Securing healthcare information system through fuzzy based decision-making methodology

Abdullah Alharbi
Department of Information Technology, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia

Masood Ahmad
Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, India

Wael Alosaimi
Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia

Hashem Alyami
Department of Computer Science, College of Computers and Information Technology, Taif University, Taif, Saudi Arabia

Amal Krishna Sarkar
Department of Biostatistics and Health Informatics, Sanjay Gandhi Post Graduate Institute of Medical Sciences, Lucknow, India

Alka Agrawal
Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, India

Rajeev Kumar
Centre for Innovation and Technology, Administrative Staff College of India, Hyderabad, India

Raees Ahmmd Khan
Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, India

Corresponding author:
Rajeev Kumar, Centre for Innovation and Technology, Administrative Staff College of India, Bella Vista, Raj Bhavan Road, Khairatabad, Hyderabad-500082, Telangana, India.
Email: rs0414@gmail.com

Creative Commons Non Commercial CC BY-NC: This article is distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 License (https://creativecommons.org/licenses/by-nc/4.0/) which permits non-commercial use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (https://us.sagepub.com/en-us/nam/open-access-at-sage).
Abstract
The purpose of the healthcare Information System (HIS) is to replace the conventional method of data gathering and organization in hospitals into a modern method of systematic data collection, maintenance and dissemination. There has been an unprecedented rise in the malware and cyber-attacks on HIS recently. Cyber-attacks have become a major crisis for the healthcare industry. To address this scenario, the present paper conducts a study on the security factors integral to the healthcare information system and conducts the performance analysis of these factors. For this intent, the study has employed the Fuzzy Analytic Hierarchy Process (F.AHP) integrated with Technique Order Preference by Similarity to Ideal Solution (TOPSIS) integrated framework for evaluating the performance of each factor. Thereafter, the factors that play a vital role in healthcare data security breaches have been prioritized as per their security weights. Furthermore, the validity of the results obtained by the stated methodology has been established by conducting the sensitivity analysis and comparison of results with the other methods by using the same data set. Based on results thus obtained, the access control and software security have been identified as the most promising security factors.

Keywords
healthcare information system, fuzzy analytic hierarchy process-technique order preference by similarity to ideal solution, malware, cyber-attacks, security factors

Introduction
Nowadays, healthcare is generating a large amount of data, and this necessitates the use of robust information systems that can cater to both the hospitals’ as well as the patients’ needs efficiently and securely. Healthcare information system (HIS) is used for managing information, people and processes. Healthcare information system is like a system, which takes data as inputs, processes on the data, stores, and transmits the information. Adopting the HIS improves the efficiency and effectiveness of the hospital’s work. HIS replaces the paperwork of hospitals by digitalization; digitalization of the hospitals facilitates in the easy access of the patient’s history in the system. However, the increased dependency on digitalization has led to several security issues in the digital world.

Security is an essential part of analyzing the medical data. Healthcare information system shares the data of the patients over the system; thus, reducing overcrowding at the hospitals. It is easy for the patients to communicate with the doctors remotely. Moreover, the doctors can also connect frequently with patients and diagnose the patients’ ailments at an early stage. In the present era, the security of the Information system is a vital issue. The high costs of the medical data on the dark web and several vulnerabilities in the information systems make healthcare sector the most targeted industry of the cyber invasions. In the electronic health system, assurance of the data security, and availability of the information between the doctor and patient is both a sensitive and a critical concern.

Many researchers are already working on the MCDM approach with different aims in this league. Rajeev et al. (2020) applied fuzzy-based AHP-TOPSIS procedure for evaluating the impact of harmful factors of HIS. In this study, the authors prioritized the harmful factors which affect the data layers used in HIS. The authors focused basically on the data layers affected by harmful factors of HIS.
Zarour et al. (2021) have used the Fuzzy AHP approach for ensuring data integrity of healthcare information in digital health. The authors have prioritized the data integrity techniques that are used for maintaining the integrity of healthcare data. M.H. Behzadi (2015) did a comparative study on Fuzzy AHP and Fuzzy TOSIS approaches in math teachers’ selection and found that both the fuzzy based techniques obtained better results than the traditional approaches. In the case of inventory, Kabir and Hasin (2011) illustrated the benefits of capturing the fuzziness of human thought and assisting in the solution of the research issue through a systematic and straightforward approach. They identified the flexibility of manipulating criteria for a specific implementation, different classification analyses for different inventory records, application specific variable sets and crisp comparison values can be substituted for fuzzy comparison values for optimization if fuzzy comparisons aren’t available in case.

However, according to Mishra and Thakar (2012), the main advantage of Fuzzy AHP approaches is that they can be utilized for both qualitative and quantitative criteria, as well as convincingly resolve the conflicting assessments made by several decision-makers methodically. In addition, a fuzzy AHP can fix and assist spatial cognition issues in several of circumstances, including: hospital site selection (Chi and Kue, 2001), screening potential landfill sites (Champpratheep et al., 1997), teacher selection (M.H. Behzadi 2015).

