EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

DURASec: Durable Security Blueprints for Web-Applications Empowering Digital India Initiative

Md Tarique Jamal Ansari[1,*], Alka Agrawal[1] and Raees Ahmad Khan[1]

[1]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow 226025, Uttar Pradesh, India

Abstract

Adversaries always eager to take advantage of flaws in emerging healthcare digital solutions. Very few authors discussed durable application security. Therefore there is a need for a durable security mechanism that must be adequately efficient, is reliable, and defend critical data in an emergency situation. It ensures that the application can be serviced and meet the needs of users over an extended period of time. This paper presents the fuzzy TOPSIS based method to evaluate the behavioural impact for durable security in the context of the Digital India initiative. This paper also presents novel DURASec blueprints for trustworthy and quality healthcare application development.. Even though the advantages of such technologies may outweigh the dangers, hospitals, drugstores, clinics, practitioners, the drug industry as well as medical device manufacturers, should be prepared to identify and minimize security threats in order to protect sensitive healthcare data.

Keywords: Durable Security, Web-Applications, Cyber-security, Security risk, fuzzy TOPSIS

Received on 12 December 2021, accepted on 09 January 2022, published on 13 January 2022

doi: 10.4108/eai.13-1-2022.172816

*Corresponding author. Email: tjtjansari@gmail.com

1. Introduction

Indian government inaugurated 'Digital India' on July 1 2015 with the goal of connecting all gram panchayats to the internet, promoting e-governance, and transforming India into an electronic knowledge-based economy. This is also applicable in the healthcare industry, where combining digital and traditional approaches can assist address concerns such as access, price, and quality. A digital healthcare system like this fits nicely with the vision of an all-digital nation backed by initiatives like Ayushman Bharat as well as Make in India [1-3].

Implementing digital solutions, together with protection, diagnosis, and treatment can enable India to get closer to its objective of national digital health. A digital health environment must include information technology and access to them in order to focus attention [4]. Different health firms are already making progress in this approach by using technology to provide patient-centric treatment in comfort and privacy. It is now feasible to not only observe a person's status at residence but also to cure them there. This promises well for the aging population, as they will be able to avoid hospital-acquired diseases. In extreme instances, such as the current epidemic, digital technology also allows for remote patient monitoring.

Telemedicine is a pioneering component of both digital health as well as India's National Health Policy (NHP). Although implementation is prevalent, it is imperative that this element be effectively nurtured. During COVID-19, telemedicine showed a lot of potential in terms of providing access to consultations from the comfort of one's own home. In this arena, adequate regulation is required, as well as putting it under policy consideration. This will provide access to expert medical consulting services across India, alleviating the problem of doctor shortages and easing the pressure on tertiary-care facilities in rural areas. Also there is a demand for additional attention in telemedicine, particularly from the private industry, but this may be addressed with clear regulation and law [4-9].

However, considering the rise in cyber-threats, the big endeavor has aroused significant concerns amongst security professionals. According to them, the digital transformation of all processes will expose security flaws. Experts feel that the success of 'Digital India' would be determined by the security platforms that supply the services, and they urge that the process include the development of centralized incident management abilities. The National Digital Health Mission (NDHM) has been extensively recognized as a game-changer for a previously under-documented country like India, with the goal of entirely redrawing the country's primary healthcare services landscape [10-12]. The Mission envisions the digitalization of the whole health ecosystem, including specialists, treatment centers, insurance corporations, pharmacies, laboratories, and diagnostic institutes, in addition to providing individual health identities to 130 crore individuals. As with any project of major significance involving cyber technology, it is likely to raise concerns about the security and privacy of clinical records. The primacy of data privacy and security must stay non-negotiable, considering the inherently confidential nature of the medical record.

Given the interrelated type and extent of the initiative, which involves such a diverse range of people and is supported by a variety of technology, it is inherently vulnerable to data breaches. Indeed, procedures have been written forth in the proposed Health Data Management Policy allowing health information suppliers and customers to access information under authorized permission administrators only after getting the data supervisor's informed consent, with "real collective ownership" staying with the data owners [13]. The fact that the authorization administrator would be an automated instrument adds to its vulnerability. Then there's the opportunity for sharing anonymized information for policy and research development, which is challenging because anonymized information can be reidentified when coupled with other data sets, raising serious concerns about data privacy. Likewise, the use of an individual health identifier to differentiate one data principle from another is incredibly dangerous.

Healthcare cybersecurity has emerged as one of the highest consequences to the economy. Due to the obvious specifications described in the Health Insurance Portability and Accountability Act (HIPAA) rules, as well as the ethical obligation to aid patients and the devastation that medical security breaches may do, IT experts must consistently address healthcare information security vulnerabilities. EHRs, or patient records, include a wealth of confidential material about individuals' medical history, making healthcare network security a top IT priority. Physicians as well as other healthcare workers, as well as insurance firms, can communicate vital information through EHRs. This allows organizing care as well as dealing with insurance issues [14]. The networked aspect of modern healthcare, on the other hand, poses IT security problems, as storing so much vital data in an area that practically everyone uses makes it a visible target for hackers and thieves. In fact, the significance of data protection in the healthcare industry has never been higher. Medical organizations must be diligent in developing precautions against internet threats now more than ever, which is why a thorough awareness of the hazards and protections offered is essential.

Organizations may have very few options except to embrace the risk associated with particular medical devices due to regulatory and risk concerns. Older devices that don't permit robust security control or don't offer a secure integration with the security architecture can be problematic. In such a case, it's critical to consider risk. Although there are circumstances when there isn't much that could be done to reduce the possibility, one can emphasize the consequence. The perfect situation for such kinds of incidents is to be able to notice any variation immediately and neutralize it as early as feasible. Wherever possible, IT personnel should endeavor to keep current software versions and upgrades, set up a solid backup and disaster recovery solution that is secure against network connectivity, and activate two-factor verification on network equipment and applications.

As per a new analysis from Grand View Research, Inc., the worldwide cyber security industry is predicted to hit USD 205.51 billion by 2024. The increased emphasis of businesses on information technology, as well as the critical nature of electronically stored data, has increased the stakes for cyber-attackers, with economic benefit becoming the main motivation.

