EAI Endorsed Transactions
on Context-aware Systems and Applications
Research Article EAI.EU

Analyzing Healthcare Device Security through Fuzzy Rule-based Multi-criteria Model

Neetu Yadav[1], Shafeeq Ahmad[1], and Naseem Ahmad Khan[1,*]

[1]Department of Computer Science & Engineering, Azad Institute of Engineering & Technology, Lucknow, Uttar Pradesh, India

Abstract

Managing risk as well as safeguarding electronic health records can be difficult for small medical practises. As a result of their vulnerability to various attacks, Internet of Health Things (IoHT)-based devices require appropriate security. In this paper, fuzzy TOPSIS is used to assess the security characteristics of IoHT-based devices in a medical setting. This technique utilizes a security evaluation of alternative solutions depending on security factors. The results of the presented security evaluation approach demonstrate that the most trustworthy as well as safe alternative among several of the alternative solutions is chosen for the IoHT model. This strategy could be used as a model for future IoHT structures or even other IoT-based domains. To the authors' knowledge, it is an unique strategy to IoT security evaluation, as well as such MCDM method have not been utilised before for evaluation as well as decision - making process in IoHT security systems.

Keywords: Healthcare informatics, IoHT, fuzzy logic, MCDM, security evaluation

Received on 02 May 2022, accepted on 13 May 2022, published on 16 May 2022

doi: 10.4108/eai.16-5-2022.173978

*Corresponding author. Email: naseemkhan033@gmail.com

1. Introduction

Healthcare has changed dramatically in recent years, as well as the development that has been made appears to be directly out of a science fiction story. For example, the Human Genome Project completed mapping genetic Information just over a decade back, as well as individual people may now undertake cost effective at-home genetic screening. Patient data were once managed to keep in thick file folders, but now numerous patients connect their health records as well as test findings through web platforms. Although the enormous amount and accessibility of data is beneficial to patients, it is even more beneficial to cybercriminals. The security risk to many personal information is evolving as the healthcare sector emerge with modern innovation as well as legislative action [1-5].

Personal information is relevant to every aspects of human life, however and those pertaining to the health and quality of life are of particular importance. Prior to the development of electronic health records (EHR), clinical information privacy was complicated too much. However, with the growth of the big data market as well as Artificial Intelligence (AI) innovations, it has become much more advanced as well as secretive than before. This makes ensuring the patients' privacy even more difficult [6, 7].

Information assurance, data security, as well as information systems are all concerned with preventing unauthorised access to private data. It is accomplished by guaranteeing integrity, availability and confidentiality of data. In public healthcare, where privacy, integrity, as well as availability are also important, it means ensuring that electronic medical information is not revealed to unauthorised people or operations. Furthermore, merely providing confidentiality in the modern period is insufficient to ensure personal rights. Similarly, we must protect the integrity of healthcare information which has not been tampered with or destructed illegally. The property of availability should include the property of making electronic medical information

attainable upon demand through an authorised person [8-10].

Protecting data in a world where information has become more commercially viable is both flattering as well as demanding, as it parallels the enormous milestone to safeguard the data from modern-day data infringement. Healthcare organisations encounter various security threats, ranging from ransomware to insecure IoT devices as well as, the ever-present human aspect. When combined with HIPAA as well as other compliance standards that make safeguarding protected health information (PHI) a main concern, healthcare organisations face a slew of serious security concerns which must be acknowledged in order to guarantee patient privacy as well as security [11-14].

According to a latest study by Grand View Research, Inc., the worldwide cyber security market is projected to attain USD 205.51 billion by 2024. The reliance of businesses on information technology, as well as the sensitivity of electronically stored data, has elevated the stakes for cyber-attackers, with economic benefit becoming a primary motivation. Providers of security mechanisms are conducting research and innovation to create next-generation security products. Science Applications International Corporation (SAIC), for example, has introduced an innovative cybersecurity technology that assists the government in protecting critical data, mitigating risks, and establishing a thorough defence against cyber-attacks. Also there is a strong focus on intelligence-led protection as traditional security technology solutions such as online platform, document management, as well as network security fail to reach security problem monitoring.

As government entities choose the cloud interface for information sharing, the cybersecurity sector is poised to see a surge in market for cloud-based implementations [11-14].

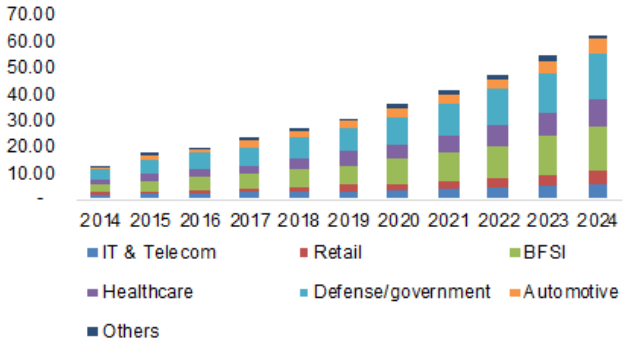

Figure 1. Cyber Security Market Size

2. Healthcare Information Security

Healthcare information system is composed of five elements: physical components, applications, a repository, a connection, as well as individuals. These five elements work together to provide input, processing, output, feedback, as well as regulate. Input/output gadgets, processors, operating systems, as well as media devices make up hardware. Multiple programs as well as processes make up an application. The data in a database is organised in the necessary configuration. Hubs, communications networks, as well as network devices make up a network. Gadget operators, network managers, as well as system specialists make up the workforce. Input, data analysis, storage systems, output, as well as control are all parts of processing information. Data specifications are supplied to the systems during the input terminal, as well as software programmes and other requests work on them during the processing stage. Healthcare information is provided in a structured manner as well as findings during the output stage.