Motivated by quality results obtained by using the fuzzy AHP and Fuzzy TOPSIS, the authors applied the fuzzy.AHP.TOPSIS approach for the scientific analysis of the security factors. This study commenced by reviewing the research articles that specify the possible factors that are affecting the security of the healthcare information system security. HIS also needs sustainable security features that can ensure confidentiality, integrity and Access control. However, identifying the factors in the healthcare infrastructure is a complex task; this is one of the key reasons for data breaches on the healthcare systems. To increase the security and quality of healthcare information system services, full understanding of the notion of the security and variables that influence healthcare information system security becomes as important research query.

Furthermore, the contributions of the study are as: Section 2nd presents the Literature Review related to security factors in the HIS. The 3rd section discusses the HIS and factors for securing the HIS. Section 4th contains the methodology and sensitivity analysis. Section 5 and 6 present the discussion and conclusion, respectively.

**Literature study**

Though we reviewed several studies for our reference, the present section specifically mentions the studies related to approaches for securing the HIS. Managing security of HIS is the most critical aspect because attackers frequently and easily prey on the medical data.

*Noor and Nur (2017)* discussed the barriers in technology by adopting the information system. This review article pointed out the technical difficulties like long system response time, system orientation and system interactions, inconvenience in practice, system does not support work flow that arises in the implementations. The solutions suggested for the same included: monitor the advance effects on patient’s safety, and make a secure intranet for information sharing.

*The study by J.G. Ronquillo et al. (2018)* discusses the adoption of IT in health, cybersecurity and breaches. This study provides effective solutions for reducing the cybersecurity at multilevel. In this context, the authors suggested the physical, technical safeguards. In the study, the authors cite that 85% of the data breaches were due to hacking. *Park et al. (2018)* discussed about the patient’s information disclosure. The study also defined the factors, which affect the patient’s information
factors, security awareness and medical assessment. This article evaluates the results, which affect the healthcare information system.\textsuperscript{20}

Md. Shirdeli et al. (2018) discusses the outsourcing of information security services in healthcare. The article examines healthcare information technology services from the perspective of experts and identifies the elements that motivate and influence healthcare organizations to outsource services. For assessing the numerous aspects, the paper employs an analytical hierarchy process technique.\textsuperscript{21}

A. Mcleod et al. explored the elements that influenced data breach and modeled them constructively in order to extract some useful information from them. The study included a fair review of the literature on numerous data breaches as well as a model of factors that affect data breaches directly or indirectly.\textsuperscript{22}

Rajeev et al., (2020) applied fuzzy-based AHP-TOPSIS procedure for evaluating the impact of harmful factors of HIS. In this study, the authors prioritized the harmful factors which affect the data layers used in HIS. The authors focused basically on the data layers affected by harmful factors of HIS.\textsuperscript{10}

S.R. Kessler et al. (2019) conducted a study on the healthcare information security, divided the professionals, and assessed the status of information security in healthcare.\textsuperscript{23} The proven results in the publication provide an effective roadmap for the researchers working in this domain.

G. Narayan et al. (2010) tried to find the possible threats in the healthcare information system, and identified that the key factors in this league were power failure, human error and technical factors, etc. In this study, the authors categorised the threats.\textsuperscript{24}

Although most of the authors have worked on the security of the information system, only a select few have done work on the healthcare information system security. Authors have opted CIA factors and sub factors which directly affects the HIS security. Multi-Criteria Decision Making (MCDM) technique is rarely used in the healthcare information system. However, we have observed that the accuracy of the MCMC technique is high, and hence, appropriate for reliable results. We have used the integrated technique of Fuzzy-AHP.TOPSIS for accurate assessment.

Figure 1. Healthcare information system architecture.
Materials and methods

Healthcare information system security

The use of Information System (IS)\(^25\) in healthcare is in the digitalization of healthcare. Healthcare industry is adopting IS to replace the manual processing. Since the patient’s information contains personal information, information security becomes a critical issue because the data is daily uploaded and retrieved online.\(^26\) HIS’s architecture is depicted in Figure 1. HIS can be divided into two parts: first, is the patients’ management system, and, the other is the managerial information system. PMS contains all the activities related to patients and MIS contains all the I managerial activities performed by the hospital staff. Collection of all information related to the patients is known as the Electronic Health Record (EHR).

Electronic Health Records (EHR) stores the personal details and the present and past history of the patient’s diseases and many more test results. EHRs records can be shared easily. Without the security framework, the patients’ information can be used in an illegal way and be sold on the black web. Healthcare data are highly lucrative and hence frequently targeted by the attackers. Thus, healthcare sector must develop its own cybersecurity plan and operations addressing these three key issues:

Prevent-In this key, first of all, the healthcare organization should know what information is stored and where, how it is managed and accessed, Confidentiality, Integrity, and Authenticity threats (CIA) in the assets.\(^27\) For the prevention, use defence techniques to make sure that the information is protected.

Detect-The detection phase points to the regular and irregular access of data, and monitors the methods of accessing the information. Hence, identifying the non-functional features like types of device being accessed, verifying the access method and allowing access to the user, and checking the patterns and changes in the behaviour of the user become crucial in this phase.

Respond-Healthcare organizations should have an efficient response mechanism to counter any security incident. Healthcare organisations should measure the working strategies of controls, response activities including communication over the healthcare system.