In order to produce next-generation security mechanisms, software vendors are investing in research and development. Science Applications International Corporation (SAIC), for example, has created cutting-edge cybersecurity technology that aids the government in protecting sensitive data, mitigating risks, and establishing a comprehensive defence from cyber-attacks. Traditional security solutions, including web, document management, and network monitoring, are failing to achieve the surveillance of security occurrences, thus there is a growing importance on intelligence-led protection. As government organizations choose the cloud infrastructure for data exchange, the information security sector is predicted to see a surge in interest in cloud-based services [15]. The graphical illustration of this report can be seen in the following Fig. 1.

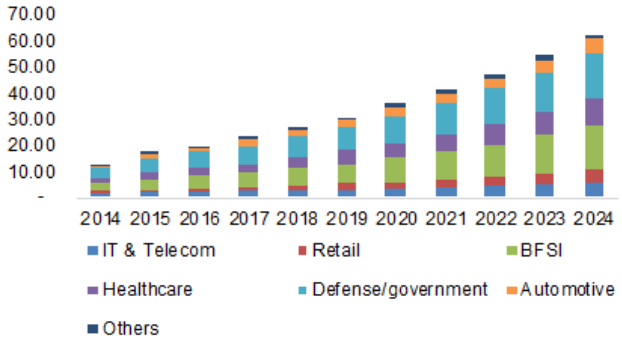

Figure 1. Global Cyber Security Market Size (Source: Grand View Research, Inc)

Due to the growing security threats in the digital world, employing secure software, services, and platforms has

become critical. With huge volumes of citizens' personal data stored on government IT systems, protecting people's privacy is crucial. It's crucial to have established software procurement procedures in place, with a particular focus on protective measures. This would not only assist to defend the government's IT architecture, and it would also contribute to building confidence among all participants, including citizens. The Multi-Criteria Decision Making approach is a useful method that may be used to make a variety of complex judgments. It works best when dealing with challenges that require a decision between several options. It possesses all of the qualities of a helpful decision-making aid: it assists us in focusing on what is essential, is reasonable and rational, and is simple to use. MCDM (Multi-criteria decision-making) is effective for breaking down a choice into simpler, better understandable components, examining each aspect, and putting the pieces together to create a powerful solution.

Unfortunately, when security safeguards are easier to enforce than they must be, the risk of data leakage and manipulation increases, which can impede productivity. As the name implies, the CIA Triad is not a top-secret, government architecture, but rather an ingeniously adaptable paradigm that can be used to safeguard any organization's business systems, operations, and infrastructure. In such situation there is an extreme need for a durable security blueprints. A blueprint is a comprehensive set of actions or planning process. When considering a web-application security blueprint, one should consider the entire architecture first, followed by the specific processes.

The rest of this study is organized as follows: In Section 2, the paper discusses the recent related works. Section 3 presents the Case Study in healthcare perspective and also demonstrates the need for a novel security mechanism. Section 4 discusses the overview of the DURASec Blueprints for web-applications. Finally, the paper concludes in Section 5.

2. Related Works

A web application is a programme that can be accessed using a web browser across a network for example the Internet or an intranet. Web-based applications are popular today due to the browser's widespread use as a client. One of the main reasons for their appeal is the capability to upgrade and manage mobile apps without deploying and software configuration on possibly thousands of client machines [16]. Web apps are used to develop a wide range of applications such as e-commerce, internet banking, email, enterprise applications, and many others. Web application security is the most ignored component of business security today, and it must be a top concern in any organization. Hackers are progressively focusing their attention on web-based applications such as checkout processes, forms, login pages, multimedia content, and so on. Insecure online apps, which are available 24x7 from anywhere in the world, enable simple access to backend company databases while also allowing hackers to undertake unlawful acts using the targeted sites.

To produce high-quality applications, developers must adhere to the highest standards of performance and security. The most straightforward way to accomplish application quality is to design security while working. Durability is employed as a security characteristic to solve these problems. This innovative method reveals security threats from a durability standpoint, where security design is created; hence not only high assessments but also a minimal supportability process for long-term security. This study assesses the existing obstacles that efforts to connect durability research to safeguarding face, and it recommends a path ahead in relation to security. Several research studies are available in this regard, involving durability; that is, the definition of durable security, and also the obstacles for modeling durability and security.

Kumar et al. [17] investigated the relationship between durability with software. Durability in software development is primarily determined by four attributes: trustworthiness, human trust, dependability, and software usability. To tackle the connection between these qualities, software developers examine the durability requirements that would need to be incorporated in order to meet these specific application serviceability criteria. The primary goal of their work was to provide a thorough awareness of the relation among application as well as durability attributes.

Agrawal et al. [18] assessed the security durability of 2 domestically built application systems, version 1 as well as version 2. The mixed fuzzy analytic hierarchy process (AHP) decision methodology was used by the authors to examine the security durability. The consequence of security durability on other characteristics had been quantified. Their research result includes an evaluation of security durability. They recommended based on their research finding that would help practitioners examine and enhance the security life cycle of software applications.

Mougouei [19] suggested recognizing partial fulfillment of security standards when acceptable rather than disregarding or deferring them in the foreseeable. They developed a goal-based model that enabled the prioritization and partial allocation of security criteria in relation to security goals. Their proposed methodology assists in reducing the amount of disregarded (postponed) security needs and, as a result, the negative consequences of neglecting security requirements in applications.

Ansari et al. [20] identified security concerns early stages of the software product lifecycle to assist requirement engineers in eliciting suitable security needs in a more structured manner across the requirement engineering procedures to aid secure and high-quality software development. Their proposed STORE technique for security requirements specification regarding security threats assessment is proposed in this study, which comprises the determination of four levels for successful security attack assessment.

Ali et al. [21] developed a patient healthcare system that outperforms existing blockchain-based network access in terms of security, reliability, as well as authenticity. Nasiri

et al. [22] highlighted the aspects and concepts related to IoT security needs in healthcare systems. A survey was done on the security requirements of IoT in the healthcare sector. From 2005 through September 2019, four popular digital databases were analyzed. Furthermore, they adhered to worldwide norms and approved guidelines covering cyber security needs.

