach incidents due to web application failure. According

The associate editor coordinating the review of this manuscript and approving it for publication was Zhipeng Cai.

to the detailed statistics, many patients' personal information was disclosed due to web application's weak information security processes [4]. Decidedly, there is a need for solid information security in web applications of healthcare sector. A simple rule of security in SDLC tells that rather than providing a security approach after the development of any web application, it is more effective to secure an application during the development process for efficient security.

Providing effective information security for any web application is a decision-based task. In particular, Multi-criteria decision-making procedures play a very significant and critical role in these types of tasks [5]. A. Mardaani *et al.* provides a clear and detailed description on multi criteria decision making (MCDM) methodologies. The researchers also emphasise that selecting and choosing this MCDM methodology would be better and effective idea for research endeavors [6]. MCDM covers various methods, but it is evident that fuzzy MCDM is one of the most effective approaches in the current era [7], [24], [27], [29]–[33], and [35]. Moreover, authors of the present study have their own expertise in this scientific approach through their previous research initiatives [26], [28], [31], [32], [34], [36]–[40] in various fuzzy based multi criteria decision making methodology. The barriers of AHP approach and implications of the method is described and analyzed by D. Garg et al in their paper briefly [8]. Due to the drawbacks in this approach, we have used the a combined hybrid approach of fuzzy set theory and analytical hierarchy process (AHP) called fuzzy-AHP [5], associating with TOPSIS method to evaluate the various factors of healthcare information security.

For accurate evaluation of information security through integrated fuzzy MCDM methodology, defining various security attributes by a systematic and step-by-step (tree based) format is important and necessary. Therefore, the third segment of this paper entails a description of the information security factors in healthcare web applications by employing a tree structure. The results of the evaluation of tree structure through fuzzy AHP-TOPSIS method will help the experts in constructing more secure healthcare web applications for information security. Furthermore, with the intent of providing a more corroborative reference for the experts, this study also analyzes the sensitivity of the evaluated results in the section on *Threat to Validity* through sensitivity analysis and confusion matrix approach.

The rest of the paper has been envisioned as: Second section of the paper discusses about the previous research initiatives and research ideas. Third section of the paper talks about threat model of healthcare information security in current situation and its possible effect. The fourth section presents the description of various selected factors and their significance towards the security of healthcare web application. Section 5 and 6 of the paper illustrate the methodology and its calculative implementation on the developed hierarchy. Comparison of the obtained results and sensitivity analysis has been described in section 7 and 8, respectively. Section 9 and 10 of the study provide the discussion and conclusion, respectively.

II. PAST RESEARCH ACTIVITIES

Several experts and researchers have proposed their security models and frameworks for implementing a type of development life cycle related to applications [3], [7]. Many researchers have also worked in information/data security in the healthcare sector but the authors of this study were able to sieve out only a few endeavors available in the context of information security on healthcare web applications.

Furthermore, in order to summarize and collect research studies for the proposed paper, authors undertook a scrutiny of the existing research pursuits in healthcare information security. While conducting the examination for healthcare information security, we applied the search strings (Fuzzy AHP-TOPSIS for healthcare; Healthcare Information Security; Fuzzy AHP-TOPSIS information security, etc.) on various popular data repositories related to scientific paper, like IEEE Xplore, PubMed, Google Scholar, etc. During the process of selecting and finding articles, we found several articles and reports related to various aspects of healthcare security and information security. However after analyzing them, it was evident that there is rather limited literature available on healthcare information security directly or indirectly. Our intent was to peruse only those specific research studies that discussed healthcare information security directly or indirectly. Moreover, we focused on outsourcing those analyses that provided key observations in context of healthcare information security and its factors. Some related initiatives have been outlined below:

- **Christian Esposito** *et al.* presented a paper in 2018 discussing blockchain technology in healthcare data. The paper focused mainly on data/information privacy and data integrity [9]. The authors have provided an overview scenario and a model of blockchain data handling for healthcare in the paper. In the context of information security, the paper concludes that integrity and privacy are the two main factors that need significant attention.
- **Eric Affuldadzie** *et al.* stated in 2016 that many online portals and websites are providing health-related information but there is no ranking and validation model available for assessing the reliability and usefulness of the information [10]. To help the healthcare organizations and patients, the authors provided a framework with the help of fuzzy VIKOR based method for assessing and ranking the online health information. In the context of information security, this paper provides the approach for fetching reliable and useful quality of information from online portals.
- **Anastasia Theodouli** *et al.* presented a paper in 2018 which proposed a blockchain secure data sharing model for two healthcare organizations. Authors of the paper provided a private and *manipulation-free*

approach for sharing clinical healthcare data between two entities [11].

- **Iuliana Chiuchisan** *et al.* presented a paper in 2017 which discussed a security approach for home-based healthcare services. Paper provided data privatization, access role management and availability assurance in home-based healthcare service scenarios. In the context of information security, this paper discusses the information confidentiality, availability as well as accessibility for healthcare web applications through home-based healthcare services [12].
- **Steve G. Langer**presented a paper in 2016 discussing the cyber security issues and implications in healthcare information security. The paper talks about the accountability, authorization, authentication, and reliability of healthcare information through various papers and descriptive explanations [13].
- Various terms like technical, administrative, physical, etc., are discussed in paper written by **Esmaeil Mehraeen** *et al.*in the context of information security in healthcare services. The authors of the paper used a questionnaire for conducting the survey and fetching the results according to them. In the context of information security, this paper discussed the accessibility as well as interoperability of healthcare data for simple and easy data transactions between health entities [14].
- **Roy** *et al.* provide a great research article on mobile cloud computing for making the healthcare services easy for patients. The proposed model in this paper enables the patients to access their medical records, suggestions and recommendations through a restricted access into controlled cloud environment [42]. This type of secure model motivated us to analyze the factors for concern and attention in the healthcare web application security.
- **Jindal** *et al.* discussed about the remote healthcare application and its data handling approaches in their paper. The researchers used fuzzy rule based classifier to process the large volume f data that is acquired via remote medical services. This paper also presents the model for data management and its challenges [45]. This study motivated the authors of proposed study to use fuzzy based multi criteria decision making approaches for obtaining more accurate results.

Although previous research initiatives do discuss various factors and attributes of healthcare information security, many factors and studies [46]–[48] still need to be addressed and given specific attention in the information security of healthcare web applications.

Though different research investigations do provide various outcomes related to healthcare and information security, there is yet no specific study that pertains to key issues for healthcare information security. The studies discussed above contribute to a specific part of healthcare and its information security. Our research vision is premised on the need to discuss and assess healthcare information security as a whole. During the selection and analysis process of literature, we traced certain articles that discussed the confidentiality of information specifically in healthcare through different techniques. One study, in particular, also dwelt on secure IoT communication for preventing data manipulation in healthcare environment, and suggested a secure approach for basic functionality integrity.

Our research interest was also to map an exhaustive repository of the available literature which could be an effective weapon against information breaches and manipulation in the healthcare sector. For achieving this objective, we summarized and then analyzed the literature to collate various factors for healthcare information that would help the experts and developers in the future to maintain healthcare information security in web applications.

For achieving the effective and the desired level of information security in healthcare web applications, the framework proposed in this study is going to be a milestone for research community. Furthermore, this study also estimates the information security of all 15 versions of locally developed hospital software of Varanasi, Uttar Pradesh, India. For measuring the information security of web application, this paper uses a fuzzy AHP-TOPSIS methodology.

III. THREAT PLOT OF HEALTHCARE WEB APPLICATION SECURITY

Healthcare services are the key targets of the intruders and the last five years have seen unprecedented rise in data breach episodes in this sector. High impact as well as higher cost of data makes this sector a heaven for attackers. It is evident that attackers are penetrating healthcare web applications rapidly from various techniques. However, a good and securely developed healthcare web application can respond accurately during these penetrating processes.

A report from Juniper Research predicts that the growth of estimated data breach cost is going to be 5 times more in 2020 in the comparison of 2015 [49]. Another analysis firm reported various threat factors that create huge inconvenience in securing healthcare data privately and manipulation-free. These factors are:

Growth in attack implementation scale: -The report states that current healthcare data breaches are much larger than the attacks carried out ten years ago. Statistics show that previous largest data breach incident in 2014 was 400 Gbps and other incidents are 300, 170 Gbps. But if you look at the previous data of the last 10 years, the scale of attacks was only maximum 8Gbps [50].

Trending use of Advance Persistent attacks: - Advance persistent attacks are called advance persistent threat (APT). It is a new and a very harmful attack type that renders the whole healthcare system hollow, just like termites infesting wood. APT is a new and advance way to attack large organizations for a long period of time [25]. APT attacks work on multi-vector attack methodology, i.e. attacker tricks the system or user through various layers and doors that are exploited by the intruder.

Frequent use of DDoS attack: -DDoS attacks are third and most irritating threat factor for healthcare data security experts. DDoS attacks are old but still a golden path for intruders to penetrate and trick any organization into a pandemic mode. A report from a company cites that 79% of the organizations are unable to detect whether their web traffic is coming from humans or bots [51].

