NSS
Neutrosophic Sets and Systems, Vol. 58, 2023
University of New Mexico

Neutrosophic Model for Evaluation Healthcare Security Criteria for Powerful and Lightweight Secure Storage System in Cloud-Based E-Healthcare Services

Ahmed A. El-Douh[1], SongFeng Lu[2], Ahmed Abdelhafeez[3], Ahmed M. Ali[4], Alber S. Aziz[5]

[1]School of Cyber Science and Engineering, Huazhong University of Science and Technology, Wuhan 430074, China; Ahmed.eldouh.csis@o6u.edu.eg

[2]School of Cyber Science and Engineering, Huazhong University of Science and Technology, Wuhan 430074, China; lusongfeng@hust.edu.cn

[3]Faculty of Information Systems and Computer Science, October 6th University, Giza, 12585, Egyptl aahafeez.scis@o6u.edu.eg

[4]Faculty of Computers and Informatics, Zagazig University, Zagazig 44519, Sharqiyah, Egypt; aabdelmonem@fci.zu.edu.eg

[5]Faculty of Information, Systems and Computer Science, October 6th University, Giza, 12585, Egypt; albershawky.csis@o6u.edu.eg

Abstract: Large data volumes make manually keeping and preserving health records for future reference problematic. Most unusual is the coronavirus epidemic's overcrowding of hospitals. The Secure Pattern Electronic Healthcare Records (SPEHR) scheme provides a powerful and lightweight secure storage system for cloud-based E-healthcare services that meets remote healthcare security criteria. So we proposed a neutrosophic model with a multi-criterion decision-making (MCDM) method for the analysis and evaluation of these criteria. The neutrosophic model is used to deal with vague and uncertain data. Then we integrated the neutrosophic model with the AHP method to rank and compute the weights of the criteria. Offering stakeholders a secure interface and avoiding unwanted access to cloud-stored data mitigates E-healthcare risks. The key derivation ensures end-to-end data. ciphering to prevent unauthorized use (KDF). This work provides robust security solutions for various environments. This work can meet security needs for people and secure-communicating organizations. We found the data privacy is the best criterion.

Keywords: Neutrosophic Set, Multi-Criteria Decision Making (MCDM), Data Security, Privacy-preserving, Authentication, Access Control, Uncertainty.

1. Introduction

The Large data volumes make manually storing and maintaining health records for future reference difficult [1]. Most unusual is the coronavirus epidemic's overcrowding of hospitals. Due to its inability to accommodate more patients, healthcare systems in the US, Brazil, and India are under strain [2]. The global pandemic's impact on healthcare is

incomprehensible [3]. Manually recording data makes it hard to find a patient's information in a record room full of health records. Finding a patient's medical record is time-consuming. Disasters can also wipe data. Since the data is in plain text, it can be hacked and read, written, or modified [4].

Recently, IoT medical record storage. E-healthcare security is crucial because health data is sensitive. Attackers exploit open wireless channels [5]. Attackers exploit open wireless channels [5]. These attacks could cause several E-healthcare difficulties. Consider a patient who is admitted to a hospital in a different city for treatment and then returned home. Later, he falls ill and is admitted to a local hospital, but he cannot access his previous data or files. A lack of understanding may postpone his treatment fatally. If the patient's information was saved on devices that could connect to the cloud, the new medical staff may start treatment immediately [6]. Health care can store encrypted data in the cloud using secure cryptographic techniques. These algorithms allow only authorized individuals to view the information from any remote place with internet connectivity, wired or wireless [7]. "Cloud" servers allow users to host a variety of applications and databases that can be viewed online. Cloud platforms exist worldwide [8]. Sponsors, health insurers, and healthcare organizations no longer need to maintain servers or administer applications [9].

E-healthcare can adapt in institutions without cloud-based services [10]. Paper can keep general hospital data, but the cloud can save essential data. Authorized users worldwide can securely share information [11]. Selected stakeholders can access, remove, and change data [12]. Protecting patient privacy and data integrity is difficult [13,14].

We evaluated the healthcare security by analyzing its criteria. We used the MCDM method to evaluate the criteria [25]. The healthcare security has many component as shown in Figure 1.

For a fresh take on ambiguity, imprecision, inconsistency, and fuzziness, see Florantin Smarandache's neutrosophic sets, which expand on Atanassov's intuitionistic fuzzy sets (IFSs). Smarandache defined a neutrosophic set with three parts: truth membership, indeterminacy membership, and falsity membership, and he established the degree of indeterminacy/neutrality as a new and independent component of fuzzy sets. The use of neutrosophic sets in decision-making may improve outcomes due to the indeterminacy parameter's contribution to a more precise formulation of membership functions [26,27]. A neutrosophic set, on the other hand, is more difficult to implement in actual scientific and technical domains. The distinction between absolute truth and relative truth in logic, as well as between absolute membership and relative non-membership, is a particularly valuable application of neutrosophic logic. A decision maker is relieved of the burden of ensuring that the sum of the items in a membership function for a given event is at most 1. If they're unrelated, the amount might go up to 3 [28, 29].