Attaallah et al. [23] offered a strategy that would aid in the development of software that can combat risks without relying on external security tools. As a result, it is critical to assess the impact of security threats throughout software design. The researcher utilized the hybrid Fuzzy AHP-Methodology in their work to analyze the risks for increasing the security durability of various Institutional Web Applications. Furthermore, the e-component of security risk was assessed based on software durability. Their findings may be useful for improving the security and longevity of various web applications.

Although there has been lots of research work done by several authors to strengthen the quality of application in the context of durable security, yet there is a lack of an appropriate mechanism that is specifically designed for ensuring durable security. Therefore, this paper presents novel DURASec blueprints for trustworthy and quality application development. The proposed DURASec Blueprints ensure durable security capabilities early during the application development process.

3. Case Study in Healthcare Perspective

One of the most difficult challenges in behavioural impact analysis for durable healthcare security is determining the most efficient security threat. This is complicated by the presence of qualitative criteria as well as the ambiguity in analyzing them. Each security threat has technical, economic, environmental, and other benefits and drawbacks that create a set of limits. As a result, a comparison analysis is required in order to arrive at a scientifically sound and appropriately justified answer. MCDM is a complex decision-making technique that takes into account both statistical and subjective aspects [31]. Many MCDM methods and technologies have been proposed in recent years in order to select the most likely optimal solutions. The rankings of alternatives vs factors, as well as the significance weights of all factors, are evaluated in linguistic value determined by fuzzy figures in this work, which is an expansion to the fuzzy multiple criteria decision making (MCDM) model. In particular, in a fuzzy context, a modification of the TOPSIS approach is used. Many academics have created and applied the concept of similarity to an optimal situation in a fuzzy environment in a variety of domains. The method to achieve the objectives of this research is categorized in the following sub-sections.

3.1 Criteria and alternatives selection

Because the healthcare sector has too many variables to be put into a single unit, assessing the effectiveness of healthcare services is a difficult undertaking. Furthermore, there are no appropriate performance measurements for the healthcare sector because each provider, client, and payer determines healthcare efficiency according to their own goals, interests, and perceptions.

The main criteria were determined using extensive literature studies and experts' opinions. The institutes that were found to give special recommendations for the selection of different criteria for the security threat evaluation. The following Table 1 discuss the different types of healthcare information loss due to security threat.

Table 1. Different types of healthcare information loss due to security threat

Alternatives	Description
Collective loss (S1)	Collective loss refers to the combination of confidentiality, integrity and availability loss at the same time.
Confidentiality loss (S2)	When data or information supplied in secret to someone by an user is shared with any third party outside his knowledge and consent, it is considered a violation of confidentiality. Even if most breaches of confidence are accidental, individuals may suffer financial damages as a result.
Integrity loss (S3)	An unauthorised person has altered or deleted data or an Information system, resulting in a loss of integrity. It could be a record alteration or a change in the system's settings. When a file is attacked with malware, for instance, the file's integrity is compromised. Likewise, if a message inside an email is altered while in transmission, the integrity of the email is compromised.
Availability loss (S4)	The availability of data and systems guarantees that they are available when required. In other words, loss of availability means that data or a service is unavailable when a user requires it. For instance, if a Web server is unavailable when a visitor wishes to make a transaction, the Web server has experienced a loss of availability.

The following Figure 2 shows the hierarchical structure for the MCDM evaluation of different common security threats from a healthcare perspective in order to achieve durable security.

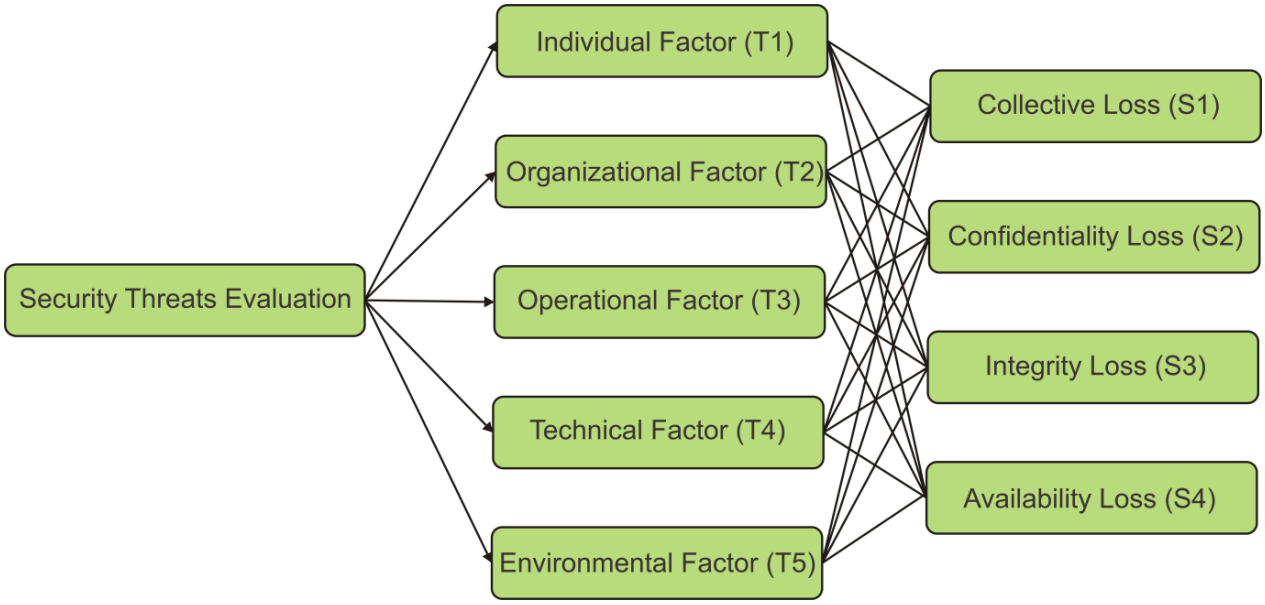

Figure 2. Hierarchical structure for the evaluation

3.2 Fuzzy TOPSIS Methodology

TOPSIS is centred on a resemblance or proximity index to the optimal solution, as well as the largest range from the negative-ideal solution. Chen and Hwang [32] develop TOPSIS. The TOPSIS technique evaluates the alternatives based on the weights assigned to each criterion, then normalizes the results and estimates the geometric distance between the ideal and negative-ideal solutions. The alternate solution that comes closest to the optimum solution is selected.