These threat factors are important and common vectors that need extra attention of the security experts. Malwares are also another important and most harmful concern for healthcare industry. Furthermore, their impact ratio is also very high [37]. Thus, the prevailing and emerging threats became the premise of investigating a more assured and convincing mechanism for information security of healthcare web application.

IV. INFORMATION SECURITY IN HEALTHCARE WEB APPLICATION

Attackers are targeting healthcare information and medical services continuously and sell these information's on dark web in high costs due to its sensitivity as well as for more profit [15]. These types of disclosures and breaches can be detrimental for healthcare organizations. HIPPA journal recently released a July cyber-attack statistics for 2019. The survey cites that emails and IT infrastructure are the most vulnerable information pools in the healthcare organization [4], [16]. Thus, the developers need to adopt highly secure information security architecture. For understanding the factors of information security better, authors of this study prepared a questionnaire enlisting 20 specific contexts.

The respondents of this questionnaire were 101 experts working in the domain of healthcare information security as well as web application security. After collating all the responses, the authors elicited 72 valid responses and on the basis of these responses, the present research study identified key factors that were elemental to information security. This has been depicted in the hierarchy shown in figure 1. According to the hierarchy, it is clear that web application information security for healthcare is affected by confidentiality, integrity, availability, interoperability, etc., which have been discussed below:

- *Confidentiality:* In the context of information security preventing information from unauthorized access and maintaining the privacy of information is called confidentiality. In simple language, we can say that preventing unauthorized persons from looking and accessing the information is called confidentiality [17]. J. Srinivas *et al.* describe the privacy or confidentiality issue of medical data in healthcare services. The researchers provide the authenticated Real- OR Random (ROR) approach to secure the connection between the patient and healthcare medical services [44].
- *Integrity:* In terms of information security, integrity is maintaining the originality of information in a model. For easy understanding, integrity provides security for information from manipulation or tampering [9].
- *Availability:* Availability is best defined as the information which is always present for the authorized users whenever they need to access it. Most intruders try to interrupt the availability of information in any web application so that when a rightful user tries to fetch any information from the information system, the user is unable to access that information. Recent attacks are targeting the availability of information [12]. P. Singh *et al.* provide an excellent article on managing availability of healthcare data securely in network architecture and describe a model for security in healthcare ad-hoc network [43].
- *Scalability:* Scalability refers to the ability of any healthcare web application or system for adopting the large demand of data or users according to the trend. In simple words blockchain is a new approach that has been adopted by many healthcare security researchers and experts. However, blockchain has been classically developed for financial transactions. Hence given its basic attributes, especially in the case of healthcare data transactions, blockchain fails because of heavy data load or large volume of data. This type of issue is called the scalability related issue. Thus, put more aptly, scalability is the ability to meet the increasing demand of information [18].
- *Interoperability:* Interoperability is the ability of healthcare information to work together in different work environments. Different healthcare technologies and institutions use various different formats of information for exchange and transfer. Meeting these formats is called interoperability of information [19].
- *Accountability:* In the context of information security, accountability refers to the answerability, i.e., the users working within an information system bear the responsibility to maintain the security of information from their own end. Every specific node of information model is answerable for any mistake or disruption in accessing the information [20].
- *Accessibility:* Accessibility refers to which user has how much access to information. For instance, if a doctor is using a mobile health application for managing the patients' record and providing them prescriptions and other medical facilities, the doctor does not need to access the information related to the patients' financial transactions and information. Similarly, if an employee in the accounts department of any healthcare organization cannot be privy to the information related to patients' medical condition. This type of access restriction is called accessibility in the healthcare information system [21].

Factors of information security in healthcare web applications are represented in a hierarchal model in figure 1. These factors directly affect information security in healthcare web applications. Maintaining these factors during the development of any healthcare web application can provide a secure and *breach-free* environment in healthcare

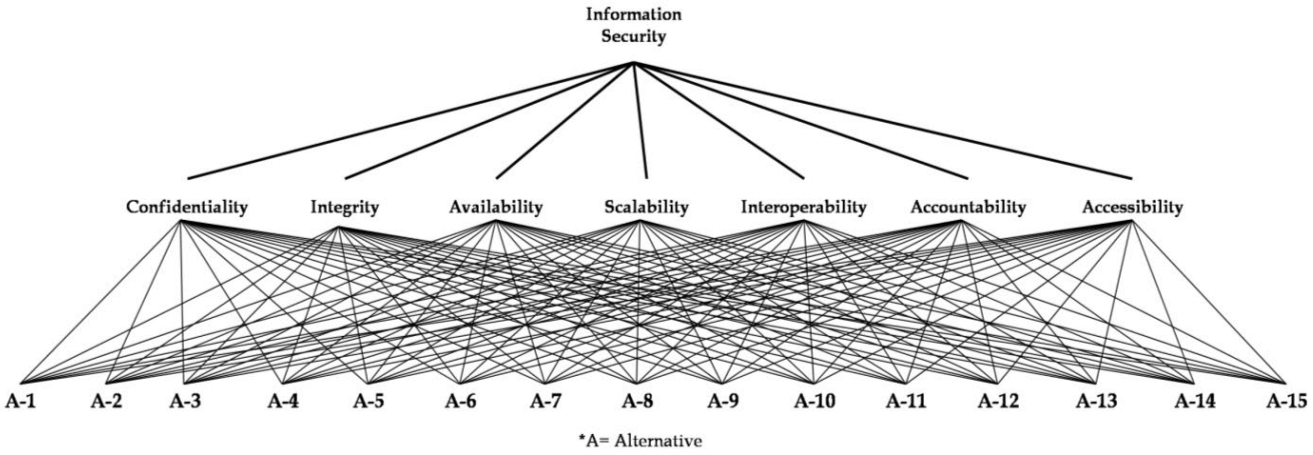


FIGURE 1. Hierarchical view of various factors.

organization. Authors have chosen and selected these factors as per the experts' suggestion and analyzed their significance against various types of healthcare data security threat vectors. This type of analysis has been performed by various researchers in their studies [41]. A detailed analysis of the factors has been described in the following table.

The factors and their significance described in table 1 clearly show that the web application developers and experts must essentially focus on the most prioritized factors. This would facilitate in achieving a two pronged target. Firstly, focus on the most relevant factors will result in assuring high end security. Secondly, it would reduce both the time and resources invested in analyzing and accurately evaluating the efficacy of the web application. Hence, the authors have attempted a step-wise methodology that can be entailed for assessing and then prioritizing the factors that significantly determine information security in the healthcare web application. While following this concept, the present study uses an integrated multi-criteria decision method. Furthermore, our study also provides a path for developing an effective information security wall against healthcare data breach attacks through evaluated results.

V. METHODOLOGY FOLLOWED

Information security is an essential part of any web application security. Although many researchers have worked on information security maintenance in healthcare in previous years, a safe and effective healthcare information system still sounds like a dream. There is a need to evaluate the effect of factors that are directly affecting information security in healthcare web applications for providing them an effective security wall. The multi-criteria decision method is the most practiced and used approach for measuring the various factors for any topic. AHP (Analytical Hierarchy Process) is the most effective approach in the other all MCDM approaches. Since AHP is unable to resolve some implications related to accountability of results discussed in the previous work of authors [5], this paper uses a combination of fuzzy and AHP with TOPSIS methodology to assess the security factors ranking according to the steps described in figure 3.

Figure 3 illustrates the prototype or step-wise process that is followed by authors for evaluating the factors priority and its assessment.

Fuzzy Analytical Hierarchy Process (AHP) is an effective and useful method against multi-dimensional decision situation. It provides very crisp and valuable results in an integrated pair- wise matrix [22]. For simple understanding, hybrid approach of fuzzy and analytical hierarchy process uses triangular fuzzy number to evaluate the wrights of the factors that are provided by a hierarchy. Saaty proposed the concept of fuzzy AHP for the first time in his paper [23].

In our study, we have used a combined hybrid approach of fuzzy AHP-TOPSIS for the evaluation of factors described and illustrated in figure 1. Towards this intent, a questionnaire to locate the factors that affect the information security in healthcare web application was profiled and distribute it in between experts from various healthcare industry and IT development field. The opinions and the suggestions of the experts were collated to prepare a hierarchy in order to cover the basic issues of healthcare web applications regarding information security. After a successful tree hierarchy creation, in the next step, the linguistic values were converted into triangular fuzzy numbers (TFN) for every individual element of hierarchy. For making the analysis part simple and easy, authors have used triangular fuzzy numbers (TFN) in the evaluation process [5]. The value of triangular fuzzy number is in between 0 and 1.Similarly, the membership function of triangular fuzzy numbers have been described in equation (1) and (2) and the evaluated value of numbers are described in between 1,2,3,4....9.

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

TABLE 1. Factors and their significance in web application security.