![Security factors hierarchy](image)

Figure 2. Security factors hierarchy.
Factors for securing HIS. A lot of factors have been identified for securing the HIS. However, for effective security management of HIS, the focus should be on the main important factor, that is the HI system that helps in protecting the vulnerabilities in healthcare information is several ways. Factors that may affect the security of the HIS are shown in Figure 2. We have addressed three main factors that affect the security and other sub-factors related to the main factors are shown in the figure.

Confidentiality. In the context of healthcare, confidentiality is the obligation of the professionals to save the patients’ information that is confidential. Sensitive information of patients’ needs special confidentiality, and must be preserved by the health information management professionals.

a. Malware and phishing. Malware and phishing attacks invade the systems with the malicious code that compromises the security. Most of the malware and phishing attempts are engineered through emails.

b. Man-in-middle attacks. Man-in-middle attacks are also known as the brute force attacks. In this attack, the attackers trespass the data when the communication happens between the doctors and patients or data is sent for processing over the network.

c. Encryption. If the information is encrypted, then the data cannot be trespassed when data is transmitted to the system or the authorised users.

d. Eavesdropping attacks. These attacks are also known as the sniffing or snooping attacks. In such attacks, the attackers steal the data when the information is transmitted over the network. Such attacks cannot be detected easily because no anomaly is observed in the network.

Integrity. Data should not be altered without proper verification of the users. Data integrity maintains the accuracy of the patient’s records, health summary, test results and other information of the patient’s over the lift-cycle of it. Healthcare information should be error-free and accurate and follow the latest security policies and procedure of the industry.

a. Secure wireless network. In the present context, almost all the healthcare organizations are providing free Wi-Fi to the patients and visitors. Since the network is always turned on and open to all, the HIS become even more vulnerable.

b. Paper record security. In the HIS, ignoring the security of paper records can result in easy access of data and its theft. Paper record security requires proper training of auditing staff; lack of training of staff is the main reason for the breaches and alteration of data.

Access control. Access control over the system is very important by the separate and frequently updated login information, identity verification and auto logs off after a period of time.

a. Software security. Software security also plays role in access control. Through the software vulnerabilities, attackers can enter the system and get control of the whole HIS. HIS software should be up to date with current patches. If the software is not updated timely, then the system runs with a high risk.
b. **Hardware security.** When hard disk of the system is changed, then the disk should be properly disposed of. If the hard disk is not properly disposed of, then the data can be easily recovered. The company should implement proper hardware protection devices - and these include the hardware protection such as HP, IBM, etc.

c. **Password changing reminder.** To protect the system from the unauthorized access, one should set a reminder for changing the password of the system. The alarm setting is done on the software, which creates a sound or sends a message to the authority to change the password after a time limit.

**Methodology**

This section deals with evaluating and prioritising the performance of various factors for Securing Healthcare Information System. Prioritizing the securing factors provides a systematic way to the security experts of the hospital management to design a secure healthcare information system.

![Figure 3. Working of Proposed framework for HIS security.](Image)
Authors’ contribution to this study is the quantitative analysis of factors’ performance in securing the healthcare information system with the help of MCDM. MCDM is used to calculate the results with validation and accuracy.

**Fuzzy AHP TOPSIS**

AHP is the most widely used MCDM technique for assessing the weights of factors. Fuzzy-AHP uses triangular fuzzy numbers instead of crisp values for calculating the weights of factors. The authors used here F.AHP.TOPSIS integrated technique for ranking the factors as discussed in Figure 2,\textsuperscript{10,11} The authors have designed a hierarchy by the help of experts and applied the F.-AHP.TOPSIS on it.

The fuzzy AHP.TOPSIS technique is particularly well suited to solving group decision-making problems in fuzzy environments.\textsuperscript{27} Fuzzy AHP.TOPSIS techniques were used to estimate the feasibility of the whole weight collection process. The sequential procedure of the fuzzy AHP.TOPSIS methodology depicts on Figure 3.

**Step 1**: Weight of each factor is calculated by converting the linguistic terms into TFNs. TFNs numbers lie between the value [0, 1]. In Table 1, the linguistics terms along with their respective crisp values have been shown; the values are between 0–9. Membership value is obtained by formulas.

$$\mu_a(x) = Tn \rightarrow [0, 1]$$

$$\mu_a(x) = \begin{cases} \frac{x}{m-h} - \frac{l}{m-h} & x \in [l, m] \\ \frac{x}{m-h} - \frac{1}{m-h} & x \in [m, h] \\ 0 & Otherwise \end{cases}$$

In Figure 4, $l$, $m$, $h$ represented lower middle and higher, respectively. The authors in Table 1 for allotting the scores of the factors have described. By using the Table 1, performance of the factors has been calculated in the numeric form.

With the help of equations (3)–(6), the linguistic terms are converted into precise Triangular Fuzzy Number (TFNs).