The safety of information as well as information processes from unauthorised access, use, disclosing, interruption, amendment, or damage is referred to as information security. Security measures is implemented to ensure information's confidentiality, integrity, as well as availability. Confidentiality, integrity, and availability in healthcare system, as well as for the applications of this reference, imply the following:

• Confidentiality – the characteristics of not making electronic health information accessible or disclosing it to unauthorised people or procedures.

• Integrity – the fact that digital health information has not been tampered with or destructed in an unauthorised way.

• Availability – the ability of an authorised person to retrieve and utilise electronic health records on demand.

To evaluate the confidentiality, integrity, and availability of one’s electronic health records, individuals must first comprehend the organisation's health IT setting. This might include devices one‟s process uses for both medical and management applications, as well as where and how those medical devices are physically applied and positioned within ones practise. Consider the circumstances that could result in unauthorised access, utilise, disclosure, interruption, alteration, or breakdown of electronic health records as users assess their health IT landscape. These circumstances are significant to the practise and may take the form of technological issues for example, an absence of securely designed computer parts, procedural challenges for example, an absence of a surveillance emergency response strategy, or personnel challenges for example, absence of inclusive information security training [14, 15].

Due to the sheer behaviour of the information gathered by the healthcare industry, it may be more precious than credit card sensitive data. And besides, a patients personal history cannot be cancelled or changed, giving hackers a plethora of new avenues through which to intrude on their victims by phishing attacks, misuse, or extortion.

Because of the mixture of low protection and lucrative information, the healthcare industry is a great target. Whereas monetary profit is the primary motivation for intrusions, cybercriminals are far from the only risk. State-sponsored actors were also recognised to penetrate organisations in the hopes of gaining precious Intellectual Property (IP), especially in the medical sector.

The Internet of Things (IoT) – the connections of networking technologies in daily necessities – is slowly being implemented to medical applications, resulting in the Internet of Health Things (IoHT). Whereas the emergence of IoHT would then increase productivity in the already

overloaded healthcare sector, it would also invent different cybersecurity threats to patients as well as healthcare organisations.

Closely safeguarding sensitive data is not just a requirement; it is also a strategic imperative for healthcare organisations to make sure that sensitive data is accurately secured for the purpose of business operations. Healthcare organisations are accountable not only for their clients' health information as well as the ultimate security of their equipment, but they also have a responsibility to safeguard private information and assets in order to sustain a competitive benefit.

Inability to provide it jeopardises patients' security and anonymity, whereas failing to safeguard sensitive business information jeopardises the organisations' ability to operate effectively. As the widespread adoption of IoHT equipment in the healthcare industry keeps going, security implications must be prioritised to counterbalance the security flaws they initiate.

3. Related Works

Box and Pottas [16] conducted a literature review to learn more about the healthcare as well as information security contexts at work. They used study of behavior modification enforcers as Information Technology-use motivating factors to investigate the disparity among the specific intent to use Information Technology as well as actual conformance. According to their research, feelings are powerful motivators of behavior and attitudes.

Armstrong [17] presented a project that involved information security management and planning at a major private health centre. The Orion Tactic, a high level prototype obtained using the Soft Systems Methodology, was incorporated as well as further established throughout its implementation using Action Research. The technique involved a higher level of customer involvement, such as education workshops and seminars with healthcare senior as well as middle management. Their research study resulted in a marked enhancement in the hospital's security standards, increased understanding of security concerns, as well as staff acknowledgement of responsibility of the resulting security plan.

Alharam and El-Madany [18] presented a relative research on the various applications of computer security as well as the modifications in risk stages for different sectors. Their research focused on the usages of cyber-security in the healthcare sector, as well as the various techniques utilised it to safeguard the Internet of Things (IoT)-based medical industry. Their research also investigated various kinds of security risks in the healthcare sector.

Dong et al. [19] presented a research model that identifies organisational climate of information security (OCIS) as well as social bond concept in order to improve ISPC among nursing staff. A questionnaire was used, and responses were collected from 241 nurses working in 30 Malaysian health care facilities. The research's results demonstrated that OCIS aspects improve ISPC between many nurses. When the moderating impact of the social connection was considered, the impact on ISPC became even more substantial. It assumes that impactful OCIS variables strengthen social ties between nurses, thereby increasing the ISPC. The research findings emphasized the pervasiveness of socio-active information governance in healthcare organisations to improve ISP adherence among nursing staff for information security professionals.

Appari and Johnson [20] conducted a systematic review of the literature on data privacy and security in health care services, which was authored in information management publications as well as numerous other associated areas such as medical informatics, health services, regulation, medical science, trade press, as well as organisational records. They also presented a comprehensive overview of recent research and propose new areas of interest to the information systems community.

Nemati and Church [21] introduced a strategic plan for health care organisations looking to enhance their information security processes in order to conform with HIPAA as well as other regulatory requirements. Their focus was indeed on securing an organisation from insider threats through proper employee education and the development of an organisational culture in which processes have been appreciated. They claimed that their framework required the collection of empirical evidence through thorough business analysis with healthcare professionals in order to demonstrate the real significance of its implementation.