Factor	Significance against threat
Confidentiality	Managing confidentiality of web application during its development phase can protect the healthcare organization from packet tracing, sniffing, session hijacking and many other confidentiality breach attacks.
Integrity	Integrity management plays a key role in web application security and its management from web application development can provide security against various network related attacks like, Salami attack, Data diddling attack, Man in the middle attack and various other attacks.
Availability	A concrete availability managed web application can prevent against DDoS, SYN flood, Ping flood and many other availability targeting attacks.
Scalability	A solid management of scalability from development phase can make a web application performance more accurate and prevent attacks like buffer overflow.
Interoperability	Management of interoperability can provide a relaxation to the web application from data error and miss match in data formatting standard.
Accountability	Managing accountability can allow the web application to follow a basic rule of security called non-repudiation or in simple words authenticity for every node in order to secure data handling in web application architecture.
Accessibility	A well-managed accessibility factor can produce a highly secure web application with restricted and authenticated access control environment.

$$\mu_a(x) = \begin{cases} \frac{x}{mi - lo} - \frac{b}{mi - lo} & x \in [lo, mi] \\ \frac{x}{mi - up} - \frac{u}{mi - up} & x \in [mi, up] \\ 0 & \text{Otherwise} \end{cases} \quad (2)$$

In the above triangular membership function l, mi and u are showing the lower, middle and upper limit of TFN. Triangular fuzzy numbers idea and description is illustrated in figure 2. In the above figure 2, *l, mi, u* represent the triangular fuzzy numbers. Further in this paper, Table 2 describes the standard value system for assigning ranking after evaluating the weights of factors through the methodology.

Furthermore, for converting the numeric values into triangular fuzzy number, the authors have used equation (3-6).

$$n_{ij} = (l_{ij}, m_{iij}, u_{ij}) \quad \text{where } l_{ij} \le m_{iij} \le u_{ij} \quad (3)$$

$$l_{ij} = (J_{ijd}) \quad (4)$$

$$m_{iij} = (J_{ij1}, J_{ij2}, J_{ij3})^{1/x} \quad (5)$$

$$= (J_{ijd}) \quad (6)$$

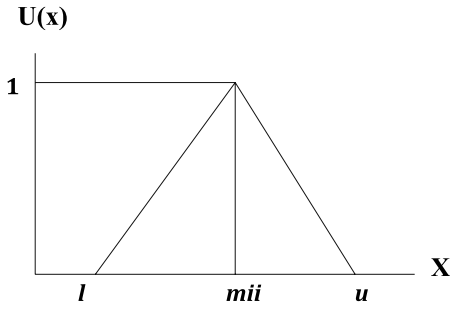


FIGURE 2. TFN.

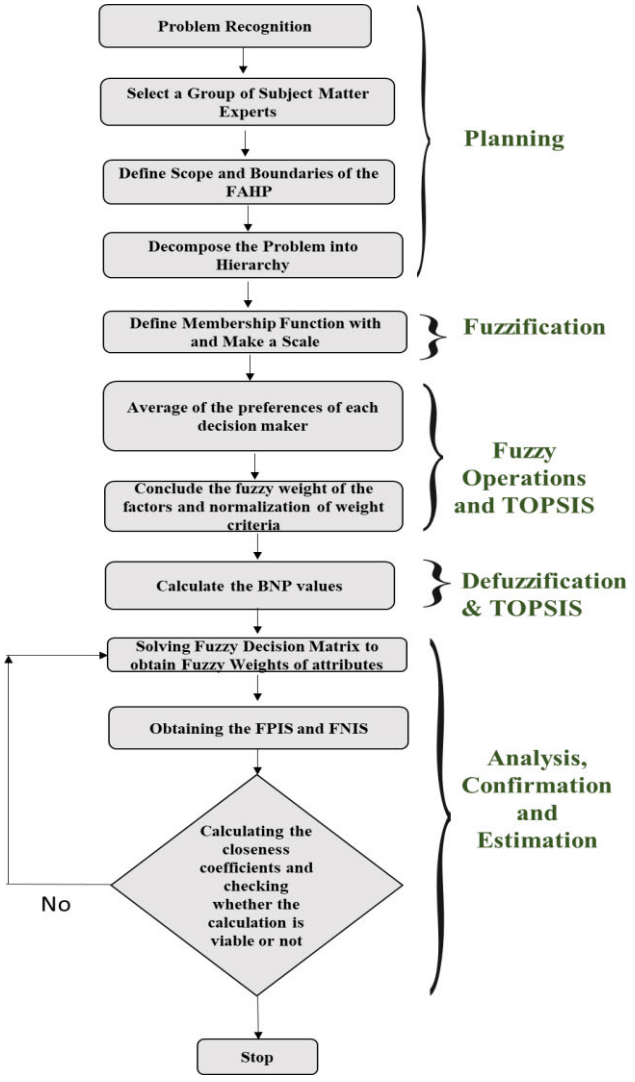


FIGURE 3. Step-wise methodology for evaluation.

From equation (3 – 6), lower limit, middle limit and upper limit is described and represented through l_{ij}, m_{iij} and u_{ij} respectively. For combining the TFN values, equation (7-9) is used by evaluator.

$$(l_1, mi_1, u_1) + (l_2, mi_2, u_2) = (l_1 + l_2, mi_1 + mi_2, u_2 + u_2) \quad (7)$$

TABLE 2. Triangular fuzzy number scale.

Saaty Scale Definition	F T 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 adjacent scales	(1 ,2, 3)
4		(3 ,4, 5)
6		(5 ,6, 7)
8		(7 ,8, 9)

$$(l_1, mi_1, u_1) \times (l_2, mi_2, u_2) = (l_1 \times l_2, mi_1 \times mi_2, u_1 \times u_2) \tag{8}$$

$$(l1, mi1, u1) - 1 = (1/\mathrm{u}_1, 1/\mathrm{m}_{i1}, 1/l_1) \tag{9}$$

After, evaluating all the TFN values, the analysts need to construct an *nxn* fuzzy comparison matrix through equation (10).

$$\tilde{A^d} = \begin{bmatrix} \tilde{k}^d_{11} & \tilde{k}^d_{12} & \tilde{k}^d_{1n} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots \\ \tilde{k}^d_{n1} & \tilde{k}^d_{n2} & \tilde{k}^d_{nn} \end{bmatrix} \tag{10}$$

In this context, if more than one preference is available during the calculation process, then the examiner uses following equation (11) to find the average of preferences.

$$\tilde{k}_{ij} = \sum_{d=1}^{d} \tilde{k}^d_{ij} \tag{11}$$

After calculating the average preference, the evaluators updated the fuzzy integrated comparison matrix for hierarchy prepared through the practitioners' views. For calculating this step, the experts used the following equation (12):

$$\tilde{A} = \begin{bmatrix} \tilde{k_{11}} & \cdots & \tilde{k_{1n}} \\ \ldots & \ddots & \ldots \\ \tilde{k_{n1}} & \cdots & \tilde{k}_{nn} \end{bmatrix} \tag{12}$$

Now, examiner uses equation (13) to assess the geometric mean and fuzzy weights of the factors.

$$\tilde{P}_i = \left(\prod_{j=1}^{n} \tilde{k}_{ij}\right)^{1/n}, \quad i = 1, 2, 3, 4, \ldots..\mathrm{n} \tag{13}$$

In the end of the AHP methodology, equation (14 – 16) is used by evaluator to normalize and calculate the average of factors' weights.

$$\tilde{w}_i = \tilde{p}_i \oplus (\tilde{p}_2 \oplus \tilde{p}_3 \ldots. \oplus \tilde{p}_n)^{-1} \tag{14}$$

$$\mathrm{M_i} = \frac{\tilde{w}_1 \oplus \tilde{w}_2 \ldots..\oplus \tilde{w}_\mathrm{n}}{\mathrm{n}} \tag{15}$$

$$\mathrm{Nr_i} = \frac{\mathrm{M_i}}{\mathrm{M_1} \oplus \mathrm{M_2} \oplus \ldots\ldots \oplus \mathrm{M_n}} \tag{16}$$

After calculating the concluding weights and its average, the examiners use the equation (17) for evaluating BNP value from the calculated weights.

$$BNPwD1 = \frac{[(uw1 - lw1) + (miw1 - lw1)]}{3} + lw1 \tag{17}$$

TABLE 3. Scale for ratings.