The goal of this research is to evaluate the different healthcare security threats based on a number of factors such as individual factors, organizational factors, operational factors, technical factors, and environmental factors denoted by T1, T2, T3, T4, and T5 respectively. Due to its sensitivity, ambiguity, inconsistency, and a large number of parameters, dry bulk carrier selection is a challenging decision-making problem that requires consideration. As a result, a model is developed that translates linguistic terms into trapezoidal fuzzy formulations for evaluating criteria as well as rating alternatives in order to determine precedence weights. The fuzzy TOPSIS method was chosen for four main reasons: the context and way of thinking are logical, comprehensible, and sensible; the computation is simple; the algorithm offers a possibility to follow the alternative solutions for each criterion in a simple numerical form, and the correlation algorithm offers with the ranking weights. The fuzzy TOPSIS algorithms have been employed in a number of investigations [33-37].

Figure 3 shows the systematic process of the fuzzy TOPSIS approach used in this research for the evaluation of different healthcare security threats.

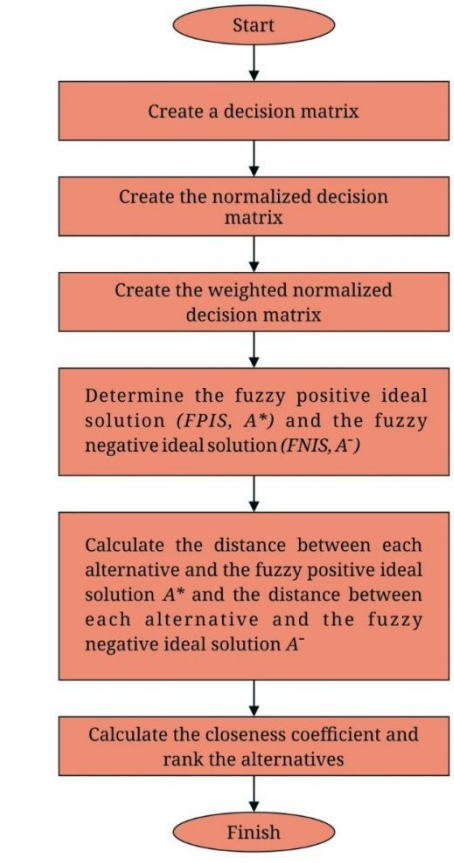

Figure 3. Fuzzy TOPSIS Methodology

The sample for this research came from the different educational institutions as well as state hospitals in Lucknow district of Uttar Pradesh, India. In order to evaluate healthcare researchers' and professionals' perceptions of individual factors, organizational factors, operational factors, technical factors, and environmental factors are added as evaluation factor indicators of health outcomes. A survey questionnaire is used to assess perceptions of service quality based on these three factors. To acquire approval to use the questionnaire in state hospitals, a procedure was also established. This preliminary study includes 60 participants who are randomly selected. Firstly, fuzzy TOPSIS is used to monitor the efficiency of healthcare security threats. Decision-makers in this research employed the linguistic variables "very low (VL)", "low (L)", "medium (M)", "high (H)" and "very high (VH)" to convey their judgments for tangibility, responsiveness, and empathy criteria, as well as to measure significance levels.

Step 1: Create a decision matrix

In this study, there are 5 criteria and 4 alternatives that are ranked based on the Fuzzy TOPSIS method. Table 2 below shows the type of criterion and weight assigned to each 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 following Table 3 shows the fuzzy scale used in the model.

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

Step 2: Create the normalized decision matrix

Based on the positive and negative ideal solutions, a normalized decision matrix can be calculated by the following relation:

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

Step 3: Create the weighted normalized decision matrix

Considering the different weights of each criterion, the weighted normalized decision matrix can be calculated by multiplying the weight of each criterion in the normalized fuzzy decision matrix, according to the following formula.

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

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

Step 4: Determine the fuzzy positive ideal solution (FPIS, A*) and the fuzzy negative ideal solution (FNIS, A⁻)

The FPIS and FNIS of the alternatives can be defined 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 max value of i for all the alternatives and $\tilde{v}_1^-$ is the min value of i for all the alternatives. B and C represent the positive and negative ideal solutions, respectively.

Step 5: Calculate the distance between each alternative and the fuzzy positive ideal solution A* and the distance between each alternative and the fuzzy negative ideal solution A⁻

The distance between each alternative and FPIS and the distance between each alternative and FNIS are respectively calculated as follows:

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

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

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

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

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

Step 6: Calculate the closeness coefficient and rank the alternatives

The closeness coefficient of each alternative can be calculated as follows:

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

3.3 Results

Collected data and results of statistical analysis should be outlined in this section.
The alternatives in terms of various criteria are evaluated and the results of the decision matrix are shown as follows. Note that if multiple experts participate in the evaluation, then the matrix below in Table 4 represents the arithmetic mean of all experts.

Table 4. Decision Matrix

	C1	C2	C3	C4	C5
A1	4.567,6.567,8.367	4.333,6.333,8.100	4.233,6.233,8.067	4.233,6.233,8.000	4.233,6.233,8.067
A2	4.500,6.500,8.267	4.600,6.600,8.333	(4.700,6.700,8.333)	(4.167,6.167,7.967)	(4.333,6.333,7.900)
A3	4.533,6.533,8.267	4.567,6.567,8.300	(4.100,6.100,8.000)	(4.333,6.333,8.167)	(4.333,6.333,8.100)
A4	4.300,6.300,8.033	4.767,6.767,8.367	4.433,6.433,8.167	4.400,6.400,8.233	4.067,6.067,7.933

The normalized decision matrix is shown in Table 5 below.