**Table 1.** TFNs value with their Linguistic terms.

| Saaty scale | TFNs value       |
|-------------|------------------|
| 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)    |
where \( l_{ij} \leq m_{ij} \leq h_{ij} \)

\[
\begin{align*}
\text{Step 2:} & \quad \text{Pair-wise decision matrix is designed after the receiving the expert's response. The matrix is calculated by equation (10).} \\
\tilde{A}^d = \begin{bmatrix}
\tilde{k}_{11}^d & \tilde{k}_{12}^d & \ldots & \tilde{k}_{1n}^d \\
\tilde{k}_{21}^d & \tilde{k}_{22}^d & \ldots & \tilde{k}_{2n}^d \\
\vdots & \vdots & \ddots & \vdots \\
\tilde{k}_{n1}^d & \tilde{k}_{n2}^d & \ldots & \tilde{k}_{nn}^d
\end{bmatrix}
\end{align*}
\]

Where, \( \tilde{k}_{ij}^d \) represents the \( d \)th decision makers. If there is more than one expert, \( i \)th criteria is preferred over the \( j \)th criteria.

The average of the preferences of each expert is evaluated by

\[
\tilde{k}_{ij} = \sum_{d=1}^{d} \tilde{k}_{ij}^d
\]

Figure 4. Triangular fuzzy number.
Stage 3: In this stage, the authors updated the pair-wise comparison matrixes for all factors in Figure 3 based on the results obtained by as follows

\[
\tilde{A} = \begin{bmatrix} \tilde{k}_{11} & \ldots & \tilde{k}_{1n} & \ldots & \tilde{k}_{n1} & \ldots & \tilde{k}_{nn} \end{bmatrix}
\]

(12)

We obtained the geometrical mean and fuzzy weights of all factors that were achieved by as follows

\[
\tilde{p}_i = \left( \prod_{j=1}^{n} \tilde{k}_{ij} \right)^{\frac{1}{n}}, \quad i = 1, 2, 3 \ldots n
\]

(13)

Stage 4: The assessment of the fuzzy weight of all factors was done by

\[
\tilde{w}_i = \tilde{p}_i \otimes \left( \tilde{p}_1 \oplus \tilde{p}_2 \oplus \tilde{p}_3 \ldots \oplus \tilde{p}_n \right)^{-1}
\]

(14)

After that, average weights were calculated and normalized weight of criteria was achieved by as follows

\[
M_i = \frac{\tilde{w}_1 \oplus \tilde{w}_2 \oplus \ldots \oplus \tilde{w}_n}{n}
\]

(15)

\[
N_{ri} = \frac{M_i}{M_1 \oplus M_2 \oplus \ldots \oplus M_n}
\]

(16)

Stage 5: In this stage, we have done the de-fuzzification of the values to obtain again the crisp values. The BNP (Best Non-fuzzy Performance) value of the fuzzy weights of every measurement was done by

\[
BNP_{wD1} = \frac{\left( uw_1 - lw_1 \right) + \left( miw_1 - lw_1 \right)}{3} + lw_1
\]

(17)

Step 6: TOPSIS is used here to calculate the performance ranking of each factor and alternative. This is evaluated by as follows

\[
E_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}}
\]

(18)

Where, \(i = 1, 2, \ldots m; \) and \(j = 1, 2, \ldots n.\)

Step 7: In this step, the Normalized Weighted Decision Matrix is calculated.

\[
s_{ij} = w_i E_{ij}
\]

(19)

Where, \(i = 1, 2, \ldots m \) and \(j = 1, 2, \ldots n.\)

Step 8: Positive and negative ideal solution is evaluated in this step

\[
I^+ = s_1^+ , s_2^+ , s_3^+ \ldots s_n^+
\]

\[
I^- = s_1^- , s_2^- , s_3^- \ldots s_n^-
\]

(20)
**Step 9:** In this step, the distance from positive \( (d_i^+) \) and distance from \( (d_i^-) \) negative ideal solution is calculated.

Distance from \( d_i^+ \)

\[
    d_i^+ = \sqrt{\sum_{j=1}^{m} (s_i^+ - s_{ij})^2}; \quad i = 1, 2, 3, \ldots m
\]

Distance from \( d_i^- \)

\[
    d_i^- = \sqrt{\sum_{j=1}^{m} (s_i - s_{ij})^2}; \quad i = 1, 2, 3, \ldots m
\]

**Step 10:** With the help of equation (23) calculating the preference value and satisfaction degree of all-alternative.

\[
    C \tilde{C}_i = \frac{k_i^-}{k_i^+ + k_i^-} = 1 - \frac{k_i^+}{k_i^+ + k_i^-}, \quad i = 1, 2, \ldots, m
\]

Where, \( i = 1, 2, 3 \ldots m \)

By the help of the above steps, the authors evaluated the performance of factors for securing the HIS by using F.AHP.TOPSIS approach. We have evaluated the performance of the factors for securing the HIS in the next section.

**Results and outcome**

Performance evaluation of various factors for securing healthcare information system (HIS) quantitatively is very hard for the experts. For any calculation factors, identification is a vital task. If the factors are identified properly, then the calculation for the statement will be effective for any system. We used the F.AHP.TOPSIS integrated technique for ranking the selected factors and evaluated the performance of the factors for securing the HIS. F.AHP.TOPSIS is the best MCDM technique.