Linguistic Variable	Corresponding TFN
Very Poor	(0, 1, 3)
Poor (P)	(1, 3, 5)
Fair (F)	(3, 5, 7)
Good (G)	(5, 7, 9)
Very good (VG)	(7, 9,10)

A. FUZZY TOPSIS

TOPSIS is a methodology that is additionally used with the MCDM approaches for evaluating the results calculated by MCDM methodologies through alternatives assessment in n-dimensional space. Additionally, in our case this TOPSIS methodology uses the fuzzy numbers rather than using precise numbers for evaluation. A detailed description of the methodology is described below:

After evaluating the weights from fuzzy AHP methodology, the TOPSIS approach uses equation (18) and table 3 to prepare a comparison matrix.

$$\tilde{K} = \begin{array}{c} \\ A_1 \\ \ldots\ldots \\ A_m \end{array} \begin{array}{c} \begin{array}{ccc} C_1 & \ldots\ldots & C_n \end{array} \\ \begin{bmatrix} \tilde{x}_{11} & \cdots & \tilde{x}_{1n} \\ \ldots & \ddots & \ldots \\ \tilde{x}_{m1} & \cdots & \tilde{x}_{mn} \end{bmatrix} \end{array} \tag{18}$$

Thereafter, the matrix is normalized by the equation (19) to prepare a normalized comparison matrix though equation (20).

$$\tilde{P} = \left[\tilde{P}_{ij}\right]_{m \times n} \tag{19}$$

$$\tilde{Q} = \left[\tilde{q}_{ij}\right]_{m \times n} i = 1, 2, 3, \ldots \ldots..m \quad j = 1, 2, 3, 4, \ldots \ldots n \tag{20}$$

Finally, after evaluating the entire steps, the examiners calculated the gap degree of factors in alternatives by the equation (21).

$$C\tilde{C} = \frac{\tilde{k}_i^-}{\tilde{k}_i^+ + \tilde{k}_i^-} = 1 - \frac{\tilde{k}_i^+}{\tilde{k}_i^+ + \tilde{k}_i^-}, \quad i = 1, 2, \ldots\ldots., m \tag{21}$$

Similarly, as a final result of the evaluation process authors find the ranking of factors described in hierarchy.

VI. DATA EVALUATION AND RESULT ASSESSMENT

Analyzing the security of any web application through a mathematical scientific process is a challenging task [44], [45]. This study, in particular, uses a well examined and verified hybrid fuzzy AHP-TOPSIS methodology towards developing a standardized process which can be enlisted by the practitioners. The accuracy and efficacy of this methodology has been proven and well established by our research team in our earlier endeavours.

For the present analysis, the authors have compiled the suggestions from 80 experts from the healthcare industry and IT sector to identify real and validated facts and factors. In order

to conduct evaluation through methodology, the authors used equation (1-9) and table 1 for converting linguistic value into triangular fuzzy numbers and numeric values. After the evaluation and conversion, the comparison matrix of factors is constructed and displayed in table 4.

TABLE 4. Integrated fuzzy comparison matrix of different factors.

	F1	F2	F3	F4	F5	F6	F7
F1 (Confidentiality)	1.000, 1.000, 1.000	0.770, 1.000, 1.000	0.900, 1.000, 1.000	0.670, 1.000, 1.000	1.000, 1.000, 1.000	1.000, 1.000, 1.350	1.000, 1.000, 1.500
F2 (Integrity)	0.770, 1.000, 1.000	1.000, 1.000, 1.000	0.900, 1.000, 1.000	0.900, 1.000, 1.000	1.000, 1.000, 1.000	1.000, 1.350, 1.350	1.000, 1.350, 1.850
F3 (Availability)	0.710, 0.870, 1.000	0.770, 1.000, 1.150	1.000, 1.000, 1.000	0.770, 1.000, 1.000	1.000, 1.000, 1.150	1.000, 1.000, 1.500	1.000, 1.150, 1.650
F4 (Scalability)	0.440, 0.570, 0.810	0.550, 0.770, 1.000	0.620, 0.900, 1.000	1.000, 1.000, 1.000	0.670, 1.000, 1.000	0.900, 1.000, 1.000	1.000, 1.000, 1.000
F5 (Interoperability)	0.770, 1.000, 1.000	1.000, 1.000, 1.000	0.900, 1.000, 1.350	0.900, 1.000, 1.000	1.000, 1.000, 1.350	1.000, 1.000, 1.690	1.000, 1.350, 1.850
F6 (Accountability)	0.710, 0.870, 1.000	0.770, 1.000, 1.150	1.000, 1.000, 1.000	0.770, 1.000, 1.000	1.000, 1.000, 1.150	1.000, 1.000, 1.000	1.000, 1.150, 1.650
F7 (Accessibility)	0.440, 0.570, 0.810	0.550, 0.770, 1.000	0.620, 0.900, 1.350	0.500, 0.670, 1.000	0.670, 1.000, 1.000	0.900, 1.000, 1.000	1.000, 1.000, 1.000

Additionally, now through the equation (11-16), the authors calculated the weights of the factors. Then, through the equation (21), the BNP value of factors was evaluated. Table 5 below represents the final weights for the factors.

TABLE 5. Weights of factors.

Factors	Weights	BNP	Rank
F1 (Confidentiality)	0.1252, 0.1753, 0.2601	0.2130	1
F2 (Integrity)	0.1091, 0.1532, 0.2142	0.1740	3
F3 (Availability)	0.1042, 0.1393, 0.1971	0.1420	4
F4 (Scalability)	0.1141, 0.1563, 0.2292	0.1810	2
F5 (Interoperability)	0.0981, 0.1362, 0.1823	0.1280	5
F6 (Accountability)	0.0851, 0.1241, 0.1633	0.0920	6
F7 (Accessibility)	0.0772, 0.1172, 0.1583	0.0780	7

Thereafter, the alternative for validating the calculated results was evaluated. Table 5 describes the ranking and priority of various factors according to evaluation. These ranks will help the developers to focus on specific factors for developing effective security mechanisms. The analysis cites that the developers must give high priority to: First, the confidentiality; second, the scalability; third, the integrity and so on during healthcare web application development phase. Fifteen projects are taken by authors as alternatives from local hospital software of Varanasi. All alternatives are represented by *A1, A2, A3*.....*A15* in tables and figure 1. For the purpose of evaluation, we took the alternatives of highly sensitive projects of hospital software. For the assessment, we referred to the technological data from the equations (3–9) that is illustrated in table 6. After the entire calculations and evaluations, table 7 shows the normalized fuzzy matrix

TABLE 6. Subjective cognition results.

Alternatives/ Factors	F1	F2	F3	F4	F5	F6	F7
A1	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000	5.6200, 7.6200, 9.3100	5.7600, 7.7600, 9.3800	5.0000, 7.0000, 9.0000	3.7600, 5.7600, 7.7600	6.2400, 8.2400, 9.6200
A2	7.0000, 9.0000, 10.000	3.0000, 5.0000, 7.0000	5.0000, 7.0000, 9.0000	4.3800, 6.3800, 8.3800	7.0000, 9.0000, 10.000	1.6200, 3.6200, 5.6200	5.6200, 7.6200, 9.3100
A3	6.2400, 8.2400, 9.6200	3.0000, 5.0000, 7.0000	4.3800, 6.3800, 8.3800	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000	5.6200, 7.6200, 9.3100	5.7600, 7.7600, 9.3800
A4	5.6200, 7.6200, 9.3100	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000	5.0000, 7.0000, 9.0000	4.3800, 6.3800, 8.3800
A5	7.0000, 9.0000, 10.000	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000	7.0000, 9.0000, 10.000	3.0000, 5.0000, 7.0000	4.3800, 6.3800, 8.3800	3.0000, 5.0000, 7.0000
A6	6.2400, 8.2400, 9.6200	5.0000, 7.0000, 9.0000	3.7600, 5.7600, 7.7600	6.2400, 8.2400, 9.6200	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000
A7	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000	5.6200, 7.6200, 9.3100	5.7600, 7.7600, 9.3800	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000	7.0000, 9.0000, 10.000
A8	7.0000, 9.0000, 10.000	3.0000, 5.0000, 7.0000	5.0000, 7.0000, 9.0000	4.3800, 6.3800, 8.3800	5.0000, 7.0000, 9.0000	3.7600, 5.7600, 7.7600	6.2400, 8.2400, 9.6200
A9	6.2400, 8.2400, 9.6200	3.0000, 5.0000, 7.0000	4.3800, 6.3800, 8.3800	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000	5.6200, 7.6200, 9.3100	5.7600, 7.7600, 9.3800
A10	7.0000, 9.0000, 10.000	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000	7.0000, 9.0000, 10.000	3.0000, 5.0000, 7.0000	5.0000, 7.0000, 9.0000	4.3800, 6.3800, 8.3800
A11	6.2400, 8.2400, 9.6200	5.0000, 7.0000, 9.0000	3.7600, 5.7600, 7.7600	6.2400, 8.2400, 9.6200	3.0000, 5.0000, 7.0000	4.3800, 6.3800, 8.3800	3.0000, 5.0000, 7.0000
A12	5.6200, 7.6200, 9.3100	7.0000, 9.0000, 10.000	1.6200, 3.6200, 5.6200	5.6200, 7.6200, 9.3100	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000
A13	5.7600, 7.7600, 9.3800	6.3800, 8.3800, 9.6900	4.3800, 6.3800, 8.3800	7.0000, 9.0000, 10.000	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000	7.0000, 9.0000, 10.000
A14	7.7600, 9.3800, 10.000	7.0000, 9.0000, 10.000	7.0000, 9.0000, 10.000	6.2400, 8.2400, 9.6200	5.0000, 7.0000, 9.0000	3.7600, 5.7600, 7.7600	6.2400, 8.2400, 9.6200
A15	1.0000, 3.0000, 5.0000	3.0000, 5.0000, 7.0000	7.0000, 9.0000, 10.000	5.6200, 7.6200, 9.3100	7.0000, 9.0000, 10.000	1.6200, 3.6200, 5.6200	5.6200, 7.6200, 9.3100

evaluated through equation (20. And after that, equation (21) is used by the authors to evaluate the satisfaction degree and gap degree of factors that has been described in table 8.