Gritzalis [22] presented operating and evolving healthcare information security guidelines, which were also identified as well as critically examined. As a consequence, the main outcomes of their works were the recognition of disparities as well as contradictions in existing standardisation, the characterization of standards' disagreement with regulations, as well as the analysis of the consequences of such guidelines for user organisations.

Hassan et al. [23] carried out an evaluation of the proposed conceptual framework, which was also based on Systematic Literature Review (SLR), strategic leadership qualities, as well as the Health Belief Model (HBM). Nineteen healthcare professionals were interviewed in a semi-structured survey. The criteria that may impact information security tradition in the health informatics setting were discovered to be divided into twelve themes. The findings of their study could help in designing a suitable Information Security Management System (ISMS) for constructing an information security policy in medical institutions.

Velibor [24] addressed such issues and offered potential solutions. There were also various researches on the subject, but these focus on only one aspect of information security management. Throughout investigation, researcher used case studies, observations, and model construction. The outcomes were also discussed. The findings would be useful to anyone concerned about information security in organisations. The importance of this research work is that it demonstrated the requirement for a cross - disciplinary strategy to information security management.

Janczewski and Shi [25] started with a review of New Zealand's medical information systems facilities as well as related security challenges related to privacy and confidentiality, accompanied by a thorough outline of the security benchmark strategy. Researchers examined each provision of AS/NZS 4444 in light of the information gathered about technological as well as non-technical strategies to medical information systems protection, which included a series of multi-case research of healthcare organisations that gather, process, store, as well as transfer electronic health records. Ultimately, based on previous study, researchers introduced a new list of information security benchmarks for building an information security prototype for healthcare organisations.

He et al. [26] expanded on the work by assessing the G.S.T. in healthcare. A research study with health care providers from a Chinese healthcare organisation demonstrates that the G.S.T. may also improve the present method for interacting lessons with the ISMS.

Shahid et al. [35] discussed the numerous elements of IoHT as well as classified different health gadgets according to their capabilities as well as implementation. They also discussed the various points and causes of data leakage, including legal inconsistencies, the use of subpar devices, an unawareness, as well as the lack of devoted local law policing organisations. Their work highlighted the growing need for an appropriate legislative structure and examines IoHT device conformance issues with regard to healthcare information privacy and security regulations.

Al Momin [36] gave a brief introduction of security risks, possible solutions, as well as constraints on implantable medical devices (IMD) programs that make attempting to solve these problems harder. Afterward, the work looked into the security concerns as well as background of pacemaker security flaws in order to demonstrate theoretical concepts using a particular device.

4. Materials and Methods

4.1. Hierarchy for the Evaluation

Treatment modalities regarding medical devices are becoming increasingly important, hitting new markets around the world and providing technological advancements in disease prevention for a wide range of conditions. Moreover, such initiatives may carry both predictable and unexpected risks, that in some cases may result in instant life-threatening implications. Governing agencies assessing new product market authorization must balance the potential advantages of proposed possible treatments against their possible consequences. The gathering of risk data about devices persists past the point of compliance decision-making for business approval and into the post-approval time frame. Several techniques have been established to assess device effectiveness particularly in the post-approval configuration.

In the aftermath of security concerns encompassing implantable cardioverter-defibrillator gives rise, orthopaedic items, as well as breast augmentation, the advantages and limitations of pre-approval as well as post-approval monitoring systems for medical equipment have been heavily debated in various countries across the world in recent times. Surprisingly, these conflicts have impacted countries to different degrees as well as elicited a range of reactions due to differences in regulatory settings.

Table 1 shows the brief description about the different factors used in the healthcare device security evaluation process.