Table 5. A normalized decision matrix

	C1	C2	C3	C4	C5
A1	0.546,0.785,1.000	0.518,0.757,0.968	0.508,0.748,0.968	0.514,0.757,0.972	0.523,0.770,0.996
A2	0.538,0.777,0.988	0.550,0.789,0.996	0.564,0.804,1.000	0.506,0.749,0.968	0.535,0.782,0.975
A3	0.542,0.781,0.988	0.546,0.785,0.992	0.492,0.732,0.960	0.526,0.769,0.992	0.535,0.782,1.000
A4	0.514,0.753,0.960	0.570,0.809,1.000	0.532,0.772,0.980	0.534,0.777,1.000	0.502,0.749,0.979

The following Table 6 demonstrates the weighted normalized decision matrix

Table 6. The weighted normalized decision matrix

	C1	C2	C3	C4	C5
A1	0.109,0.157,0.200	0.104,0.151,0.194	0.102,0.150,0.194	0.103,0.151,0.194	0.105,0.154,0.199
A2	0.108,0.155,0.198	0.110,0.158,0.199	0.113,0.161,0.200	0.101,0.150,0.194	0.107,0.156,0.195
A3	0.108,0.156,0.198	0.109,0.157,0.198	0.098,0.146,0.192	0.105,0.154,0.198	0.107,0.156,0.200
A4	0.103,0.151,0.192	0.114,0.162,0.200	0.106,0.154,0.196	0.107,0.155,0.200	0.100,0.150,0.196

The positive and negative ideal solutions are shown in Table 7 below.

Table 7. The positive and negative ideal solutions

	Positive ideal	Negative ideal
C1	(0.109,0.157,0.200)	(0.103,0.151,0.192)
C2	(0.114,0.162,0.200)	(0.104,0.151,0.194)
C3	(0.113,0.161,0.200)	(0.098,0.146,0.192)
C4	(0.107,0.155,0.200)	(0.101,0.150,0.194)
C5	(0.107,0.156,0.200)	(0.100,0.150,0.195)

Table 8 below illustrates the distance from positive and negative ideal solutions

Table 8. Distance from positive and negative ideal solutions

	Distance from positive ideal	Distance from negative ideal
A1	0.026	0.015
A2	0.014	0.029
A3	0.02	0.021
A4	0.019	0.023

The top alternative is nearby to the FPIS and furthest to the FNIS. The closeness coefficient of every alternative and the ranking order of it are shown in Table 9 below.

Table 9. Closeness coefficient

	Ci	rank
A1	0.371	4
A2	0.676	1
A3	0.518	3
A4	0.549	2

The following graph shows the closeness coefficient of each alternative.

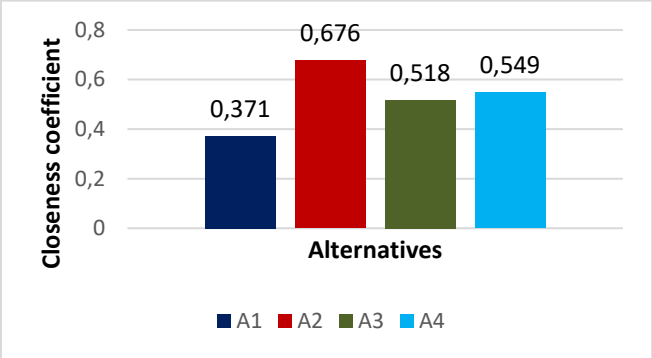

Figure 4. Closeness coefficient graph

From the findings presented in Fig. 4, it is clear that the alternative A2 which is the confidentiality loss is the most significant healthcare security threat followed by the availability loss, integrity loss, and collective loss. Further in next section, an effective and durable security technique is proposed in this study to give a stronger CIA mechanism to fight hacking attempts in security-critical web applications.

4. DURASec Blueprints for Web-Applications

Cybersecurity has evolved from a quality component to a top priority for organizations of all types. Malicious actors continue to breach organizations' data as well as systems on a daily basis, despite organizations' efforts to improve their defences. Creating a solid security strategy will aid organizations in strengthening company defences and achieving the company goals, as well as helping clients through an extremely sophisticated security and technology environment. To accomplish this, the blueprint must tackle the technologies that collaborate to produce an end-to-end service, as well as security vulnerabilities and client maturity levels. Secure Blueprint is a one-of-a-kind cyber management system that allows companies to integrate their cybersecurity program with their investments and business goals. Secure Blueprint assesses the maturity of a company's cyber programme by comparing its capabilities to modern cybersecurity management paradigms [24].

Building a sequence of technology components that constitute a cybersecurity foundation is critical. Risk analytics, strengthening and decreasing the attack vector, monitoring and response, mitigation solutions, and sophisticated defence against potential attacks such as malware and ransomware are all part of this strategy. Additionally, businesses can request that their security suppliers offer managed detection and mitigation services for continuous attack avoidance and threat tracking to proactively identify hidden intruders. One can combine as many of these technological layers as feasible with a single security solution. As a consequence, the company can assist their clients' unique requirements through a central point of responsibility.

The CIA triad, or confidentiality, integrity, and availability, is a concept intended to govern rules for cybersecurity within a company [25]. Even though the CIA triad parts are three of the most fundamental and critical cybersecurity demands, experts think the CIA triad requires an improvement to be efficient. In this sense, confidentiality refers to a set of policies that control access to information, whereas integrity refers to the guarantee that the data is trusted and correct, and availability refers to the promise that authorized people will have consistent access to the data. Figure 5 illustrates the main factors for achieving durable security in the application development process.