Table 8 represents the last and overall results of the case study. The results described in this table are showing that gap degree is between *good* and *very good.* Therefore, it can be conclusively drawn that information security of various selected alternatives is in *good* and *very good* condition.

VII. THREAT TO VALIDITY

Validating the calculated results in a scientific calculation is a significant step and process. Sensitivity analysis is a process of threat to validity that helps the researchers to authenticate their results by numeric calculation. A threat to validity step provides an idea to researcher about how different sources of results affect the proposed mathematical model in study. This section helps in understanding the effectiveness and certainty of results by changing the important criteria. In order to implement threat to validity in this research article,

TABLE 7. Weighted normalized fuzzy-decision matrix.

Alternative/ Factors	F1	F2	F3	F4	F5	F6	F7
A1	0.03000, 0.04000, 0.04800	0.01100, 0.01800, 0.02500	0.02300, 0.03100, 0.03800	0.03000, 0.04000, 0.04800	0.01100, 0.01800, 0.02500	0.02300, 0.03100, 0.03800	0.03000, 0.04000, 0.04800
A2	0.02300, 0.03300, 0.04300	0.01100, 0.01800, 0.02500	0.02000, 0.02800, 0.03600	0.02300, 0.03300, 0.04300	0.01100, 0.01800, 0.02500	0.02000, 0.02800, 0.03600	0.02300, 0.03300, 0.04300
A3	0.01600, 0.02600, 0.03700	0.01200, 0.02100, 0.02900	0.01500, 0.02200, 0.02800	0.01600, 0.02600, 0.03700	0.01200, 0.02100, 0.02900	0.01500, 0.02200, 0.02800	0.01600, 0.02600, 0.03700
A4	0.01600, 0.02600, 0.03700	0.01200, 0.02100, 0.02900	0.01000, 0.01700, 0.02400	0.01600, 0.02600, 0.03700	0.01200, 0.02100, 0.02900	0.01000, 0.01700, 0.02400	0.01600, 0.02600, 0.03700
A5	0.03600, 0.04700, 0.05200	0.01100, 0.01800, 0.02500	0.01200, 0.02000, 0.02800	0.03600, 0.04700, 0.05200	0.01100, 0.01800, 0.02500	0.01200, 0.02000, 0.02800	0.03600, 0.04700, 0.05200
A6	0.03200, 0.04300, 0.05000	0.01800, 0.02500, 0.03200	0.01500, 0.02300, 0.03100	0.03200, 0.04300, 0.05000	0.01800, 0.02500, 0.03200	0.01500, 0.02300, 0.03100	0.03200, 0.04300, 0.05000
A7	0.01200, 0.02000, 0.02800	0.03600, 0.04700, 0.05200	0.03600, 0.04700, 0.05200	0.01100, 0.01800, 0.02500	0.01200, 0.02000, 0.02800	0.03600, 0.04700, 0.05200	0.03600, 0.04700, 0.05200
A8	0.01500, 0.02300, 0.03100	0.03200, 0.04300, 0.05000	0.03200, 0.04300, 0.05000	0.01800, 0.02500, 0.03200	0.01500, 0.02300, 0.03100	0.03200, 0.04300, 0.05000	0.03200, 0.04300, 0.05000
A9	0.06200, 0.07100, 0.07400	0.01600, 0.02600, 0.03700	0.01600, 0.02600, 0.03700	0.03300, 0.04400, 0.05400	0.06200, 0.07100, 0.07400	0.01600, 0.02600, 0.03700	0.01600, 0.02600, 0.03700
A10	0.01500, 0.02200, 0.02800	0.01600, 0.02600, 0.03700	0.01600, 0.02600, 0.03700	0.01200, 0.02100, 0.02900	0.01500, 0.02200, 0.02800	0.01600, 0.02600, 0.03700	0.01600, 0.02600, 0.03700
A11	0.01000, 0.01700, 0.02400	0.01600, 0.02600, 0.03700	0.01600, 0.02600, 0.03700	0.01200, 0.02100, 0.02900	0.01000, 0.01700, 0.02400	0.01600, 0.02600, 0.03700	0.01600, 0.02600, 0.03700
A12	0.01500, 0.02200, 0.02800	0.01600, 0.02600, 0.03700	0.01600, 0.02600, 0.03700	0.01200, 0.02100, 0.02900	0.01500, 0.02200, 0.02800	0.01600, 0.02600, 0.03700	0.01600, 0.02600, 0.03700
A13	0.01000, 0.01700, 0.02400	0.01600, 0.02600, 0.03700	0.01600, 0.02600, 0.03700	0.01200, 0.02100, 0.02900	0.01000, 0.01700, 0.02400	0.01600, 0.02600, 0.03700	0.01600, 0.02600, 0.03700
A14	0.01200, 0.02000, 0.02800	0.03600, 0.04700, 0.05200	0.03600, 0.04700, 0.05200	0.01100, 0.01800, 0.02500	0.01200, 0.02000, 0.02800	0.03600, 0.04700, 0.05200	0.03600, 0.04700, 0.05200
A15	0.01500, 0.02300, 0.03100	0.03200, 0.04300, 0.05000	0.03200, 0.04300, 0.05000	0.01800, 0.02500, 0.03200	0.01500, 0.02300, 0.03100	0.03200, 0.04300, 0.05000	0.03200, 0.04300, 0.05000

the authors chose 15 alternative projects or experiments for testing sensitivity. Table 9 describes the analyzed results of sensitivity analysis in detail. Figure 4 portrays a graphical representation of sensitivity analysis for easy understanding and clear details.

Second column of table 8 represents the original weights of this publication. According to the original values, factor 1 has the highest satisfaction degree. Furthermore after calculating the sensitivity of results, we found that it is crucial for methodology to assess the factor 1 always as the topmost priority. The results from table 9 show that calculated results are risky and it is evident that variation in the whole information security factors is negligible. A result variation presents a view that the sensitivity of results depends on the weights of the factors.

TABLE 8. Closeness coefficients to aspired level among different alternatives.

Alternatives	di-	di+	Satisfaction degree of CCi
A1	0.7300	22.1200	0.04012
A2	0.7000	22.2100	0.04121
A3	0.7200	22.3200	0.04411
A4	0.7300	22.4200	0.04331
A5	0.6700	22.0000	0.04914
A6	0.6800	22.1400	0.03201
A7	0.6400	22.2400	0.03510
A8	0.7500	22.3100	0.03340
A9	0.7200	22.4300	0.03103
A10	0.6800	22.1400	0.04400
A11	0.7000	22.0100	0.03602
A12	0.7300	22.0500	0.02511
A13	0.6600	22.0000	0.04731
A14	0.6700	22.1400	0.03101
A15	0.6500	22.2400	0.02210

For our investigations, we adopted a confusion matrix to measure the accuracy of the results as well as the standard error rate. A confusion matrix is scientific approach that has been used to evaluate the performance of the proposed method and its' results [52]. Table 10 represents a confusion matrix in 2*2 dimensions. The matrix works with the help of four types of numbers called TP (True Positive), TN (True Negative), FP (False Positive) and FN (False Negative).

Additionally, in our case, [1]TN represents the values that did not fluctuate when resources were actually changed; [2]FN represents the value that did not fluctuate, as predicted by authors, [3]FP presents the value that fluctuated, as predicted by authors; and [4]TP presents the value that actually fluctuated. Enlisting the tabulations in table 10, we evaluated the accuracy with the following equation (a).

$$Accuracy = \frac{TP + TN}{All} \quad \text{(a)}$$

Thereafter, we calculated the error rate of results with the help of following equation (b).

$$Error\ Rate = \frac{FP + FN}{TN + FP + FN + TP} \quad \text{(b)}$$

Equations (a) and (b) were used to calculate the accuracy of result. The accuracy of the results was 82%, and error rate of results was 0.5% averages. The outcomes of confusion matrix calculation illustrate that evaluated results in this study are highly accurate and have nominal error rate.

VIII. COMPARISON WITH CLASSICAL AHP-TOPSIS APPROACH

Comparing results from other methodologies can provide a clear and significant view on calculated results. It is an important part of scientific calculation to compare the results of same data from various techniques.

TABLE 9. Sensitivity analysis.