Saaty's AHP is a well-known approach for multi-criteria decision-making. Researchers may easily determine how important certain factors are by using this method. Several fuzzy variations of the conventional AHP approach have been developed as a response to inadequate data and unpredictability [30 ,31].

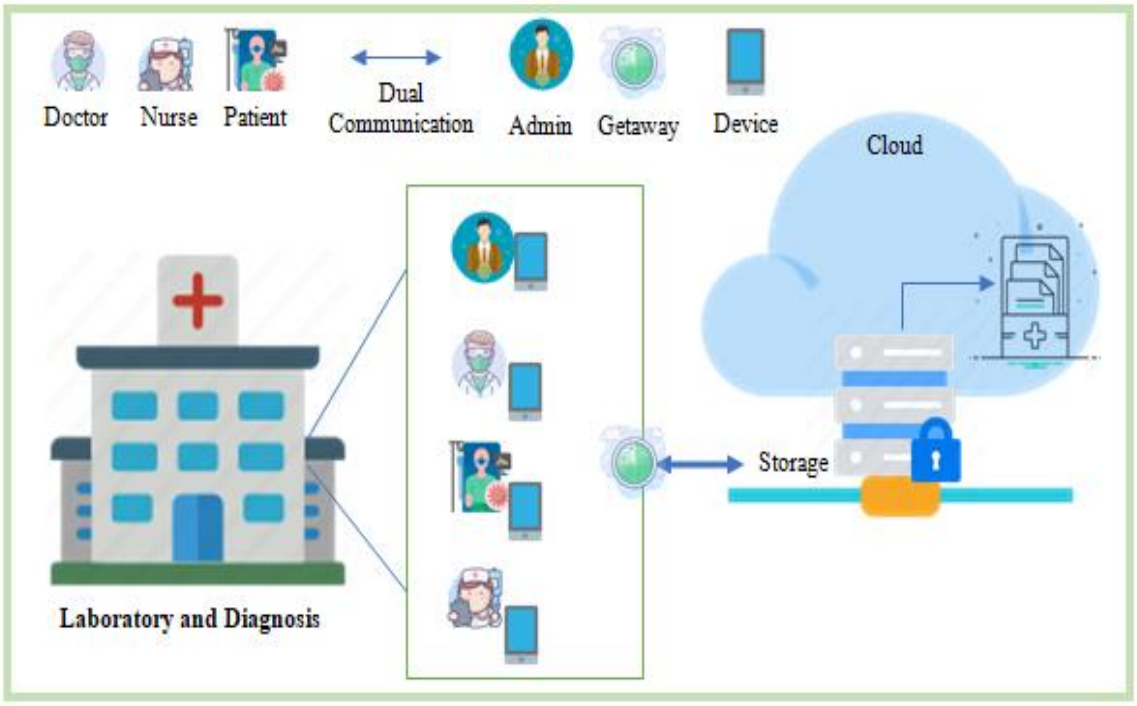

Figure 1. The component of the healthcare security.

2. Literature Review

In this sub-section, the most recent work relevant to the healthcare security is reviewed. It examines the literature and identifies the strengths and flaws of pertinent models. This subparagraph highlights academic attempts to develop new E-Healthcare security approaches [15]. Using Olutayo et al. [16] web-based solution. physicians, pharmacists, and nurses can access patients' health records. The local cloud holds patient information. Remotely editable data facilitates collaboration between hospitals and physicians through the sharing of patient records. This proposal limits patient access to their medical records.

A data sharing and profile pairing mechanism for Mobile Healthcare Social Networks (MHSN) in cloud computing for EHR is detailed in the approach [17]. Using an identity-based encryption system, the scheme enables the encryption of medical records. This approach permits conditional attribute-based re-encryption of data. This approach prevents eavesdropping on sensitive information. Using identity-based encryption and an equality test, MHSN's method for matching profiles is adaptable and secure.

A trust negotiation framework facilitates authentication, privacy, and user access for health services [18, 19]. Digital credentials enable secure transaction feature disclosure. This method cannot defend the E-healthcare system against all significant threats. Modular exponentiation-based group key agreement was proposed by S. Paliwal et al. [20]. The proposed method is secure against DOS assaults, but it is susceptible to replay attacks (lack of timestamp or random number), requires the identities of all communicating parties, loses anonymity, and cannot withstand impersonation.