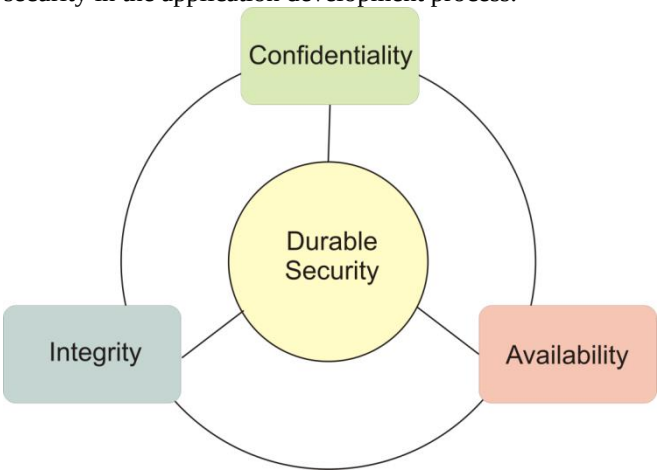

Figure 5. Durable security web for software applications

The significance of the CIA triad security architecture is self-evident, with each letter reflecting a core concept in cyberspace. Addressing these three concepts in the context of the "triad" might help promote the process of organizational security procedures. The triad assists organizations in asking targeted questions about how advantage is given in those three major areas when analyzing requirements and use scenarios for prospective new products and technologies.

The DURASec Blueprints for web applications contains following components:

- Identify Goals
- Security Management
- Security Metrics
- Durability Assurance
- Change Management

Figure 6 shows the architectural diagram of DURASec Blueprints for web applications.

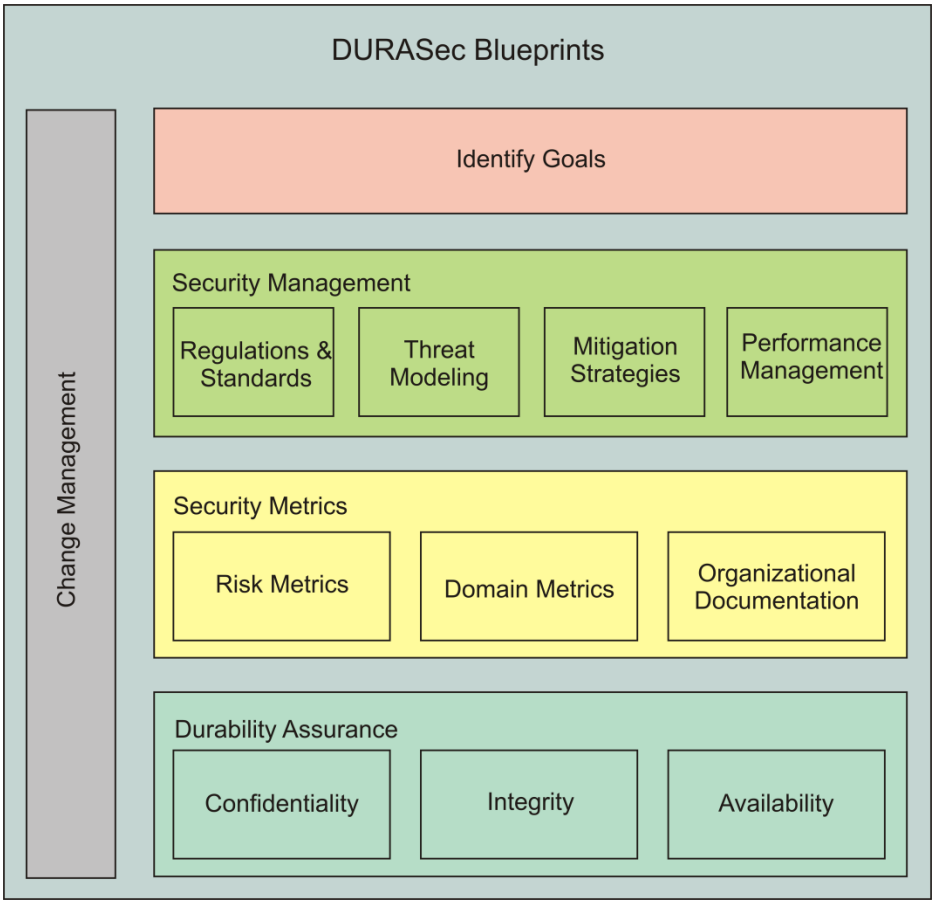

Figure 6. DURASec Blueprints Architecture for Web-Applications

4.1 Identify Goals

Goals provide a logical framework for discovering, organizing, and explaining software needs. Approaches are required for the initial selection and development of goals. Objectives are discussed from two perspectives: goal analysis and goal development. Goal-based strategy created and then outline our observations implementing it to a somewhat big case. Designers highlight some of the challenges that professionals experience when adopting a goal-based strategy to describe system requirements [26]. Any project must have at least one goal. Most have numerous goals. These are sometimes known as project objectives, or jointly as the project's aim. A vague goal will almost certainly produce hazy outcomes. Good software project management is primarily concerned with expectation management and anticipating risks. The project leader always seems to have one goal in mind: to complete the project. This is derived from the description of a system design: A one-of-a-kind, temporary initiative with set start and finish dates to accomplish one or more goals while adhering to cost, time, and performance evaluation restrictions. Sometimes, what appears to be an apparent project aim is not regarded in the same light by everyone. That's why it is critical to document and analyze it for the development team.

Determining the project goal, as well as scope, are directly influenced by the initial evaluation and conceptual model design and development methods, as well as the project planning abilities related to assessing and documenting while employing the people management skills and knowledge of management, negotiation, and compromise, and communication and collaboration. Identifying application development goals as well as dividing them down into more attainable subgoals is the first step in the goal-driven approach. It concludes with a plan for putting well-defined measurements and indicators is available to encourage the goals. It ensures accountability back to the goals throughout the journey so that individuals who gather and process observations do not lose track of the goals.

4.2 Security Management

The key to successful software security management has been highlighted primarily in order to create techniques that are practical, adaptable, and comprehensible. Any application's security is a crucial feature. Several applications are also outsourced when the development process lacks adequate application security integrations. The

increasing requirement to consider application security protocols across the development process should be explored. By integrating certain actions or processes during the development lifecycle, application security can be effortlessly integrated into the SDLC. These practices, which aim to safeguard the application produced, will be sought after by future consumers [27].