Alternatives	Original Weights	F1	F2	F3	F4	F5	F6	F7
A1	0.04012	0.05922	0.06192	0.02128	0.05728	0.02312	0.02082	0.01292
A2	0.04121	0.05281	0.06381	0.01919	0.05859	0.00921	0.01391	0.02981
A3	0.04411	0.05971	0.06491	0.01289	0.04589	0.03171	0.02811	0.01531
A4	0.04331	0.05381	0.06051	0.01509	0.04649	0.04521	0.03321	0.00339
A5	0.04914	0.05694	0.06054	0.01826	0.05066	0.01894	0.01894	0.01854
A6	0.03201	0.05501	0.06131	0.01399	0.04569	0.03251	0.02701	0.01081
A7	0.03510	0.05010	0.06280	0.01550	0.04790	0.02780	0.02610	0.01250
A8	0.03340	0.05890	0.05540	0.03480	0.07230	0.01640	0.02740	0.00160
A9	0.03103	0.05053	0.05903	0.01297	0.04397	0.01903	0.02053	0.02283
A10	0.04400	0.05030	0.06930	0.01670	0.05270	0.0260	0.02460	0.02160
A11	0.03602	0.05402	0.06802	0.01158	0.04558	0.01872	0.02242	0.03302
A12	0.02511	0.05751	0.07381	0.00989	0.04149	0.03451	0.03011	0.01551
A13	0.04731	0.05864	0.06814	0.01686	0.05236	0.02414	0.02414	0.02164
A14	0.03101	0.05251	0.06651	0.01699	0.05149	0.02201	0.02201	0.01901
A15	0.02210	0.05110	0.06110	0.01490	0.04890	0.01610	0.02010	0.02810

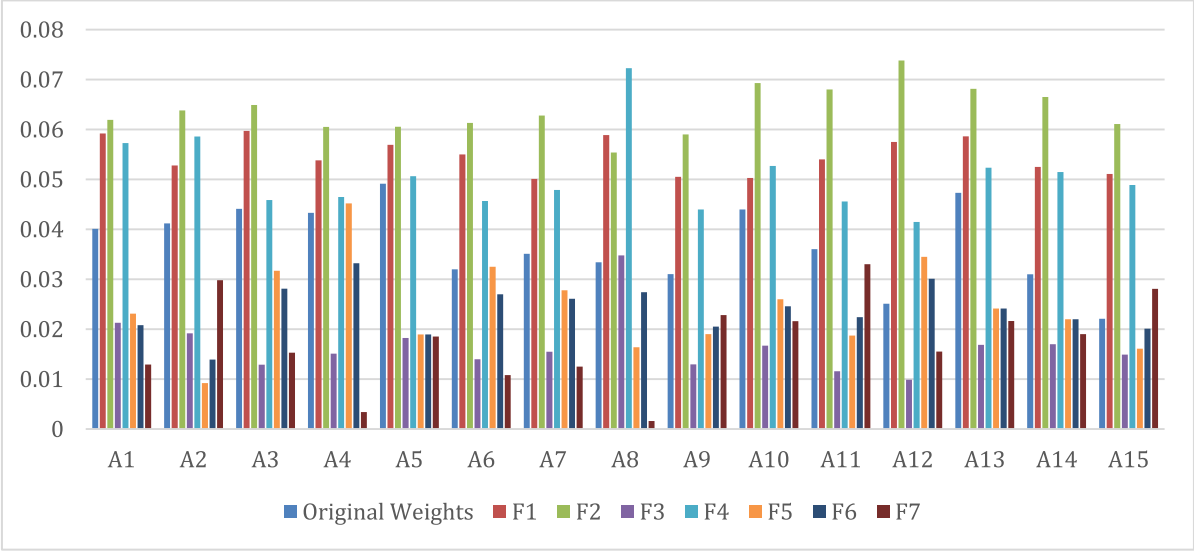


FIGURE 4. Graphical view of sensitivity analysis.

TABLE 10. Confusion matrix.

Actual/Predicted		Predicted	
		NO	YES
Actual	NO	[TN][1]	[FP][3]
	YES	[FN][2]	[TP][4]

Several research initiatives use MCDM methods to evaluate various factors and their effects in different sectors and fields. Agrawal *et al.* published an article in which the authors evaluated the condition of software durability through 3 layered tree structure [32]. They selected only 3 factors on first layer of structure and used the AHP methodology to assess the durability. Yet another research study by Rajeev Kumar *et al.* evaluated the harmful factors of healthcare web applications through same methodology with two layered tree structure [34]. The paper calculated the results with 4 factors in first layer and used the same fuzzy-AHP TOPSIS methodology. The calculation and evaluation in this study further iterate that the methodology adopted by the researchers in [34] is effective and useful. Furthermore, in the present empirical analysis, we have used7 factors in 1st layer of structure and evaluated the results through fuzzy-AHP TOPSIS method. The adopted methodology also discards the implications that are discussed by [8].

Contributors of this study have used a classical AHP-TOPSIS method for comparing the result of Fuzzy AHP-TOPSIS. This type of comparison illustrates the capabilities and accuracy of selected approach in the comparison of previous technique. Analyzed results show that selected

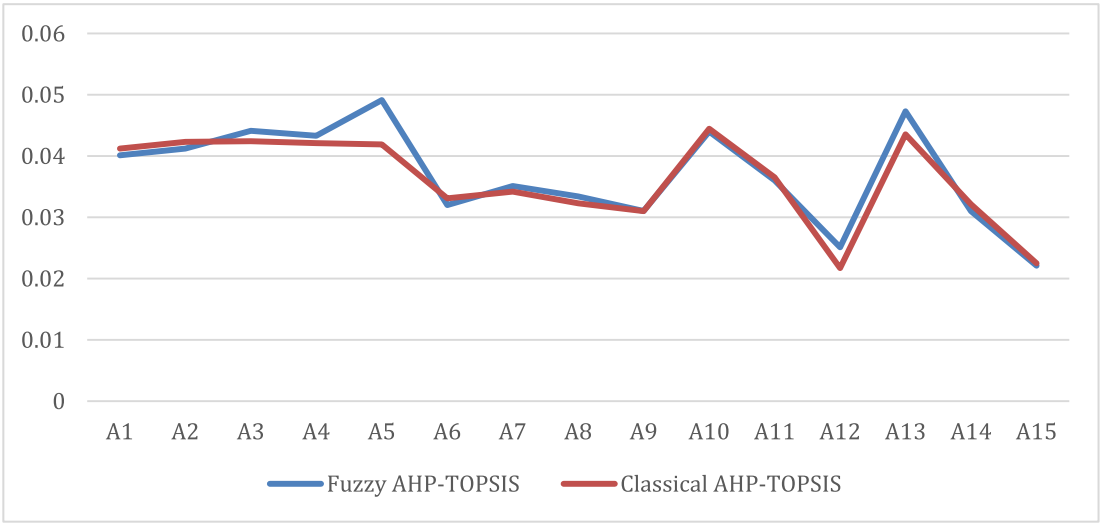


FIGURE 5. Graphical Representation of comparison.

fuzzy AHP-TOPSIS methodology can provide a slightly accurate and better result in the comparison of previous classical AHP-TOPSIS method. Addition of fuzzy set theory in the old methodology gives a better result and accuracy. Details of analyzed results are: in classical AHP-TOPSIS, the procedure for selecting and analyzing data is the same as Fuzzy AHP-TOPSIS method except for the process of fuzzification. The data is selected in its original numeric number. A comparative view on the results of both the techniques is portrayed in table 11 and figure 5. The results of classical AHP-TOPSIS methodology with fuzzy AHP-TOPSIS methodology is highly correlated (Person correlation = 0.7681). Results of both the techniques clearly illustrate that fuzzy based approach provides better results in the comparison of classical technique.

TABLE 11. Comparative view on results from both techniques.

Alternatives	Fuzzy AHP-TOPSIS	Classical AHP-TOPSIS
A1	0.04012	0.04122
A2	0.04121	0.04231
A3	0.04411	0.04241
A4	0.04331	0.04211
A5	0.04914	0.04190
A6	0.03201	0.03311
A7	0.03510	0.03420
A8	0.03340	0.03230
A9	0.03103	0.03101
A10	0.04400	0.04445
A11	0.03602	0.03652
A12	0.02511	0.02171
A13	0.04731	0.04354
A14	0.03101	0.03212
A15	0.02210	0.02250

IX. DISCUSSION

Previous data breach statistics on the attack trends point out that healthcare security is at maximum risk. Sensitive information is one of the most valuable assets of any sector, especially in case of healthcare sector. A breach in healthcare information can be devastating for the organization and, much worse, be life-threatening for a patient. With the current medical world evolving into a digital universe and adopting computers and internet in every facet, a viable and efficacious information security approach is the fundamental need for the web applications in the healthcare industry.

This research initiative evaluates the various factors of information security that are directly affecting the information security in healthcare web applications. The outcome of this research initiative will help the future researchers and the practitioners to develop information security assured web applications from the development phase itself. Many researchers are working specifically on one factor of information security in healthcare sector. However, an integrated approach with effective MCDM technique as an evaluation method is relatively less. Additionally, our study also provides highly accurate results with minimal error rate as demonstrated in the section on threat to validity in the paper. For a more thorough an expansive investigation, the threat to validity was undertaken in two scenarios. The first scenario describes the sensitivity of results in various conditions where resources get restricted. The second context is the confusion matrix method that measures the performance of evaluated results and model through mathematical equations. Hence this study posits an inventive solution. Moreover, the study bases its propositions on empirical evidence mapped through a case study involving a live project in a healthcare institution.