For the selection of the factors, we consulted different security experts from different fields like industries, academia and research. With the help of equations (1)–(20), we evaluated the performance of factors for securing the HIS. With the help of equations (1)–(9) and Table 1, we converted the linguistic terms into quantitative values. Pair-wise comparison matrix \(^{28–30}\) is designed with the TFN scale. The Authors used here the TFN membership functions in place of other membership function because of their computational simplicity. Working with TFNs is often convenient in applications, and they are effective in boosting representation and information processing in a fuzzy environment. In the same fashion, for level 1, the pair-wise comparison matrix is designed by using equation (10), a matrix is displayed in Table 2.

---

**Table 2.** Fuzzy-aggregated pair-wise comparison matrix at level 1.

|                 | Confidentiality (CO) | Integrity (In) | Access control (AC) |
|-----------------|----------------------|----------------|---------------------|
| Confidentiality | 1.000,1.000,1.000     | 0.2300, 0.2800, 0.3600 | 0.3000, 0.4400, 0.8000 |
| Integrity       | —                    | 1.000,1.000,1.000     | 0.6600, 1.1700, 1.6900 |
| Access control  | —                    | —                | 1.000,1.000,1.000     |

---
Similarly, Tables 3–11 shows the calculations. With the help of TFN values, the authors create the pair-wise comparison matrix for level 1 and level 2. By using the pair-wise comparison matrix makes the combined aggregated pair-wise comparison matrix, after that, summarising all matrixes of levels 1, 2 creates the summary results in Table 10.

### Table 3. Fuzzy aggregated pair-wise comparison matrix at level 2 for static analysis.

| Malware/Phishing (M/P)   | Man-in-middle attacks (MA) | Encryption (EN) | Eavesdropping (ED) |
|-------------------------|----------------------------|-----------------|--------------------|
| M/P                     | 1.000, 1.000, 1.000        | 0.6900, 0.8900, 1.1000 | 0.2300, 0.2800, 0.3600 | 0.7000, 0.9500, 1.3500 |
| MA                      | --                        | 1.000, 1.000, 1.000 | 0.4900, 0.6400, 1.0000 | 0.2700, 0.3500, 0.5200 |
| EN                      | --                        | --              | 1.000, 1.000, 1.000    | 1.0000, 1.3200, 1.5500  |
| ED                      | --                        | --              | --                  | 1.000, 1.000, 1.000   |

### Table 4. Fuzzy aggregated pair-wise comparison matrix at level 2 for dynamic analysis.

| Secure wireless network | Maintaining efficiency | Paper records security |
|-------------------------|------------------------|------------------------|
| NS                      | 1.000, 1.000, 1.000    | 0.6600, 1.1700, 1.6900 | 1.1500, 1.4400, 1.7000 |
| MS                      | --                     | 1.000, 1.000, 1.000    | 1.0000, 1.5200, 1.9300  |
| PS                      | --                     | --                      | 1.000, 1.000, 1.000   |

### Table 5. Fuzzy aggregated pair-wise comparison matrix at level 2 for reverse engineering.

| Control accessibility | Password changing reminder | Software security |
|-----------------------|-----------------------------|-------------------|
| CA                    | 1.000, 1.000, 1.000         | 1.1900, 1.5800, 2.1500 | 0.4900, 0.6400, 1.0000 |
| PR                    | --                          | 1.000, 1.000, 1.000 | 0.2200, 0.2900, 0.4200 |
| SS                    | --                          | --                  | 1.000, 1.000, 1.000 |

### Table 6. Combined pair-wise comparison matrix at level 1.

| CO        | IN       | AC        | Weights |
|-----------|----------|-----------|---------|
| CO        | 1.0000   | 1.1730    | 0.4940  | 0.2749 |
| IN        | 0.8525   | 1.0000    | 1.1720  | 0.3296 |
| AC        | 2.0243   | 0.8532    | 1.0000  | 0.3955 |
| CR = 0.0488 |         |           |         |    |

### Table 7. Aggregated pair-wise comparison matrix at level 2 for static analysis.

| M/P    | MA       | EN       | EA       | Weights |
|--------|----------|----------|----------|---------|
| M/P    | 1.0000   | 0.8920   | 1.1730   | 0.9940  | 0.2463 |
| MA     | 1.1211   | 1.0000   | 0.6910   | 0.3720  | 0.1820 |
| EN     | 0.8525   | 1.4472   | 1.0000   | 1.2980  | 0.2724 |
| EA     | 1.0061   | 2.6882   | 0.7704   | 1.0000  | 0.2993 |
| CR = 0.0349 |         |           |         |    |
Weights of all the factors at different level are calculated and displayed in the Tables 6–9. The weights show the performance of factors for securing the HIS. With the help of step 4 and equations (14)–(16), the study obtained the Table 10 displays the aggregated weights of factors for securing the HIS. Based on the obtained aggregated weight, the authors assigned the ranks of each security factor. The highest weight of the factors obtains the 1st ranks and rest all. In Table 10 various security sub-factors obtain the ranks based on the security level. In Table 10, Access control obtains the highest weight (0.3955) in level 1 and sub-factor of access control software security obtained (0.2.21) the highest weight, based on the obtained weight assigned the 1st rank to software security. Same integrity obtained 2nd highest weight (0.3296) for level 1 and sub-factor of integrity, network security also obtained the second highest weights (0.1267), so we assigned the 2nd rank, control accessibility based on weight (0.1250) obtained 3rd rank, maintain efficiency obtains 4th rank based on weight (0.1174), paper security obtain 5th rank based on obtained weight (0.0855), eaves-dropping obtain 6th rank based on weight (0.0823), encryption obtain 7th rank based on weight (0.0749), password changing remainder obtain8th rank based on weight (0.0685), Man in middle attacks and malware/phishing obtain 9th and 10th rank based on weight (0.0500) (0.0677), respectively. The authors have evaluated the performance of factors for securing the HIS with the help