The authors of [21] focused on privacy and E-Healthcare platform access control techniques. According to the authors, their access control technique is superior to others. The proposed access control technique relies on communication confidence. User behavior determines trust. If the user and service have mutual trust, the request is

permitted. The methodology confines record access to authorized, reliable personnel, according to the author. Li et al. [22] introduced a biometric-based authentication approach and emphasized that incorrectly developed biohashing-based protocols are susceptible to insider assaults. Comparing protocols for E-Healthcare security.

Existing systems are susceptible to numerous E-Healthcare security flaws. The vulnerabilities identified could be used by cybercriminals to execute cyberattacks against various medical devices. In terms of identity anonymity, authenticity, confidentiality, and communication integrity, the majority of provided techniques do not provide absolute security. Normal schemes are inadequate for mission-critical e-healthcare applications because they lack particular security features. Existing system frameworks contain vulnerabilities that allow unauthorized access to resources. In addition, older systems require extensive processing.

3 Neutrosophic AHP Method

Zadeh contributes to the literature by introducing the fuzzy theory, a method for dealing with ambiguity and uncertainty. To begin, the membership function is the single component of a fuzzy set. After that, a wide variety of fuzzy sets are created to help with uncertainty and ambiguity. Atanassov introduced a kind of fuzzy sets called intuitionistic fuzzy sets (IFSs) [32, 33]. The membership and non-membership functions of a fuzzy set generalize into IFSs. Smarandache extends fuzzy logic with a new function called "uncertainty" to create the neutrosophic logic as a more sophisticated form of IFSs that can more effectively handle ambiguity [34,35].

Neutrosophic set has three membership functions as truth, indeterminacy and falsity membership functions (X_T, X_I, X_F).

Definition 1

Interval valued neutrosophic number can be represented as:

$$X = \{x, [X_T^L, X_T^U], [X_I^L, X_I^U], [X_F^L, X_F^U]\} \quad (1)$$

Definition 2

We can convert the interval valued neutrosophic set into a crisp value by:

$$S(X) = \left(\frac{X_T^L + X_T^U}{2}\right) + \left(1 - \frac{X_I^L + X_I^U}{2}\right) X_I^U - \left(\frac{X_F^L + X_F^U}{2}\right)(1 - X_F^U) \quad (2)$$

Definition 3

We can compute some mathematical operations on interval valued neutrosophic numbers as:

$$x_1 = \left[{x_1}_T^L, {x_1}_T^U\right], \left[{x_1}_I^L, {x_1}_I^U\right], \left[{x_1}_F^L, {x_1}_F^U\right]; \quad x_2 = \left[{x_2}_T^L, {x_2}_T^U\right], \left[{x_2}_i^L, {x_2}_I^U\right], \left[{x_2}_F^L, {x_2}_F^U\right]$$

$$x_1 \oplus x_2 = \; < \begin{pmatrix} \left[{x_1}_T^L + {x_2}_T^L - {x_1}_T^L {x_2}_T^L, {x_1}_T^U + {x_2}_T^U - {x_1}_T^U {x_2}_T^U\right], \\ \left[{x_1}_I^L {x_2}_I^L, {x_1}_I^U {x_2}_I^U\right], \\ \left[{x_1}_F^L {x_2}_F^L, {x_1}_F^U {x_2}_F^U\right] \end{pmatrix} > \quad (3)$$

$$x_1 \ominus x_2 = < \begin{pmatrix} [x_{1_T}^L - x_{2_F}^U, x_{1_T}^U - x_{2_F}^L\ ], \\ [\max(x_{1_I}^L, x_{2_I}^L), \max(x_{1_I}^U x_{2_I}^U)], \\ [x_{1_F}^L - x_{2_T}^U, x_{1_F}^U - x_{2_T}^L] \end{pmatrix} > \quad (4)$$

$$x_1 \otimes x_2 = < \begin{pmatrix} [x_{1_T}^L x_{2_T}^L, x_{1_T}^U x_{2_T}^U], \\ [x_{1_I}^L + x_{2_I}^L - x_{1_I}^L x_{2_I}^L, x_{1_I}^U + x_{2_I}^U - x_{1_I}^U x_{2_I}^U], \\ [x_{1_F}^L + x_{2_F}^L - x_{1_F}^L x_{2_F}^L, x_{1_F}^U + x_{2_F}^U - x_{1_F}^U x_{2_F}^U] \end{pmatrix} > \quad (5)$$