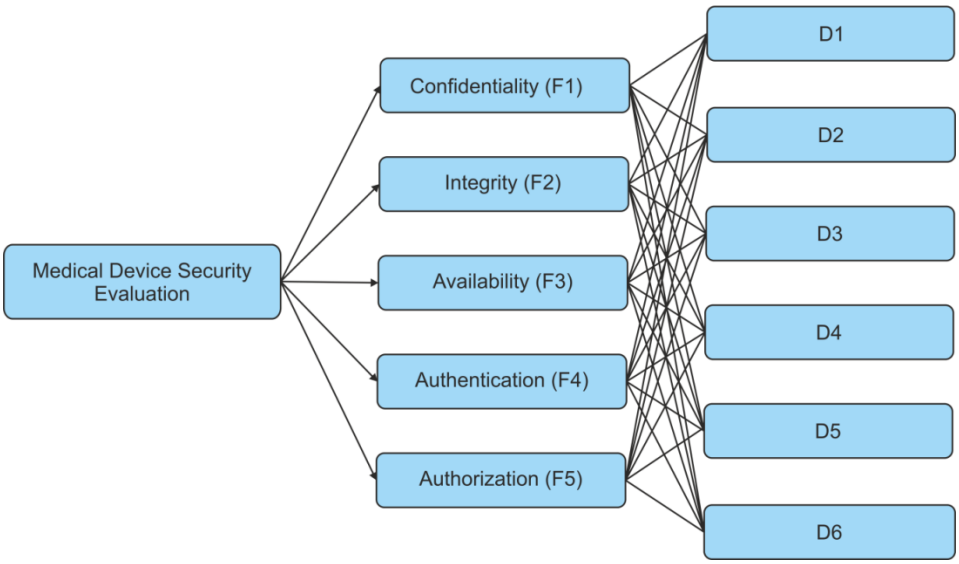

Figure 2. Hierarchy for the evaluation of healthcare device security

Table 1. Different factors used in the evaluation process

Factors	Description
Confidentiality (F1)	Confidentiality guarantees that sensitive data is only obtained by authorised individuals and is kept out of the hands of those who are not authorised to acquire it. It employs security features including login details; access control lists (ACLs), as well as encryption. It is also prevalent for data to be classified based on the potential for harm if it falls into the wrong hands. Security precautions can then be put in place as needed.
Integrity (F2)	Integrity guarantees that data is displayed in a layout that is true and accurate for its intended reasons. The recipient must have the data that the originator destined for him to possess. Only authorised individuals have access to the information, which persists in its original condition when not in use. Integrity is achieved through the use of security measures like data encryption as well as hashing. Modifications in data may also occur as a consequence of non-human-caused incidents.
Availability (F3)	The availability of information as well as resources guarantees that they are accessible to those who require them. It is carried out through the use of techniques like hardware repairs, software upgrades, as well as network management. When hardware failures occur, procedures such as redundant systems, failover, RAID, as well as high-availability groupings are utilised to mitigate severe consequences. To protect against downtime as well as unreachable data caused by malicious behaviour like distributed denial-of-service (DDoS) threats, specialised hardware components can be utilised.
Authentication (F4)	Authentication is the procedure of validating a user's or data's identity. When a user logs into a computing device, the procedure of validating that person's identity is known as user authentication.
Authorization (F5)	Authorization is a security method used to ascertain access stages or user/client advantages for system resources such as files, assistance, computer programmes, data, as well as application characteristics. This is the procedure of approving or rejecting access to a connectivity resource predicated on the user's identity, which also enables the user access to different resources.

4.2. Fuzzy TOPSIS Method

Multicriteria decision-making (MCDM) techniques could be used to deconstruct complicated problems into attainable component parts. Various dimensions that are essential for the decision-making situation can be assessed carefully one at a time with the support of MCDM. The viewpoints of numerous decision-makers potentially with distinct interests and expectations can be gathered and included in the judgement using group decision-making strategies. MCDM is a sub-discipline of business process research. Decision making usually entails inaccuracy and ambiguity, which fuzzy sets as well as fuzzy decision making methods can efficiently manage. A significant amount of study has been carried in recent times on the conceptual and implementation aspects of MCDM as well as fuzzy MCDM. In addition, decision making in overall, as well as fuzzy MCDM in specific, have been used in this paper.

The Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) proposed by Hwang and Yoon [27] is regarded as among the most well-known methods in the MCDM field. It is because of its consistency as well as easiness of use with fundamental data. Furthermore, TOPSIS is among the MCDM methods that specialists use to determine their final outcome because it is simple to understand and accurately measure [6]. The research of Chen and Hwang [28] and Negi [29] is used to develop a prototype fuzzy TOPSIS. Chen authored its overall augmentation for group decision problems in a fuzzy setting. Kahraman [30] and his research group suggested a new fuzzy TOPSIS technique in 2007 that can take into account the hierarchy of attributes as well as alternatives. This procedure outperforms traditional fuzzy TOPSIS strategies (Kahraman et al. [31]).

Zadeh proposed the Fuzzy Sets (FS) procedure in 1965. This FS is well-known for its ability to address issues of uncertainty as well as subjectivity. Afterward, in 2000, Chen [32] devised the Fuzzy TOPSIS (FTOPSIS) methodology based on the FS concept. This FTOPSIS technique can be used to replace the crisp output in grade

evaluation. Furthermore, it can find the most subjective nature alternative(s) from a collection of n possible options based on expert preference using subjectivity standards as well as weights.

Rouhani et al. [33] used fuzzy TOPSIS technique to deliver a straightforward approach to evaluating enterprise systems in terms of business intelligence. Such a method also assists the decision-maker in selecting an enterprise system with appropriate intellectual ability to assist managers' decision-making operations. 34 factors for business intelligence requirements are calculated using a broad literature search.

Tadić et al. [34] utilised fuzzy TOPSIS MCDM to assess suppliers of one specific medical device against a variety of criteria, considering the type of every criterion as well as its relative value.

This FTOPSIS method generally consists of seven main steps. General process of FTOPSIS is described as follows [14]:

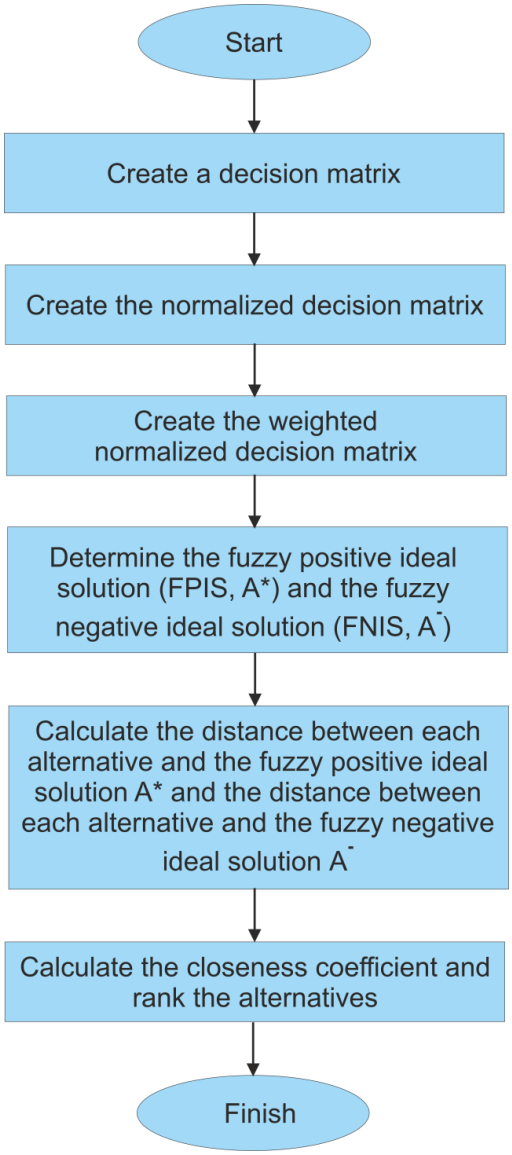

Figure 3. Flow chart of Fuzzy TOPSIS

Step 1: Construct a decision matrix

In this research article, 5 factors as well as 6 alternative solutions are consistently rated using the FUZZY model. Based on the hierarchical structure of the evaluation 45 security expert's decisions have been recorded for MCDM analysis. The Table 2 below summarizes the set of criteria type as well as weight designated to every criterion.

Table 2. Characteristics of Criteria

	name	type	weight
1	C1	+	(0.200,0.200,0.200)
2	C2	+	(0.200,0.200,0.200)
3	C3	+	(0.200,0.200,0.200)
4	C4	+	(0.200,0.200,0.200)
5	C5	+	(0.200,0.200,0.200)

The fuzzy measure used throughout the methodology is shown in the Table 3 below.

Table 3. Fuzzy Scale

Code	Linguistic terms	L	M	U
1	Very low	1	1	3
2	Low	1	3	5
3	Medium	3	5	7
4	High	5	7	9
5	Very high	7	9	9

The alternative solutions are assessed in aspects of different measures, and also the decision matrix consequences can be seen below. It should be noted that if more than one specialist participates in the assessment, the matrix below in Table 4 actually reflects the arithmetic average of all specialists.

Table 4. Decision Matrix

	C1	C2	C3	C4	C5
D1	(4.378, 6.378,8.378)	(4.156, 6.156,7.578)	(4.733, 6.733,7.978)	(3.844, 5.844,7.311)	(3.533, 5.489,7.178)
D2	(3.756, 5.711,7.400)	(4.022, 6.022,7.578)	(3.800, 5.800,7.267)	(3.933, 5.933,7.444)	(3.667, 5.667,7.356)
D3	(3.756, 5.711,7.622)	(4.333, 6.333,7.800)	(4.200, 6.111,7.578)	(4.333, 6.333,7.622)	(4.156, 6.111,7.622)
D4	(3.711, 5.622,7.356)	(4.022, 6.022,7.711)	(3.933, 5.933,7.622)	(4.067, 6.067,7.667)	(4.067, 6.067,7.844)
D5	(4.111, 6.111,7.711)	(3.889, 5.889,7.400)	(4.111, 6.111,7.756)	(3.711, 5.711,7.311)	(4.244, 6.244,8.022)
D6	(4.911, 6.867,8.289)	(4.822, 6.822,8.111)	(5.178, 7.178,8.200)	(5.133, 7.133,8.200)	(5.000, 7.000,8.156)

Step 2: Construct the normalized decision matrix

A normalised decision matrix can also be computed using the following resemblance refers to the positive as well as negative ideal solutions:

$\tilde{r}_{ij} = \left(\frac{a_{ij}}{c_j^*}, \frac{b_{ij}}{c_j^*}, \frac{c_{ij}}{c_j^*}\right)$; $c_j^* = \max_i c_{ij}$; Positive ideal solution

$\tilde{r}_{ij} = \left(\frac{a_j^-}{c_{ij}}, \frac{a_j^-}{b_{ij}}, \frac{a_j^-}{a_{ij}}\right)$; $a_j^- = \min_i a_{ij}$; Negative ideal solution

The following Table 5 depicts the normalised decision matrix.

Table 5. A normalized decision matrix

	C1	C2	C3	C4	C5
D1	(0.523, 0.761,1.000)	(0.512, 0.759,0.934)	(0.577, 0.821,0.973)	(0.469, 0.713,0.892)	(0.433, 0.673,0.880)
D2	(0.448, 0.682,0.883)	(0.496, 0.742,0.934)	(0.463, 0.707,0.886)	(0.480, 0.724,0.908)	(0.450, 0.695,0.902)
D3	(0.448, 0.682,0.910)	(0.534, 0.781,0.962)	(0.512, 0.745,0.924)	(0.528, 0.772,0.930)	(0.510, 0.749,0.935)
D4	(0.443, 0.671,0.878)	(0.496, 0.742,0.951)	(0.480, 0.724,0.930)	(0.496, 0.740,0.935)	(0.499, 0.744,0.962)
D5	(0.491, 0.729,0.920)	(0.479, 0.726,0.912)	(0.501, 0.745,0.946)	(0.453, 0.696,0.892)	(0.520, 0.766,0.984)
D6	(0.586, 0.820,0.989)	(0.595, 0.841,1.000)	(0.631, 0.875,1.000)	(0.626, 0.870,1.000)	(0.613, 0.858,1.000)

Step 3: Construct the weighted normalized decision matrix

The weighted normalised decision matrix can also be determined by calculating the weight of evey criterion in the normalised fuzzy decision matrix through the following equations, taking into account the various weights of every criterion.