| Level 1 methods | Local weights of level 1 | Level 2 methods | Local weights of level 2 | Overall weights | Overall ranks |
|-----------------|--------------------------|-----------------|--------------------------|----------------|--------------|
| CO              | 0.2749                   | M/P             | 0.2463                   | 0.0677         | 9            |
| MA              | 0.1820                   |                 | 0.0500                   | 10             |
| EN              | 0.2724                   |                 | 0.0749                   | 7              |
| EA              | 0.2993                   |                 | 0.0823                   | 6              |
| IN              | 0.3296                   | NS              | 0.3843                   | 0.1267         | 2            |
| ME              | 0.3562                   |                 | 0.1174                   | 4              |
| PS              | 0.2595                   |                 | 0.0855                   | 5              |
| AC              | 0.3955                   | CA              | 0.3159                   | 0.1250         | 3            |
| PR              | 0.1731                   |                 | 0.0685                   | 8              |
| SS              | 0.5110                   |                 | 0.2021                   | 1              |

Table 8. Aggregated pair-wise comparison matrix at level 2 for dynamic analysis.

|          | NS  | ME  | PS  | Weights |
|----------|-----|-----|-----|----------|
| NS       | 1.0000 |     |     | 0.3843   |
| ME       | 0.8533 | 1.1720 |     | 0.3562   |
| PS       | 0.7337 | 0.6707 | 1.0000 | 0.2595   |
| CR = 0.0025 |

Table 9. Aggregated pair-wise comparison matrix at level 2 for reverse engineering.

|          | CA  | PR  | SS  | Weights |
|----------|-----|-----|-----|----------|
| CA       | 1.0000 |     |     | 0.3159   |
| PR       | 0.6124 | 1.6330 |     | 0.1731   |
| SS       | 1.4472 | 3.3003 | 1.0000 | 0.5110   |
| CR = 0.0052 |

Table 10. Summary of the results.
Table 11. Subjective cognition matrix.

|     | WA1     | WA2     | WA3     | WA4     | WA5     | WA6     |
|-----|---------|---------|---------|---------|---------|---------|
| A11 | 1.0000  | 2.6400  | 4.4500  | 5.0000  | 6.7300  | 8.4500  |
| A12 | 0.7300  | 2.2700  | 4.2700  | 5.3600  | 7.3600  | 8.7300  |
| A13 | 0.8200  | 2.4500  | 4.4500  | 4.1800  | 6.6400  | 7.5500  |
| A14 | 1.0000  | 2.4500  | 4.4500  | 5.0000  | 7.0000  | 8.4500  |
| A21 | 0.7300  | 2.2700  | 4.2700  | 5.3600  | 7.3600  | 8.7300  |
| A22 | 1.6400  | 3.3600  | 5.3600  | 6.2700  | 8.2700  | 9.4500  |
| A23 | 0.8200  | 2.4500  | 4.4500  | 4.1800  | 6.6400  | 7.5500  |
| A31 | 1.0000  | 2.6400  | 4.4500  | 5.0000  | 7.0000  | 8.4500  |
| A32 | 0.7300  | 2.2700  | 4.2700  | 5.3600  | 7.3600  | 8.7300  |
| A33 | 1.6400  | 3.3600  | 5.3600  | 6.2700  | 8.2700  | 9.4500  |
of criteria. We opted for six-hospital information systems of the hospitals in Varanasi to evaluate the factors’ performance for securing the HIS. Here WA1 to WA6 are alternatives that represent the HIS of different hospitals. Table 11 is constructed again with the help of equations (4)–(9). By using the equation (15), we calculated the normalized weights of the matrix.

By using the equations (17)–(23), the authors evaluated the positive and negative ideal solutions, Gap degree and Satisfaction degree as shown in Table 12. Closeness coefficients of each alternative are examined and displayed in Table 12. In this table, the positive and negative ideal solution means how near to positive values and how far from the negative values. Here, the authors assigned the ranks to the hospital-based on the satisfaction degree of the closeness coefficients of alternatives. Highest satisfaction degree obtains 1st ranks, so hospital WA1 information system obtains 1st rank, WA2 obtains 2nd, WA5 obtains 3rd, WA3 obtains 4th WA6 obtains 5th and WA4 obtains 6th ranks. The authors represented here, WA1-WA6 for different hospitals HIS in Varanasi.

### Sensitivity analysis

For the checking the accuracy and validation of the results, sensitivity analysis is the most essential procedure. In the sensitivity analysis, we checked their results by changing the variable used in the analysis. We have used here 10 experiments for sensitivity analysis; we opted for 10 experiments because 10 factors were selected at the last level. In our observation, each factor’s sensitivity weight is different, other factors’ weights; closeness coefficients are same at experiment time. The calculated sensitivity results analyses are displayed in Figure 5.