$$x_1^{\wedge} = < \begin{pmatrix} [1 - (1 - x_{1_T}^L)^{\wedge}, 1 - (1 - x_{1_T}^U)^{\wedge}\ ], \\ [(x_{1_I}^L)^{\wedge}, (x_{1_I}^U)^{\wedge}], \\ [1 - (1 - x_{1_F}^L)^{\wedge}, 1 - (1 - x_{1_F}^U)^{\wedge}\ ] \end{pmatrix} > \quad (6)$$

$$\wedge x_1 = < \begin{pmatrix} [1 - (1 - x_{1_T}^L)^{\wedge}, 1 - (1 - x_{1_T}^U)^{\wedge}\ ], \\ [(x_{1_I}^L)^{\wedge}, (x_{1_I}^U)^{\wedge}], \\ [(x_{1_F}^L)^{\wedge}, (x_{1_F}^U)^{\wedge}] \end{pmatrix} > \quad (7)$$

Based on the logic of arranging issues in hierarchical and then assessing each element in the order via pairwise comparisons, the AHP technique was created and systematized by Thomas Saaty and introduced to the literature through systematization. Although AHP is widely utilized, there are situations when it does not accurately represent human reasoning when solving MCDM issues. IVN-AHP is an improvement over conventional AHP because it incorporates human cognition more effectively into the process of making choices and allows for a powerful expression of uncertainty using three variables.

Step 1. Build the comparison matrix

$$A = \begin{bmatrix} < [x_{11_T}^L, x_{11_T}^U], [x_{11_I}^L, x_{11_I}^U], [x_{11_F}^L, x_{11_F}^U] > & \cdots & < [x_{1m_T}^L, x_{1m_T}^U], [x_{1m_I}^L, x_{1m_I}^U], [x_{1m_F}^L, x_{1m_F}^U] > \\ \vdots & \ddots & \vdots \\ < [x_{m1_T}^L, x_{m1_T}^U], [x_{m1_I}^L, x_{m1_I}^U], [x_{m1_F}^L, x_{m1_F}^U] > & \cdots & < [x_{mm_T}^L, x_{mm_T}^U], [x_{mm_I}^L, x_{mm_I}^U], [x_{mm_F}^L, x_{mm_F}^U] > \end{bmatrix} \quad (8)$$

Step 2. Add the numbers in every column

$$Ad = < \begin{pmatrix} [\sum_{k=1}^m x_{kj_T}^L, \sum_{k=1}^m x_{kj_T}^U,], \\ [\sum_{k=1}^m x_{kj_I}^L, \sum_{k=1}^m x_{kj_I}^U,] \\ [\sum_{k=1}^m x_{kj_F}^L, \sum_{k=1}^m x_{kj_F}^U,] \end{pmatrix} > \quad (9)$$

Step 3. Normalize the pairwise comparison matrix

$$Z_{ij} = < \begin{pmatrix} \left[\frac{x_{kj_T}^{L}}{\sum_{k=1}^{m} x_{kj_T}^{U}}, \frac{x_{kj_T}^{U}}{\sum_{k=1}^{m} x_{kj_T}^{U}}\right], \\ \left[\frac{x_{kj_I}^{L}}{\sum_{k=1}^{m} x_{kj_I}^{U}}, \frac{x_{kj_I}^{U}}{\sum_{k=1}^{m} x_{kj_I}^{U}}\right] \\ \left[\frac{x_{kj_F}^{L}}{\sum_{k=1}^{m} x_{kj_F}^{U}}, \frac{x_{kj_F}^{U}}{\sum_{k=1}^{m} x_{kj_F}^{U}}\right] \end{pmatrix} > \tag{10}$$