This study's contribution to the possible research and policy forums is listed below:

- The results of this study will help the researchers and developers in developing novel information security models as well as securing the web application right from its design phase.
- Healthcare organizations can enhance their information security methods by alluding to the results of this research and improvise on their brand credibility.

- The case study results and findings can aid in formulation of policies that are much needed to create an enhanced, informed and viable environment for highly secure information systems in the healthcare sector.
- Research ideology that is used in this paper can also be used in various other sectors and perspectives for security-enhancement.
- The addition of machine learning approach with selected MCDM methodology in our paper will also provide effective and advanced results with less manpower consumption and time.

With specific relevance to future research investigations that can be undertaken in this domain, we would also emphasize on the need and scope to analyze the threat model and its adversary benefits for healthcare infrastructure, especially for healthcare information security. Similarly, there is an immense need to create a perfect and balanced threat model for healthcare information security through a literature examination approach. Moreover, prospective research endeavours can also examine web application security by analyzing OWASP, CVE listed threats and their effect on software quality. This research could have certain delimits which the authors have cited below:

- The volume of data that is collected for web applications is small in comparison of big healthcare service providers. Due to this limitation of the study, the results can differ in some conditions.
- There are many sub-factors which indirectly affect information security. But these factors have not been discussed in this research study.

X. CONCLUSION

Recent trends of cyber-attacks portend massive data breaches in the healthcare industry. Unless the cyber security experts and practitioners develop information security systems that are both effective and feasible, the digital health data is at huge risk. Towards this intent, the authors of this research study recommend that implementing security in-between web application development is the most effective way to secure a web application. To establish the workability of this methodology, the authors of this study provided a systematic path and evaluated results which were drawn from 15 different projects of local hospital software of Varanasi. The findings of this study would be an integral referral point in the efforts of all researchers and developers working in the domain of secure web applications.

ACKNOWLEDGMENT

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

REFERENCES

[1] (2016). *How Evolving Healthcare Cybersecurity Threats Affect Providers*. Accessed: Mar. 10, 2020. [Online]. Available: https://healthitsecurity.com/features/how-evolving-healthcare-cybersecurity-threats-affect-providers

[2] (2016). *Understanding Web Application Security in Healthcare*. Accessed: Mar. 10, 2020. [Online]. Available: https://healthitsecurity.com/news/understanding-web-application-security-in-healthcare

[3] (2019). *Healthcare Data Breach Statistics*. Accessed: Mar. 10, 2020. [Online]. Available: https://www.hipaajournal.com/healthcare-data-breach-statistics/

[4] (Jul. 2019). *Healthcare Data Breach Report*. Accessed: Mar. 10, 2020. [Online]. Available: https://www.hipaajournal.com/july-2019-healthcare-data-breach-report/

[5] R. Kumar, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal, and R. A. Khan, "A knowledge-based integrated system of hesitant fuzzy set, AHP and TOPSIS for evaluating security-durability of Web applications," *IEEE Access*, vol. 8, pp. 48870–48885, 2020, doi: 10.1109/ACCESS.2020.2978038.

[6] A. Mardani, A. Jusoh, K. Nor, Z. Khalifah, N. Zakwan, and A. andValipour, "Multiple criteria decision-making techniques and their applications-a review of the literature from 2000 to 2014," *Econ. Res.-EkonomskaIstraživanja*, vol. 28, no. 1, pp. 516–571, 2015.

[7] (Oct. 2019). *Healthcare Data Breach Report*. Accessed: Mar. 12, 2020. [Online]. Available: https://www.hipaajournal.com/october-2019-healthcare-data-breach-report/

[8] D. Garg, S. Luthra, and A. Haleem, "Ranking of performance measures of GSCM towards sustainability: Using analytic hierarchy process," *Int. J. SocManag. Econ. Bus Eng.*, vol. 8, no. 3, pp. 764–770, Feb. 2014.

[9] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Comput.*, vol. 5, no. 1, pp. 31–37, Oct. 2018.

[10] E. Afful-Dadzie, S. Nabareseh, Z. K. Oplatková, and P. Klímek, "Model for assessing quality of online health information: A fuzzy VIKOR based method," *J. Multi-Criteria Decis. Anal.*, vol. 23, nos. 1–2, pp. 49–62, 2016.

[11] A. Theodouli, S. Arakliotis, K. Moschou, K. Votis, and D. Tzovaras, "On the design of a blockchain-based system to facilitate healthcare data sharing," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Aug. 2018, pp. 699–706.

[12] I. Chiuchisan, D.-G. Balan, O. Geman, T. Chiuchisan, and A. Gordin, "A security approach for health care information systems," in *Proc. E-Health Bioeng. Conf. (EHB)*, Jun. 2017, pp. 721–724.

[13] S. G. Langer, "Cyber-security issues in healthcare information technology," *J. Digit. Imag.*, vol. 30, no. 1, pp. 117–125, 2016.

[14] E. Mehraeen, H. Ayatollahi, and M. Ahmadi, "Health information security in hospitals: The application of security safeguards," *Acta Inform. Medica*, vol. 24, no. 1, p. 47, 2016.

[15] *Here's How Much Your Personal Information Selling for on the Dark Web*. Accessed: Jun. 22, 2020. [Online]. Available: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

[16] *Web Application Security*. Accessed: Mar. 12, 2020. [Online]. Available: https://www.techopedia.com/definition/24377/web-application-security

[17] A. Appari and M. E. Johnson, "Information security privacy in healthcare: Current state of research," *Int. J. Internet Enterprise Manage.*, vol. 6, no. 4, pp. 279–314, 2010.

[18] X. Ren, Z. Wang, Y. Wu, Y. Li, M. Chen, Y. Zhai, and Y. Li, "Design and implementation of a message-based regional telemedicine system to achieve high availability and scalability," *Telemedicine and E-Health*, vol. 25, no. 3, pp. 243–249, 2018.

[19] A. Appari and M. Johnson, "Information security and privacy in healthcare: Current state of research," *Int. J. Internet Enterprise Manage.*, vol. 6, no. 4, p. 279, 2010.

[20] D. Brinkerhoff, *Accountability and Health Systems: Overview, Framework, and Strategies*. Bethesda, MD, USA: Abt Associates, 2003.

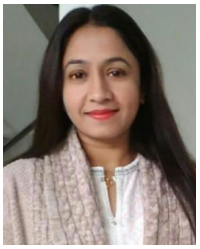
[21] X. Pan, M. P. Kwan, L. Yang, S. Zhou, Z. Zuo, and B. Wan, "Evaluating the accessibility of healthcare facilities using an integrated catchment area approach," *Int. J. Environ. Res. Public Health*, vol. 15, no. 9, p. 2051, 2018.

[22] R. Kumar, M. Zarour, M. Alenezi, A. Agrawal, and R. A. Khan, "Measuring security durability of software through fuzzy-based decision-making process," *Int. J. Comput. Intell. Syst.*, vol. 2019, pp. 627–642, Oct. 2019, doi: 10.2991/ijcis.d.190513.001.

[23] T. L. Saaty, "Transport planning with multiple criteria: The analytic hierarchy process applications and progress review," *J. Adv. Transp.* vol. 29, no. 1, pp. 81–126, 1995.

[24] K. Sahu, "Stability: Abstract roadmap of security," *Amer. Int. J. Res. Sci. Eng. Math.*, vol. 1, pp. 183–186, Oct. 2015.