As per the closeness coefficient in Table 12, Alternative 1 obtained the highest weight. Furthermore, as per the sensitivity analysis in Figure 5, we found that WA1 obtained the highest satisfaction degree in all the 10 experiments.

### Comparison with the classical AHP-TOPSIS and fuzzy weighted average method

Some authors have performed the comparative study with traditional and classical AHP, TOPSIS approach with Fuzzy AHP, TOPSIS approaches and find that Fuzzy base MCDM and TOPSIS approach obtains better results. The authors have cited some references in this section. Akin and Guzin (2007), state that the Fuzzy Analytical Hierarchy Process (FAHP) is a synthetic extension of the classical AHP method when the fuzziness of the decision-makers is considered. M.H. Behzadi (2015), has performed a comparison study of fuzzy AHP and fuzzy TOSIS approaches in math teacher’s selection. Rajeev et al., (2020), applied fuzzy-based AHP-TOPSIS procedure for evaluating the impact of harmful factors of HIS and comparing their results with other prioritized methods. The authors found that the fuzzy AHP-TOPSIS provides better results than the ones
obtained by using traditional techniques. Similarly, we have also compared our experiments’ results with the other methods discussed here.

We compared the results that were obtained by using the Fuzzy Weighted Average method with the Classical-AHP.TOPSIS method. To the results verification, the same data set was used by the authors in the traditional AHP TOPSIS and Fuzzy weighted average method. And evaluate the results of both methods and compare them with Fuzzy AHP.TOPSIS method. They compared the results of the methods depicted in Figure 6. From the comparison, we observed that F.-AHP.TOPSIS generated better results than the Fuzzy Weighted Average and Classical AHP.TOPSIS method.

The authors employed fuzzy AHP-TOPSIS commonly for selecting the most appropriate security factors. The authors discovered that all these methods are stochastic processes to deal with some uncertainty, but the major advantage of fuzzy AHP-TOPSIS is that it performs an optimization

\[ \text{Figure 5. Sensitivity analysis.} \]

\[ \text{Figure 6. Comparative analysis.} \]
with the Max-Min function to maximise the desired results and minimize potential threats, whereas traditional and classical AHP-TOPSIS and Fuzzy average weighted only determines a deterministic result.

**Conclusion**

In this article, we have discussed the various factors that are crucial for securing the HIS. We have found three main factors that significantly affect the security of HIS. These factors show that healthcare information system security is under risk. In Figure 2, the authors have constructed the hierarchy of the factors and sub-factors in different levels. These factors and sub-factors affect each other and depend on each other, as discussed in the result analysis. Given the rapid pace of digitalisation in the Healthcare sector, the HIS-staff information, patients’ information, report results, and many more essential and sensitive information will be stored and transmitted by the hospitals for processing in the near future. When healthcare sends or stores the data over the network, then the attackers trespass on the data and access or alter the sensitive information. The ranking order of performance of factors for securing the HIS obtained by our analysis is \( WA1 > WA2 > WA5 > WA3 > WA6 > WA4 \).

To achieve the intended goal, we identified and classified the various factors and sub-factors, which create the loopholes in the HIS. Thereafter, we applied the F.AHP.TOPSIS technique for assigning the ranking order. Then, we validated the accuracy of the proposed technique. Results of the F.AHP.TOPSIS technique will help the security experts to develop more secure HIS. The Findings of the proposed study can be summarized as:

- By using our study’s results, the security experts can design and find their ways to make more secure HIS.
- According to our analysis, Access control and software security are the most prioritized factors. Hence, the security experts and researchers need to focus more on these factors for future research.
- We have opted for three main factors which affect the security of HIS at every level. By using our methodology, the developers can evaluate the performance of factors for securing any HIS.

**Declaration of conflicting interests**

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

**Funding**

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: We deeply acknowledge Taif University for Supporting This research through Taif University Researchers Supporting Project number (TURSP-2020/231), Taif University, Taif, Saudi Arabia.