$$A = \begin{bmatrix} < \begin{pmatrix} \left[\frac{x_{11_T}^{L}}{\sum_{k=1}^{m} x_{kj_T}^{U}}, \frac{x_{11_T}^{U}}{\sum_{k=1}^{m} x_{kj_T}^{U}}\right], \\ \left[\frac{x_{11_I}^{L}}{\sum_{k=1}^{m} x_{kj_I}^{U}}, \frac{x_{11_I}^{U}}{\sum_{k=1}^{m} x_{kj_I}^{U}}\right], \\ \left[\frac{x_{11_F}^{L}}{\sum_{k=1}^{m} x_{kj_F}^{U}}, \frac{x_{11_F}^{U}}{\sum_{k=1}^{m} x_{kj_F}^{U}}\right] \end{pmatrix} > & \cdots & < \begin{pmatrix} \left[\frac{x_{1m_T}^{L}}{\sum_{k=1}^{m} x_{kj_T}^{U}}, \frac{x_{1m_T}^{U}}{\sum_{k=1}^{m} x_{kj_T}^{U}}\right], \\ \left[\frac{x_{1m_I}^{L}}{\sum_{k=1}^{m} x_{kj_I}^{U}}, \frac{x_{1m_I}^{U}}{\sum_{k=1}^{m} x_{kj_I}^{U}}\right], \\ \left[\frac{x_{1m_F}^{L}}{\sum_{k=1}^{m} x_{kj_F}^{U}}, \frac{x_{1m_F}^{U}}{\sum_{k=1}^{m} x_{kj_F}^{U}}\right] \end{pmatrix} > \\ \vdots & \ddots & \vdots \\ < \begin{pmatrix} \left[\frac{x_{m1_T}^{L}}{\sum_{k=1}^{m} x_{kj_T}^{U}}, \frac{x_{m1_T}^{U}}{\sum_{k=1}^{m} x_{kj_T}^{U}}\right], \\ \left[\frac{x_{m1_I}^{L}}{\sum_{k=1}^{m} x_{kj_I}^{U}}, \frac{x_{m1_I}^{U}}{\sum_{k=1}^{m} x_{kj_I}^{U}}\right], \\ \left[\frac{x_{m1_F}^{L}}{\sum_{k=1}^{m} x_{kj_F}^{U}}, \frac{x_{m1_F}^{U}}{\sum_{k=1}^{m} x_{kj_F}^{U}}\right] \end{pmatrix} > & \cdots & < \begin{pmatrix} \left[\frac{x_{mm_T}^{L}}{\sum_{k=1}^{m} x_{kj_T}^{U}}, \frac{x_{mm_T}^{U}}{\sum_{k=1}^{m} x_{kj_T}^{U}}\right], \\ \left[\frac{x_{mm_I}^{L}}{\sum_{k=1}^{m} x_{kj_I}^{U}}, \frac{x_{mm_I}^{U}}{\sum_{k=1}^{m} x_{kj_I}^{U}}\right], \\ \left[\frac{x_{mm_F}^{L}}{\sum_{k=1}^{m} x_{kj_F}^{U}}, \frac{x_{mms_F}^{U}}{\sum_{k=1}^{m} x_{kj_F}^{U}}\right] \end{pmatrix} > \end{bmatrix} \tag{11}$$

Step 4. Compute the weights of criteria

$$W = \begin{pmatrix} \frac{\left[\sum_{k=1}^{m} \frac{x_{1_T}^{L}}{\sum_{k=1}^{m} x_{kj_T}^{U}}, \sum_{k=1}^{m} \frac{x_{1_T}^{U}}{\sum_{k=1}^{m} x_{kj_T}^{U}}\right]}{m}, \\ \frac{\left[\sum_{k=1}^{m} \frac{x_{1_I}^{L}}{\sum_{k=1}^{m} x_{kj_I}^{U}}, \sum_{k=1}^{m} \frac{x_{1_I}^{U}}{\sum_{k=1}^{m} x_{kj_I}^{U}}\right]}{m}, \\ \frac{\left[\sum_{k=1}^{m} \frac{x_{1_F}^{L}}{\sum_{k=1}^{m} x_{kj_F}^{U}}, \sum_{k=1}^{m} \frac{x_{1_F}^{U}}{\sum_{k=1}^{m} x_{kj_F}^{U}}\right]}{m} \end{pmatrix} \tag{12}$$

Step 5. Rank the healthcare security criteria.

4. Analysis of criteria

We analysis the healthcare security criteria by the interval valued neutrosophic numbers. We collected nine criteria in this paper.

Security is of the utmost importance for healthcare providers because of the sensitive nature of patient data and the importance of the services they offer [23, 24]. The following factors should be taken into account while assessing healthcare security criteria:

Safeguarding sensitive patient information is of utmost importance. HIPAA (Health Insurance Portability and Accountability Act) and other data protection rules necessitate that healthcare providers take strong precautions to secure their patients' personal information. Secure access restrictions, frequent security audits, and breach response strategies are all things to consider.

Authentication and access controls are essential for protecting private data and computer systems. Strong access

control techniques, such as multi-factor authentication, role-based access restrictions, and user provisioning procedures, should be implemented in organizations. It's crucial to conduct regular checks of user access privileges and promptly revoke access for dismissed workers or contractors.

To avoid hacking and other forms of data leaks, it is crucial to keep the network's infrastructure secure. Firewalls, intrusion detection/prevention systems, and secure network segmentation are all tools that may help businesses protect their most vital information. Potential security flaws must be assessed regularly, and patches must be applied promptly.