Currently, it appears that several companies have begun to address security earlier in the lifespan in order to decrease the risk possibilities of application security breaches. There is, therefore, still room for growth. The area of application security is continually evolving. Customers who outsourced programs must ensure that the application development methodology used by the IT services provider incorporates software security. On the other hand, technological network operators must instill trustworthiness in their SDLC application security requirements. The client loses if service providers failed to comprehend the importance of such non-functional elements.

4.3 Security Metrics

Security metrics are frequently used to analyze regardless of whether a firm's protection programme is accomplishing its objectives and remaining compliant. Such standards notify customers about what is and isn't working within the information security program, allowing businesses to adjust regulations, methods, or procedures to address any gaps in data security [28].

While the reduction in risk is an effective key performance indicator (KPI) for tackling the overall success of any security programme, there are other measures capable of providing insight into programme quality. The metrics developers pick to analyze should be measurable and have an impact on behaviour and direction. It should be directed toward continuous security activities so that one can keep track of the progress of the architecture throughout time. Metrics also enable organizations to share security programme insights with management teams in an analytical, simpler way. Hard metrics and standards help to eliminate ambiguity and quickly show areas that need improvement.

Metrics might provide statistics about the effectiveness of information security strategies, regulatory standards, and the ability of staff and departments to manage security breaches for which they are responsible. Metrics can also help to quantify the degrees of risk connected with failure to enforce specified mitigation measures and, as a consequence, provide guidance for prioritization of future resource allocations. Metrics may be used to improve security consciousness inside an enterprise because they provide factual info as well as a common vocabulary for communicating threats.

4.4 Durability Assurance

Durability Assurance (DA) is a systematic process for verifying whether or not an application meets specific standards and specifications. It also focuses on process improvement in order for the organization to give higher-quality services to its customers. In project specifications, assets, asset components, and design and building components are commonly needed to have prolonged design lifetimes. Assessment, design, and management for durability are crucial in decreasing the risks of long-term disintegration of systems, architectural pieces, and modules [29].

Designers understand the flow-through impacts of durability from project initiation to completion. This method evaluates the risk of decline, the cost of preventative measures, the effectiveness and cost of corrective measures, and the cost of continual planned maintenance. These must be managed in order to obtain the best total cost and return on investment. This quality management statement ties the Quality assurance (QA) process to a company's quality management process, ensuring that the requirements and goals for an application or product are fulfilled. To validate acceptance or rejection, the QA system performs operational assessments, compares to a standard, monitors processes, and applies regulatory mechanisms.

4.5 Change Management

Change management in application design refers to the process of migrating from one form of applications products to another upgraded version of the service. It records, regulates, and promotes artefact updates such as code changes, change orders, and documentation changes. CCP (Change Control Process) examines, documents, and approves changes to application software [30]. Every application development follows the Software Development Life Cycle (SDLC), for each stage accomplished to produce a high-quality software suite. Change Management is not one of the SDLC phases, but it is critical to the whole software project.

The essential to any healthcare system is CIA. However, in order to protect the platform's privacy as well as security, adequate security controls must be included. These security mechanisms have a significant impact on the platform's functionality. As a result, finding the correct combination of security restrictions and accessibility is critical to ensuring efficient security adoption [38-40]. Implementing up-to-date encryption, demanding adequate authentication, regularly fixing known vulnerabilities, and practising software quality assurance management are all crucial factors in safeguarding web apps against exploitation. The actuality is that even in a somewhat robust security setting, skilled attackers may be capable to discover flaws, and hence DURASec approach is needed for security-critical web-applications.

5. Conclusion

Digitalization has been the most effective approach to protect health professionals on the front lines, particularly in the event of extremely contagious diseases like COVID-19, while also boosting the performance of health care facilities. In the healthcare industry, however, cybersecurity must be

an afterthought. Medical experts frequently utilize old and obsolete applications with minimal security features, personnel lacks the requisite security knowledge to apply updates and patches quickly, and several healthcare systems lack security software entirely. Employee errors or unauthorized breaches are the most common causes of data breaches, which are caused by human error. Participants pointed out that hospitals frequently have no idea what systems are running on the equipment they utilize. Because of a widespread lack of understanding, as well as the normal lack of resources, most of these gadgets are black boxes in hospitals. Medical personnel may not even be aware that they are being attacked unless they are protected by a multi-layered cyber environment.

India is on the verge of undergoing a technological change. However, digital threats have become more sophisticated, the proposed DURASec Blueprints for applications intend to empower digital India Initiatives. It will be expected to enable the construction of a thriving digital healthcare setting. If the country needs to go digital to keep up with the rest of the globe, then a robust and credible cyber environment is also required.

Acknowledgements

The authors gratefully acknowledge the support from Council of Science & Technology, Uttar Pradesh (UPCST); Letter No. CST/D-2300

References

[1] Perwez, S. K., & Perwaiz, S. Z. (2016). Digital India: A Novel Perspective for Indian People and Economy. *International Journal of Marketing and Technology*, *6*(4), 77-100

[2] Abraham, I., & Rajadhyaksha, A. (2015). State power and technological citizenship in India: From the postcolonial to the digital age. *East Asian Science, Technology and Society: An International Journal*, *9*(1), 65-85

[3] Gurumurthy, A., Chami, N., & Thomas, S. (2016). Unpacking Digital India: A feminist commentary on policy agendas in the digital moment. *Journal of Information Policy*, *6*(1), 371-402

[4] 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.

[5] Balsari, S., Fortenko, A., Blaya, J. A., Gropper, A., Jayaram, M., Matthan, R., ... & Khanna, T. (2018). Reimagining Health Data Exchange: An application programming interface–enabled roadmap for India. *Journal of medical Internet research*, *20*(7), e10725.

[6] Hossain, M. M., Tasnim, S., Sharma, R., Sultana, A., Shaik, A. F., Faizah, F., ... & Bhattacharya, S. (2019). Digital interventions for people living with non-communicable diseases in India: A systematic review of intervention studies and recommendations for future research and development. *Digital health*, *5*, 2055207619896153.

[7] Mills, C., & Hilberg, E. (2020). The construction of mental health as a technological problem in India. *Critical Public Health*, *30*(1), 41-52.