$\tilde{v}_{ij} = \tilde{r}_{ij} \cdot \tilde{w}_{ij}$

Where $\tilde{w}_{ij}$ represents weight of criterion c_j

The weighted normalised decision matrix is shown in the Table 6 below.

Table 6. The weighted normalized decision matrix

	C1	C2	C3	C4	C5
D1	) 0.105,0.152,0.2 (00	) 0.102,0.152,0.1 (87	) 0.115,0.164,0.1 (95	) 0.094,0.143,0.1 (78	) 0.087,0.135,0.1 (76
D2	) 0.090,0.136,0.1 (77	) 0.099,0.148,0.1 (87	) 0.093,0.141,0.1 (77	) 0.096,0.145,0.1 (82	) 0.090,0.139,0.1 (80
D3	) 0.090,0.136,0.1 (82	) 0.107,0.156,0.1 (92	) 0.102,0.149,0.1 (85	) 0.106,0.154,0.1 (86	) 0.102,0.150,0.1 (87
D4	) 0.089,0.134,0.1 (76	) 0.099,0.148,0.1 (90	) 0.096,0.145,0.1 (86	) 0.099,0.148,0.1 (87	) 0.100,0.149,0.1 (92
D5	) 0.098,0.146,0.1 (84	) 0.096,0.145,0.1 (82	) 0.100,0.149,0.1 (89	) 0.091,0.139,0.1 (78	) 0.104,0.153,0.1 (97
D6	) 0.117,0.164,0.1 (98	) 0.119,0.168,0.2 (00	) 0.126,0.175,0.2 (00	) 0.125,0.174,0.2 (00	) 0.123,0.172,0.2 (00

Step 4: Calculate the fuzzy positive ideal solution (FPIS, A*) as well as the fuzzy negative ideal solution (FNIS, A^-)

The FPIS as well as FNIS of the alternatives solutions may be demarcated as follows:

$$A^* = \{\tilde{v}_1^*, \tilde{v}_2^*, \dots, \tilde{v}_n^*\} = \left\{\left(\max_j v_{ij} \,|\, i \in B\right), \left(\min_j v_{ij} \,|\, i \in C\right)\right\}$$

$$A^- = \{\tilde{v}_1^-, \tilde{v}_2^-, \dots, \tilde{v}_n^-\} = \left\{\left(\min_j v_{ij} \,|\, i \in B\right), \left(\max_j v_{ij} \,|\, i \in C\right)\right\}$$

Where $\tilde{v}_i^*$ is the highest amount of i for all the alternatives and also $\tilde{v}_1^-$ is the lowest amount of i for all the alternatives. B and C characterize the positive as well as negative ideal solutions, correspondingly.

The following Table 7 shows the positive as well as negative optimized solution.

Table 7. The positive and negative ideal solutions

	Positive ideal	Negative ideal
C1	(0.117,0.164,0.200)	(0.089,0.134,0.176)
C2	(0.119,0.168,0.200)	(0.096,0.145,0.182)
C3	(0.126,0.175,0.200)	(0.093,0.141,0.177)
C4	(0.125,0.174,0.200)	(0.091,0.139,0.178)
C5	(0.123,0.172,0.200)	(0.087,0.135,0.176)

Step 5: Compute the distance among every alternative and the fuzzy positive ideal solution $A^*$and the distance between each alternative and the fuzzy negative ideal solution A^-

The range among evey alternative as well as FPIS and among each alternative as well as FNIS is calculated using the following equation:

$S_i^* = \sum_{j=1}^n d(\tilde{v}_{ij}, \tilde{v}_j^*)$ i=1,2,…,m

$S_i^- = \sum_{j=1}^n d(\tilde{v}_{ij}, \tilde{v}_j^-)$ i=1,2,…,m

d is the distance among two fuzzy numbers , when given two triangular fuzzy numbers (a_1, b_1, c_1) and (a_2, b_2, c_2), e distance among the two can be designed as follows:

$$d_v(\tilde{M}_1, \tilde{M}_2) = \sqrt{\frac{1}{3}[(a_1 - a_2)^2 + (b_1 - b_2)^2 + (c_1 - c_2)^2]}$$

Note that $d(\tilde{v}_{ij}, \tilde{v}_j^*)$ and $d(\tilde{v}_{ij}, \tilde{v}_j^-)$ are crisp numbers.

The range from positive as well as negative ideal solutions is shown in the following Table 8.

Table 8. Distance from positive and negative ideal solutions

	Distance from positive ideal	Distance from negative ideal
alternative1	0.096	0.049
alternative2	0.13	0.014
alternative3	0.095	0.05
alternative4	0.113	0.034
alternative5	0.107	0.038
alternative6	0.001	0.143

Step 6: Compute the closeness coefficient as well as priority of different alternatives.

The closeness coefficient of every alternative could be calculated by using the following equation:

$$CC_i = \frac{S_i^-}{S_i^+ + S_i^-}$$

The preferred choice is closest to the FPIS as well as farthest away from the FNIS. The Table 9 below summarizes the closeness coefficient as well as priority order of every alternative.