Data centers, server rooms, and secure storage locations all need to be protected with stringent physical security protocols. It is important to have security measures in place including access limits, video monitoring, and intrusion detection. Secure destruction procedures should be followed when disposing of paper documents or electronic storage devices.

Management of Security problems: Effectively identifying, responding to, and recovering from security problems requires dependable incident response and management procedures. Clear roles and responsibilities, incident reporting processes, and frequent testing and training exercises are all essential components of an organization's incident response strategy.

Employees have a crucial part in security, thus it's important to raise awareness and provide training on the topic. Security concerns, best practices for data management, and spotting and reporting security problems are all topics that employees should be trained on regularly.

In the healthcare industry, third-party service providers and suppliers play a vital role. To guarantee the safety of shared data and systems, it is essential to assess their security procedures. Third-party risk evaluations, as well as continuous monitoring of an organization's security practices, should all be included in contractual agreements.

HIPAA, the General Data Protection Regulation, and the Health Information Trust Alliance are just a few of the regulations that healthcare providers must follow. Evaluation of security procedures should heavily weigh how well they conform to these rules.

The availability and data integrity of vital systems and information are dependent on healthcare organizations having solid business continuity and disaster recovery strategies. It is crucial to regularly test and update these strategies to lessen the effect of any possible interruptions.

These healthcare security criteria may be used to provide a safe space for patients' information, keep services running smoothly, and prevent breaches.

Step 1. We build the comparison matrix between criteria by using Eq. (8). We collected the nine criteria to be used in this study. We used the linguistic scale of interval valued neutrosophic set to evaluate the criteria in the comparison matrix as shown in Table 1.

Table 1. The interval valued neutrosophic comparison matrix.