[8] Zarour, M., Ansari, M. T. J., Alenezi, M., Sarkar, A. K., Faizan, M., Agrawal, A., ... & Khan, R. A. (2020). Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records. *IEEE Access*, *8*, 157959-157973.

[9] Alhakami, W., Binmahfoudh, A., Baz, A., Alhakami, H., Ansari, M. T. J., & Khan, R. A. (2021). Atrocious Impinging of COVID-19 Pandemic on Software Development Industries. *Computer Systems Science and Engineering*, 323-338.

[10] Rajeev, V. R., Pillai, N. M., Radhakrishnan, A., & Bhavani, R. R. (2018). EVALUATING DIGITAL INDIA THROUGH NATIONAL DIGITAL LITERACY MISSION IN KALLIYOOR PANCHAYATH. *International Journal of Pure and Applied Mathematics*, *119*(15), 1943-1954.

[11] Bajpai, N., & Wadhwa, M. (2020). India's National Digital Health Mission.

[12] Mishra, S. K., Kapoor, L., & Singh, I. P. (2009). Telemedicine in India: current scenario and the future. *Telemedicine and e-Health*, *15*(6), 568-575.

[13] 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*.

[14] Attaallah, A., Ahmad, M., Ansari, M. T. J., Pandey, A. K., Kumar, R., & Khan, R. A. (2020). Device security assessment of Internet of healthcare things. *Intelligent Automation & Soft Computing*, *27*(2), 593-603.

[15] *Cyber security market size to grow $205.51 billion by 2024: Grand View Research, Inc. - Technologies Market*. Google Sites. (n.d.). Retrieved September 27, 2021, from https://sites.google.com/site/technologiesmarketnews/cyber-security-market.

[16] 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).

[17] Kumar, R., Khan, S. A., & Khan, R. A. (2016). Durability challenges in software engineering. *Crosstalk-The Journal of Defense Software Engineering*, 29-31.

[18] Agrawal, A., Zarour, M., Alenezi, M., Kumar, R., & Khan, R. A. (2019). Security durability assessment through fuzzy analytic hierarchy process. *PeerJ Computer Science*, 5, e215.

[19] Mougouei, D. (2017). PAPS: a scalable framework for prioritization and partial selection of security requirements. arXiv preprint arXiv:1706.00166.

[20] 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*.

[21] Ali, A., Rahim, H. A., Pasha, M. F., Dowsley, R., Masud, M., Ali, J., & Baz, M. (2021). Security, Privacy, and Reliability in Digital Healthcare Systems Using Blockchain. *Electronics*, 10(16), 2034.

[22] Nasiri, S., Sadoughi, F., Tadayon, M. H., & Dehnad, A. (2019). Security requirements of internet of things-based healthcare system: a survey study. *Acta Informatica Medica*, 27(4), 253.

[23] Attaallah, A., Algarni, A., & Khan, R. A. (2021). Managing Security-Risks for Improving Security-Durability of Institutional Web-Applications: Design Perspective. *CMC-COMPUTERS MATERIALS & CONTINUA*, 66(2), 1849-1865.

[24] Kessler, G. C., & Ramsay, J. (2013). Paradigms for cybersecurity education in a homeland security program. *Journal of Homeland Security Education*, *2*, 35.

[25] Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3).
[26] Kifer, M., Lara, R., Polleres, A., Zhao, C., Keller, U., Lausen, H., & Fensel, D. (2004, November). A Logical Framework for Web Service Discovery. In *SWS@ ISWC*.
[27] Murch, R. (2001). Project management: Best practices for IT professionals. Prentice Hall Professional.
[28] Khan, R. A., Mustafa, K., & Ahson, S. I. (2007). An empirical validation of object oriented design quality metrics. *Journal of King Saud University-Computer and Information Sciences*, *19*, 1-16.
[29] Gjorv, O. E. (2013). Durability design and quality assurance of major concrete infrastructure. *Advances in concrete construction*, *1*(1), 45.
[30] Kettinger, W. J., Teng, J. T., & Guha, S. (1997). Business process change: a study of methodologies, techniques, and tools. *MIS quarterly*, 55-80.
[31] Alosaimi, W., Ansari, M. T. J., Alharbi, A., Alyami, H., Ali, S., Agrawal, A., & Khan, R. A. (2021). Toward a Unified Model Approach for Evaluating Different Electric Vehicles. Energies, 14(19), 6120.
[32] Papathanasiou, J., & Ploskas, N. (2018). Topsis. In *Multiple Criteria Decision Aid* (pp. 1-30). Springer, Cham.
[33] 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.
[34] Yong, D. (2006). Plant location selection based on fuzzy TOPSIS. *The International Journal of Advanced Manufacturing Technology*, *28*(7), 839-844.
[35] Chu, T. C., & Lin, Y. C. (2003). A fuzzy TOPSIS method for robot selection. *The International Journal of Advanced Manufacturing Technology*, *21*(4), 284-290.
[36] Bottani, E., & Rizzi, A. (2006). A fuzzy TOPSIS methodology to support outsourcing of logistics services. *Supply Chain Management: An International Journal*.
[37] Khambhati, R., Patel, H., & Kumar, S. (2021). A performance evaluation and comparison model for urban public healthcare service Quality (Urbpubhcservqual) By fuzzy TOPSIS Method. *Journal of Nonprofit & Public Sector Marketing*, 1-20.
[38] Vimalachandran, P., Liu, H., Lin, Y., Ji, K., Wang, H., & Zhang, Y. (2020). Improving accessibility of the Australian My Health Records while preserving privacy and security of the system. *Health Information Science and Systems*, *8*(1), 1-9.
[39] Wang, H., Wang, Y., Taleb, T., & Jiang, X. (2020). Special issue on security and privacy in network computing. *World Wide Web*, *23*(2), 951-957.
[40] Vimalachandran, P., Zhang, Y., Cao, J., Sun, L., & Yong, J. (2018, November). Preserving data privacy and security in Australian my health record system: A quality health care implication. In *International Conference on Web Information Systems Engineering* (pp. 111-120). Springer, Cham.