Table 9. Closeness coefficient

	Ci	rank
D1	0.34	3
D2	0.098	6
D3	0.346	2
D4	0.233	5
D5	0.262	4
D6	0.991	1

The following Figure 4 shows the closeness coefficient of each alternative.

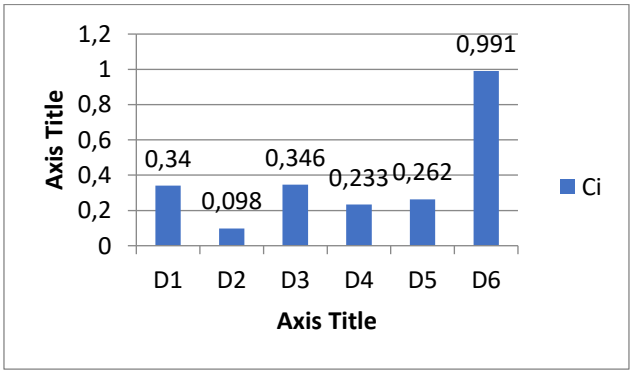

Figure 4 Graphical representation of closeness coefficient

It is observed that the effective evaluation of the best healthcare device security is based on the significance of Ci. With the help of presented method is D6>D3>D1>D5>D4>D2 (where ">" means "preferable to"). As a result, D6 is regarded as the preferred secure healthcare device.

5. Conclusion

Today's healthcare system is more electronically accessible than ever before, as well as the transition has yielded substantial advantages for both patients as well as suppliers. Physicians could indeed rapidly access as well as inform accurate records when patient data is stored electronically. The increased efficiency of care that this allows can protect lives, and organisations all over the world are practising everything they could to make sure that their technological tools develop at the same rate as the industry overall.

Moreover, as with any fast-paced digital transformation journey, there are major challenges and threats. Technological improvements, in particular, bring with them their own set of security concerns. Healthcare facilities as well as other facilities should make significant investments in secure hospital information management strategies, with very well trained team members in charge of implementing these procedures.

Advancement without security is a dangerous endeavour, as well as the reality that health care organisations acquire so much sensitive personal information tends to make this profoundly true in the healthcare domain. To work in secure hospital information planning, individuals must be planned to understand and enforce industry-specific information security recommendations affecting medical providers, as well as go above and beyond those minimum standards to establish cutting-edge information security strategies. While obtaining on health data protection is an apparent challenging task, it is also true that typically contains would be in increased trend for many years to come. By taking on these role and responsibility, individuals can become an integral element of a firm's managerial information processes group.

Medical devices are used by both patients and clinicians for health care monitoring of patients. After checking the data, healthcare gadgets send it to healthcare professionals, who then prescribe a treatment plan. Moreover, the information and platform's confidentiality is being considered. Even a minor discrepancy in the patient's information can result in an inaccurate diagnosis, putting the patient's condition at risk. The safety of medical devices can be evaluated quantitatively as well as automatically, which is an effective way to ensure their security. The D6 alternative is ranked first among the best options in this research study. This was accomplished in the present study using the fuzzy TOPSIS method. This method is most appropriate for decision-making as well as offers corroborating evidence findings among the various options. Healthcare device manufacturers can use a tried

strategy to security monitoring to safeguard healthcare devices using this conceptual model, which has been validated as well as evaluated.

Acknowledgements.
The authors gratefully acknowledge the support from Department of Computer Science & Engineering, Azad Institute of Engineering & Technology, Lucknow, Uttar Pradesh, India

References

[1] Tyali, S., & Pottas, D. (2011). Information security management systems in the healthcare context. In *Proceedings of the South African Information Security Multi-Conference: Port Elizabeth, South Africa, 17-18 May 2010* (p. 177). Lulu. com.

[2] Kwon, J., & Johnson, M. E. (2018). Meaningful healthcare security: Does meaningful-use attestation improve information security performance?. *MIS Quarterly*, *42*(4), 1043-1068.

[3] Söderström, E., Åhlfeldt, R. M., & Eriksson, N. (2009). Standards for information security and processes in healthcare. *Journal of Systems and Information Technology*.

[4] Box, D., & Pottas, D. (2014). A model for information security compliant behaviour in the healthcare context. *Procedia Technology*, *16*, 1462-1470.

[5] Ansari, M. T. J., Pandey, D., & Alenezi, M. (2018). STORE: security threat oriented requirements engineering methodology. *Journal of King Saud University-Computer and Information Sciences*.

[6] Mehraeen, E., Ayatollahi, H., & Ahmadi, M. (2016). Health information security in hospitals: the application of security safeguards. *Acta informatica medica*, *24*(1), 47.

[7] Ansari, M. T. J., Baz, A., Alhakami, H., Alhakami, W., Kumar, R., & Khan, R. A. (2021). P-STORE: Extension of STORE methodology to elicit privacy requirements. *Arabian Journal for Science and Engineering*, *46*(9), 8287-8310.

[8] Åhlfeldt, R. M., Spagnoletti, P., & Sindre, G. (2007, May). Improving the information security model by using TFI. In *IFIP International Information Security Conference* (pp. 73-84). Springer, Boston, MA.