	$HSER_1$	$HSER_2$	$HSER_3$	$HSER_4$	$HSER_5$	$HSER_6$	$HSER_7$	$HSER_8$	$HSER_9$

HSER1	1	⟨[0.95,1.0],[0.0,0.0],[0.0,0.10]⟩	⟨[0.80,0.90],[0.05,0.10],[0.10,0.20]⟩	⟨[0.55,0.65],[0.30,0.40],[0.35,0.45]⟩	⟨[0.90,0.95],[0.0,0.05],[0.05,0.15]⟩	⟨[0.90,0.95],[0.0,0.05],[0.05,0.15]⟩	⟨[0.80,0.90],[0.05,0.10],[0.10,0.20]⟩	⟨[0.95,1.0],[0.0,0.0],[0.0,0.10]⟩	⟨[0.95,1.0],[0.0,0.0],[0.0,0.10]⟩
HSER2	⟨[0.95,1.0],[0.0,0.0],[0.0,0.10]⟩	1	⟨[0.70,0.80],[0.15,0.25],[0.20,0.30]⟩	⟨[0.90,0.95],[0.0,0.05],[0.05,0.15]⟩	⟨[0.55,0.65],[0.30,0.40],[0.35,0.45]⟩	⟨[0.80,0.90],[0.05,0.10],[0.10,0.20]⟩	⟨[0.90,0.95],[0.0,0.05],[0.05,0.15]⟩	⟨[0.55,0.65],[0.30,0.40],[0.35,0.45]⟩	⟨[0.80,0.90],[0.05,0.10],[0.10,0.20]⟩
HSER3	⟨[0.80,0.90],[0.05,0.10],[0.10,0.20]⟩	⟨[0.70,0.80],[0.15,0.25],[0.20,0.30]⟩	1	⟨[0.80,0.90],[0.05,0.10],[0.10,0.20]⟩	⟨[0.95,1.0],[0.0,0.0],[0.0,0.10]⟩	⟨[0.90,0.95],[0.0,0.05],[0.05,0.15]⟩	⟨[0.90,0.95],[0.0,0.05],[0.05,0.15]⟩	⟨[0.65,0.75],[0.20,0.30],[0.25,0.35]⟩	⟨[0.65,0.75],[0.20,0.30],[0.25,0.35]⟩
HSER4	⟨[0.55,0.65],[0.30,0.40],[0.35,0.45]⟩	⟨[0.90,0.95],[0.0,0.05],[0.05,0.15]⟩	⟨[0.80,0.90],[0.05,0.10],[0.10,0.20]⟩	1	⟨[0.70,0.80],[0.15,0.25],[0.20,0.30]⟩	⟨[0.90,0.95],[0.0,0.05],[0.05,0.15]⟩	⟨[0.80,0.90],[0.05,0.10],[0.10,0.20]⟩	⟨[0.90,0.95],[0.0,0.05],[0.05,0.15]⟩	⟨[0.80,0.90],[0.05,0.10],[0.10,0.20]⟩
HSER5	⟨[0.90,0.95],[0.0,0.05],[0.05,0.15]⟩	⟨[0.55,0.65],[0.30,0.40],[0.35,0.45]⟩	⟨[0.95,1.0],[0.0,0.0],[0.0,0.10]⟩	⟨[0.70,0.80],[0.15,0.25],[0.20,0.30]⟩	1	⟨[0.70,0.80],[0.15,0.25],[0.20,0.30]⟩	⟨[0.95,1.0],[0.0,0.0],[0.0,0.10]⟩	⟨[0.65,0.75],[0.20,0.30],[0.25,0.35]⟩	⟨[0.65,0.75],[0.20,0.30],[0.25,0.35]⟩
HSER6	⟨[0.90,0.95],[0.0,0.05],[0.05,0.15]⟩	⟨[0.80,0.90],[0.05,0.10],[0.10,0.20]⟩	⟨[0.90,0.95],[0.0,0.05],[0.05,0.15]⟩	⟨[0.90,0.95],[0.0,0.05],[0.05,0.15]⟩	⟨[0.70,0.80],[0.15,0.25],[0.20,0.30]⟩	1	⟨[0.70,0.80],[0.15,0.25],[0.20,0.30]⟩	⟨[0.95,1.0],[0.0,0.0],[0.0,0.10]⟩	⟨[0.65,0.75],[0.20,0.30],[0.25,0.35]⟩
HSER7	⟨[0.80,0.90],[0.05,0.10],[0.10,0.20]⟩	⟨[0.90,0.95],[0.0,0.05],[0.05,0.15]⟩	⟨[0.90,0.95],[0.0,0.05],[0.05,0.15]⟩	⟨[0.80,0.90],[0.05,0.10],[0.10,0.20]⟩	⟨[0.95,1.0],[0.0,0.0],[0.0,0.10]⟩	⟨[0.70,0.80],[0.15,0.25],[0.20,0.30]⟩	1	⟨[0.70,0.80],[0.15,0.25],[0.20,0.30]⟩	⟨[0.95,1.0],[0.0,0.0],[0.0,0.10]⟩
HSER8	⟨[0.95,1.0],[0.0,0.0],[0.0,0.10]⟩	⟨[0.55,0.65],[0.30,0.40],[0.35,0.45]⟩	⟨[0.65,0.75],[0.20,0.30],[0.25,0.35]⟩	⟨[0.90,0.95],[0.0,0.05],[0.05,0.15]⟩	⟨[0.65,0.75],[0.20,0.30],[0.25,0.35]⟩	⟨[0.95,1.0],[0.0,0.0],[0.0,0.10]⟩	⟨[0.70,0.80],[0.15,0.25],[0.20,0.30]⟩	1	⟨[0.80,0.90],[0.05,0.10],[0.10,0.20]⟩
HSER9	⟨[0.95,1.0],[0.0,0.0],[0.0,0.10]⟩	⟨[0.80,0.90],[0.05,0.10],[0.10,0.20]⟩	⟨[0.65,0.75],[0.20,0.30],[0.25,0.35]⟩	⟨[0.80,0.90],[0.05,0.10],[0.10,0.20]⟩	⟨[0.65,0.75],[0.20,0.30],[0.25,0.35]⟩	⟨[0.65,0.75],[0.20,0.30],[0.25,0.35]⟩	⟨[0.95,1.0],[0.0,0.0],[0.0,0.10]⟩	⟨[0.80,0.90],[0.05,0.10],[0.10,0.20]⟩	1

Step 2. Add the numbers in every column by using Eq. (9).

Step 3. Normalize the pairwise comparison matrix by using Eqs. (10 and 11) as shown in Table 2.

Table 2. The Normalization matrix.

	HSER1	HSER2	HSER3	HSER4	HSER5	HSER6	HSER7	HSER8	HSER9
HSER1	0.093892	0.081637	0.079446	0.059066	0.09331	0.098941	0.093786	0.124938	0.131339

$HSER_2$	0.098259	0.085434	0.069515	0.095696	0.057593	0.086762	0.105509	0.072877	0.11011
$HSER_3$	0.117365	0.122048	0.099307	0.085063	0.099064	0.097607	0.105509	0.085996	0.090104
$HSER_4$	0.169023	0.094926	0.124134	0.106329	0.072574	0.097607	0.093786	0.118234	0.109959
$HSER_5$	0.104325	0.153796	0.103932	0.151898	0.103678	0.075917	0.111957	0.085577	0.090097
$HSER_6$	0.102918	0.106792	0.110341	0.118143	0.148111	0.108453	0.082062	0.125361	0.089646
$HSER_7$	0.117365	0.094926	0.110341	0.132911	0.108563	0.154932	0.117232	0.091834	0.131339
$HSER_8$	0.098592	0.153796	0.151498	0.117982	0.158942	0.113498	0.167474	0.131192	0.109959
$HSER_9$	0.09826	0.106645	0.151487	0.132911	0.158166	0.166282	0.122685	0.16399	0.137448

Step 4. Compute the weights of criteria by using Eq. (12) as shown in Figure 2.