**ORCID iD**

Rajeev Kumar https://orcid.org/0000-0002-1813-1362
References

1. Wager KA, Lee FW and Glaser JP. Managing health care information system: a practical approach for health care executives. John Wiley & Sons, 2010.
2. Fatima A and Colomo-Palacios R. Security aspects in healthcare information systems: a systematic mapping. *Proced Comput Sci* 2018; 138: 12–19.
3. Tabibi J, Nasiripour A, Kazemzadeh R, et al. Effective factors on hospital system acceptance: a confirmatory study in Iranian hospitals. *Middle East J Sci Res* 2011; 9(1): 95–101.
4. Abdul Karim NS and Ahmad M. An overview of electronic health record (EHR) implementation framework and impact on health care organization in Malaysia: a case study. *IEEE Int Conf Manag Innov Technol* 2014: 287–298.
5. Peikari HR, Shah MH, Lo MC, et al. Patients’ perception of the information security management in health centers: the role of organizational and human factors. *BMC Med Inform Decis Mak* 2018; 18: 102.
6. Paul RJ, Ezz I and Kuljis J. Healthcare information systems: a patient-user perspective. *Health Syst* 2012; 1: 85–95.
7. Shoniregun CA, Dube K and Mtenzi F. Introduction to e-Healthcare information security. In: *Electronic healthcare information security advances in information security*, vol 53. Springer, 2010, pp. 1–27.
8. Kruse C, Smith B, Vanderlinden H, et al. Security techniques for the electronic health records. *Health Syst* 2017; 41: 127.
9. Slamanig D and Stingl C. The Degree of Privacy in Web-based Electronic Health Records. In: Proceedings of the World Congress on Medical Physics and Biomedical Engineering 2006, Beijing, 22. Springer Science and Business Media LLC, 2009, 974–977.
10. Rajeev K, Abhishek P, Abdullah B, et al. Fuzzy-based symmetrical multi-criteria decision-making procedure for evaluating the impact of harmful factors of healthcare information security. *Symmetry* 2020; 12(664): 1–23.
11. Zarour M, Alenezi M, Ansari MTJ, et al. Ensuring data integrity of healthcare information in the era of digital health. *Healthc Technol Lett* 2021; 8: 66–77.
12. Marjan M, Shahvarani A, Behzadi M, et al. Comparison of fuzzy AHP and fuzzy TOPSIS methods for math teachers selection. *Indian J Sci Technol* 2015; 8: 1–10.
13. Golam K and Ahsan Akhtar Hasin M. Comparative analysis of AHP and fuzzy AFP models for multicriteria inventory classification. *Int J Fuzzy Logic Syst (IJFLS)* 2011; 1(1): 372–382.
14. Mishra Y and Thakar G. Comparison of classical fuzzy analytic hierarchy process and extended fuzzy analytic hierarchy process for vendor selection in automobile supply chain. In: Present at the National Conference on Emerging Challenges for Sustainable Business, 2012.
15. Abdullah AM, Abdulaziz A, Alka A, et al. A fuzzy multi-objective covering-based security quantification model for mitigating risk of web based medical image processing system. *Int J Adv Comput Sci Appl* 2020; 11: 481–489.
16. Sénor IC, Fernández-Alemán JL and Toval A. Usable privacy and security in personal health records. *In Computer Vision*, 6949. Springer Science and Business Media LLC, 2011, pp. 36–43.
17. Ronquillo JG, Winterholler JE, Cwikla K, et al. Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information. *JAMIA Open* 2018; 1: 15–19.
18. Noor AM and NurFaizah AA. The technology factors as barriers for sustainable Health Information Systems (HIS) - a review. *4th Inf Sys Instr Conf 2017, Indonesia* 2017; 124: 370–378.
19. Jay GR, Winterholler JE, Cwikla K, et al. Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information. *JAMIA Open* 2018; 1(1): 15–19.
20. Park EH, Kim J, Wiles LL, et al. Factors affecting intention to disclose patients’ health information. *Comput Secur* 2019; 87: 101340.
21. Shirdeli M, Zare S, Kharazmi E, et al. Presenting a model to evaluate factors affecting outsourcing of health information technology services. *Acta Inform Med* 2018; 26: 190–194.

22. McLeod A and Dolezel D. Cyber-analytics: modeling factors associated with healthcare data breaches. *Decis Support Syst* 2018; 108: 57–68.

23. Kessler SR, Pindek S, Kleinman G, et al. Information security climate and the assessment of information security risk among healthcare employees. *Health Informatics J* 2020; 26: 461–473.

24. Samy GN, Ahmad R and Ismail Z. Security threats categories in healthcare information systems. *Health Informatics J* 2010; 16(3): 201–209.

25. Som JO and Hod A. Examining the effects of information systems usage and managerial commitment on supply chain performance: the mediating role of supply chain integration. SAGE Open, 2022, pp. 1–15.

26. Arvanitis TN, White S, Harrison S, et al. A method for machine learning generation of realistic synthetic datasets for validating healthcare applications. *Health Informatics J* 2022; 28(2): 146045822210770.

27. AbdullahMasood AA, Abdulaziz A, Alka A, et al. A hybrid fuzzy-based multi-criteria framework for security assessment of medical device software. *Int J Intell Eng Syst* 2020; 13(5): 51–62.

28. Moayeri M, Shahvarani A, Behzadi MH, et al. Comparison of fuzzy AHP and Fuzzy TOPSIS methods for math teachers selection. *Indian J Sci Technol* 2015; 8: 1–10.

29. Mikhailov L. Deriving priorities from fuzzy pairwise comparison judgements. *Fuzzy Sets Syst* 2003; 134: 365–385.

30. Alzahrani A, Ahmad M, Nadeem M, et al. Integrity assessment of medical devices for improving hospital services. *Cmc-Compu Mater Continua* 2021; 67: 3619–3633.

31. Ahmad M, Al-Amri JF, Subahi A, et al. Healthcare device security assessment through computational methodology. *Comput Syst Sci Eng* 2022; 41: 811–828.

32. Aşkı O and Güzin O. Comparison of the AHP and fuzzy AHP for the multicriteria decision making processes with linguistic evaluations. *Istanbul Commerce Univ J Sci Year* 2007; 6(111): 65–85.