[9] Ansari, M. T. J., & Pandey, D. (2018). Risks, security, and privacy for HIV/AIDS data: big data perspective. In *Big Data Analytics in HIV/AIDS Research* (pp. 117-139). IGI Global.

[10] He, Y., & Johnson, C. (2017). Challenges of information security incident learning: an industrial case study in a Chinese healthcare organization. *Informatics for Health and Social Care*, *42*(4), 393-408.

[11] Zarei, J., & Sadoughi, F. (2016). Information security risk management for computerized health information systems in hospitals: a case study of Iran. *Risk management and healthcare policy*, *9*, 75.

[12] Agbele, K. K., Oriogun, P. K., Seluwa, A. G., & Aruleba, K. D. (2015, November). Towards a model for enhancing ICT4 development and information security in healthcare system. In *2015 IEEE International Symposium on Technology and Society (ISTAS)* (pp. 1-6). IEEE.

[13] Ansari, M. T. J., Agrawal, A., & Khan, R. A. (2022). DURASec: Durable Security Blueprints for Web-Applications Empowering Digital India Initiative. *EAI Endorsed Transactions on Scalable Information Systems.*

[14] Ansari, M. T. J., Al-Zahrani, F. A., Pandey, D., & Agrawal, A. (2020). A fuzzy TOPSIS based analysis toward selection of effective security requirements engineering approach for trustworthy healthcare software development. *BMC Medical Informatics and Decision Making*, *20*(1), 1-13.

[15] Ansari, T. J., & Pandey, D. (2017). An Integration of Threat Modeling with Attack Pattern and Misuse Case for Effective Security Requirement Elicitation. *International Journal of Advanced Research in Computer Science*, *8*(3).

[16] Box, D., & Pottas, D. (2013). Improving information security behaviour in the healthcare context. *Procedia Technology*, *9*, 1093-1103.

[17] Armstrong, H. (2000, August). Managing Information Security in Healthcare—an Action Research Experience. In *IFIP International Information Security Conference* (pp. 19-28). Springer, Boston, MA.

[18] Alharam, A. K., & El-Madany, W. (2017, May). The effects of cyber-security on healthcare industry. In *2017 9th IEEE-GCC Conference and Exhibition (GCCCE)* (pp. 1-9). IEEE.

[19] Dong, K., Ali, R. F., Dominic, P. D. D., & Ali, S. E. A. (2021). The effect of organizational information security climate on information security policy compliance: The mediating effect of social bonding towards healthcare nurses. *Sustainability*, *13*(5), 2800.

[20] Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International journal of Internet and enterprise management*, *6*(4), 279-314.

[21] Nemati, H. R., & Church, M. (2009). A human centered framework for information security management: a healthcare perspective.

[22] Gritzalis, D. A. (1998). Enhancing security and improving interoperability in healthcare information systems. *Medical Informatics*, *23*(4), 309-323.

[23] Hassan, N. H., Maarop, N., Ismail, Z., & Abidin, W. Z. (2017, July). Information security culture in health informatics environment: A qualitative approach. In *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 1-6). IEEE.

[24] Velibor, B. O. Ž. I. Ć. (2020). Managing information security in healthcare. *ORAŞE INTELIGENTE ŞI DEZVOLTARE REGIONALĂ*, *4*(02), 63-83.

[25] Janczewski, L., & Shi, F. X. (2002). Development of information security baselines for healthcare information systems in New Zealand. *Computers & Security*, *21*(2), 172-192.

[26] He, Y., Johnson, C., Lu, Y., & Lin, Y. (2014, May). Improving the information security management: An industrial study in the privacy of electronic patient records. In *2014 IEEE 27th International Symposium on Computer-Based Medical Systems* (pp. 525-526). IEEE.

[27] Yoon, K. P., & Hwang, C. L. (1995). *Multiple attribute decision making: an introduction*. Sage publications.

[28] Chen, S. M., & Hwang, J. R. (2000). Temperature prediction using fuzzy time series. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, *30*(2), 263-275.

[29] Negi, D. S. (1989). *Fuzzy analysis and optimization* (Doctoral dissertation, Kansas State University).

[30] Kahraman, C., Gündogdu, F. K., Onar, S. Ç., & Öztaysi, B. (2019, September). Hospital Location Selection Using Spherical Fuzzy TOPSIS. In *EUSFLAT Conf.*.

[31] Kahraman, C., Cebeci, U., & Ulukan, Z. (2003). Multi-criteria supplier selection using fuzzy AHP. *Logistics information management*.
[32] Chen, C. T. (2000). Extensions of the TOPSIS for group decision-making under fuzzy environment. *Fuzzy sets and systems*, *114*(1), 1-9.
[33] Rouhani, S., Ghazanfari, M., & Jafari, M. (2012). Evaluation model of business intelligence for enterprise systems using fuzzy TOPSIS. *Expert Systems with Applications*, *39*(3), 3764-3771.
[34] Tadić, D., Stefanović, M., & Aleksić, A. (2014). The evaluation and ranking of medical device suppliers by using fuzzy topsis methodology. *Journal of Intelligent & Fuzzy Systems*, *27*(4), 2091-2101.
[35] Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data protection and privacy of the internet of healthcare things (IoHTs). *Applied Sciences*, *12*(4), 1927.
[36] Al Momin, M. A. (2022). Medical Device Security. In *Security, Data Analytics, and Energy-Aware Solutions in the IoT* (pp. 173-191). IGI Global.