[25] A. K. Pandey, A. I. Y. B. A. Khan, M. M. Alam, A. Agrawal, R. Kumar, and R. A. Khan "Key issues in healthcare data integrity: Analysis recommendations," *IEEE Access*, vol. 8, pp. 15847–15865, 1998.
[26] R. Kumar, S. A. Khan, and R. A. Khan, "Analytical network process for software security: A design perspective," *CSI Trans. ICT*, vol. 4, nos. 2–4, pp. 255–258, Dec. 2016, doi: 10.1007/s40012-016-0123-y.
[27] K. Sahu and R. K. Srivastava, "Revisiting software reliability," *Data Manage., Anal. Innov.*, vol. 254, pp. 221–235, Oct. 2019.
[28] R. Kumar, A. Irshad Khan, Y. B. Abushark, M. M. Alam, A. Agrawal, and R. A. Khan, "An integrated approach of fuzzy logic, AHP and TOPSIS for estimating usable-security of Web applications," *IEEE Access*, vol. 8, pp. 50944–50957, 2020, doi: 10.1109/ACCESS.2020.2970245.
[29] K. Sahu and R. K. Srivastava, "Soft computing approach for prediction of software reliability," *ICIC Express Lett.*, vol. 12, no. 12, pp. 1213–1222, 2018.
[30] K. Sahu and R. K. Srivastava, "Needs and importance of reliability prediction: An industrial perspective," *Inf. Sci. Lett.*, vol. 9, no. 1, pp. 33–37, 2020.
[31] R. Kumar, A. Baz, H. Alhakami, V. AlhakamiW, A. Agrawal, and R. A. Khan, "A hybrid model of hesitant fuzzy decision-making analysis for estimating usable-security of software," *IEEE Access*, vol. 8, no. 4, pp. 72694–72712, 2020, doi: 10.1109/ACCESS.2020.2987941.
[32] A. Agrawal, M. Zaroor, M. Alenezi, R. Kumar, and A. Khan, "Security durability assessment through fuzzy analytic hierarchy process," *PeerJ Comput. Sci.*, vol. 5, pp. 1–43, Sep. 2019, doi: 10.7717/peerj-cs.215.
[33] K. SahuK, "Software security: A risk taxonomy," *Int. J. Comput. Sci. Eng. Technol.*, vol. 3, pp. 36–41, Oct. 2015.
[34] R. Kumar, K, Pandey, A. Baz, H, Alhakami, A. Alhakami, and M. Baz, "Fuzzy-based symmetrical multi-criteria decision-making procedure for evaluating the impact of harmful factors of Healthcare information security," *Symmetry*, vol. 12, no. 664, pp. 1–23, 2020, doi: 10.3390/sym12040664.
[35] K. Sahu, "Helpful and defending actions in software risk management: A security viewpoint," *Integr. J. Brit.*, vol. 4, pp. 1–7, Feb. 2015.
[36] R. Kumar, A. Agrawal, and A. Khan, "A wakeup call to data integrity invulnerability," *Comput. Fraud Secur.*, vol. 2020, no. 4, pp. 14–19, 2020, doi: 10.1016/S1361-3723(20)30042-7.
[37] A. Pandey, A. Tripathi, M. Alenezi, and A. K. Khan, "Framework for producing effective efficient secure code through malware analysis," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 2, pp. 497–503, 2020, doi: 10.14569/IJACSA.2020.0110263.
[38] R. Kumar, A. Khan, A. Agrawal, and A. Khan, "Security assessment through fuzzy delphi analytic hierarchy process," *Lett. Int. J. Res. Surv.*, vol. 12, no. 10, pp. 1053–1060, 2018, doi: 10.24507/icicel.12.10.1053.
[39] S. Khan, M. Alenezi, A. Agrawal, R. Kumar, and R. A. Khan, "Evaluating performance of software durability through an integrated fuzzy-based symmetrical method of ANP and TOPSIS," *Symmetry*, vol. 12, no. 4, pp. 1–15, Oct. 2020, doi: 10.3390/sym12040493.
[40] R. Kumar, A. Khan, A. Agrawal, and R. Khan, "Measuring the security attributes through fuzzy analytic hierarchy process: Durability perspective," *Int. J. Res. Surv.*, vol. 12, no. 6, pp. 615–620, 2018, doi: 10.24507/icicel.12.06.615.
[41] D. K. Das, S. Zeadally, and D. He, "Taxonomy and analysis of security protocols for Internet of Things," *Future Gener. Comput. Syst.*, 89, pp. 110–125, Oct. 2018, doi: 10.1016/j.future.2018.06.027.
[42] S. Roy, A. K. Das, S. Chatterjee, N. Kumar, S. Chattopadhyay, and J. J. P. C. Rodrigues, "Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications," *IEEE Trans. Ind. Informat.*, vol. 15, no. 1, pp. 457–468, Jan. 2019, doi: 10.1109/TII.2018.2824815.
[43] P. Singh, R. S. Bali, N. Kumar, A. K. Das, A. Vinel, and L. T. Yang, "Secure healthcare data dissemination using vehicle relay networks," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3733–3746, Oct. 2018, doi: 10.1109/JIOT.2018.2865008.
[44] J. Srinivas, A. K. Das, and N. J. K. Rodrigues, "Cloud centric authentication for wearable healthcare monitoring system," *IEEE Trans. Dependable Secure Comput.*, early access, Apr. 19, 2018, doi: 10.1109/TDSC.2018.2828306.
[45] A. Jindal, A. Dua, N. Kumar, A. K. Das, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Providing Healthcare-as-a-Service using fuzzy rule based big data analytics in cloud computing," *IEEE J. Biomed. Health Informat.*, vol. 22, no. 5, pp. 1605–1618, Sep. 2018, doi: 10.1109/JBHI.2018.2799198.
[46] R. Chaudhary, A. Jindal, G. S. Aujla, N. Kumar, A. K. Das, and N. Saxena, "LSCSH: Lattice-based secure cryptosystem for smart healthcare in smart cities environment," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 24–32, Apr. 2018, doi: 10.1109/MCOM.2018.1700787.
[47] F. Wu, L. Xu, and S. Kumari, "Lightweight and anonymous RFID tag authentication protocol with cloud assistance for e-healthcare applications," *J. Ambient Intell. Hum. Comput.*, vol. 9, pp. 919–930, Oct. 2018, doi: 10.1007/s12652-017-0485-5.
[48] M. Wazid, S. Zeadally, A. K. Das, "Analysis of security protocols for mobile healthcare," *J. Med. Syst.*, vol. 40, no. 11, pp. 1–10, Nov. 2016, doi: 10.1007/s10916-016-0596-0.
[49] (2019). *Cybercrime Will Cost Businesses Over 2 Trillion By 2019*, Accessed: May 29, 2020. [Online]. Available: https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion-by-2019
[50] (2019). *DDoS Solutions*. Accessed: May 29, 2020. [Online]. Available: https://www.netscout.com/arbor-ddos
[51] (2019). *Worried about Application Security Threat*. Accessed: May 29, 2020. [Online]. Available: https://www.radware.com/social/webapplicationsecurityreport/?utm_source=RadwareBlog&utm_campaign=FixedCTA&utm_term=7653
[52] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, S. Chen, D. Liu, and J. Li, "Performance comparison and current challenges of using machine learning techniques in cybersecurity," *Energies*, vol. 2020, 13, p. 2509, 2020.



ALKA AGRAWAL received the Ph.D. degree from Babasaheb Bhimrao Ambedkar University, (A Central University), Lucknow. She is currently working as an Assistant Professor with Babasaheb Bhimrao Ambedkar University. She is also a Passionate Researcher and has also published a number of research articles in national and international journals both. She has research/teaching experience of more than 12 years. Her areas of research include software security and software vulnerability. She is currently working in the fields of big data security, genetic algorithms, and software security.

ABHISHEK KUMAR PANDEY received the bachelor's degree in computer applications from Siddhartha University, Kapilvastu, India, in 2018. He is currently pursuing the master's degree in cyber security with Babasaheb Bhimrao Ambedkar University, A Central University, India. He is also a Passionate Researcher and frequently involved in various research initiatives. His research interests include healthcare data security, malware analysis, digital forensic, and cyber security methods. He received the Gold Medalist for his bachelor's degree.

ABDULLAH BAZ (Senior Member, IEEE) received the B.Sc. degree in electrical and computer engineering from UQU, in 2002, the M.Sc. degree in electrical and computer engineering from KAU, in 2007, and the second M.Sc. degree in communication and signal processing and the Ph.D. degree in computer system design from Newcastle University, in 2009 and 2014, respectively. He was the Vice-Dean and the Dean of the Deanship of Scientific Research, UQU, from 2014 to 2020. He is currently an Assistant Professor with the Computer Engineering Department, the Vice-Dean of DFMEA, the General Director of the Decision Support Center, and the Consultant of the University Vice Chancellor with UQU. His research interests include VLSI design, EDA/CAD tools, coding and modulation schemes, image and vision computing, computer systems and architecture, and digital signal processing. Since 2015, he has been serving as a Review Committee Member of the IEEE International Symposium on Circuits and Systems (ISCAS) and a member of the Technical Committee of the IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS AND APPLICATIONS. He has served as a Reviewer in a number of journals, including the IEEE INTERNET OF THINGS, *IET Computer Vision*, *Artificial Intelligence Review*, and *IET Circuits, Devices, and Systems*.

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

WAJDI ALHAKAMI received the B.Sc. degree in computer science from Jeddah University, KSA, and the M.Sc. degree in computer network and the Ph.D. degree in network security from the University of Bedfordshire, U.K. He is currently working as an Assistant Professor with the Department of Computer Science, Taif University.

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

RAEES AHMAD KHAN (Member, IEEE) is currently working as a Professor and the Head of the Department of Information Technology, the Dean of the School for Information Science and Technology, Babasaheb Bhimrao Ambedkar University, (A Central University), Lucknow, India. He has more than 20 years of teaching and research experience. He has published more than300 research publications with good impact factors in reputed international journals and conferences, including the IEEE, Springer, Elsevier, Inderscience, Hindawi, and IGI Global. He has published a number of National and International Books (Authored and Edited) (including Chinese Language). His research interests are in the different areas of security engineering and computational techniques.