Step 5. Rank the healthcare security criteria as shown in Figure 2. Data privacy is the best criterion.

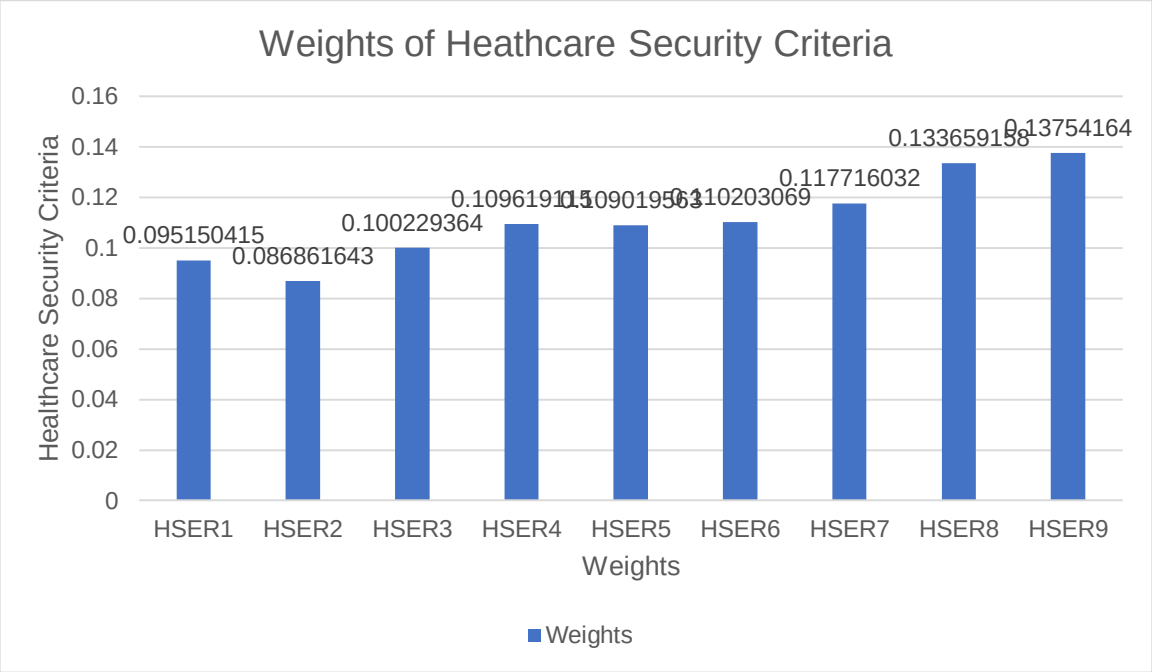

Figure 2. The weights of healthcare security criteria.

5. Conclusions

E-healthcare services are becoming increasingly popular as a result of the ease with which patients' medical records may be accessed and moved from one location to another. Because of their ability to supply solutions at a lower overall cost, cloud service providers have made it possible to practice telemedicine. Despite the many benefits it offers, the framework for storing information in the cloud and retrieving that information through the cloud is extremely susceptible since it makes use of open channels. Only authorized actors will be able to access and keep patient data under the secure interface. A full end-to-end encryption service that makes use of several KDF-derived keys is given to protect confidential patient data. The hospital is relieved of the responsibility of maintaining patient records, and improvements are made to both access to and storage of medical records.

We evaluate the criteria of healthcare security by using the interval-valued neutrosophic AHP method. The neutrosophic set is used to overcome the uncertain information. We used the AHP method to compute the weights of the criteria and evaluate them. We used the nine criteria. The main results show that data privacy is the best criterion.

Acknowledgments

This work is supported by the Hubei Provincial Science and Technology Major Project of China under the grant no. 2020AEA011 and by the Key Research & Development Plan of the Hubei Province of China under the grant no. 2020BAB100, as well as the project of Science, Technology and Innovation Commission of the Shenzhen Municipality of China under the grant no. JCYJ20210324120002006.

References

[1] Jigna J. Hathaliya, SudeepTanwar. An exhaustive survey on security and privacy issues in Healthcare 4 . 0.Computer Communications, 2020, 153:311-335

[2] Serdar Temiz, Didem G. Broo. Open Innovation Initiatives to Tackle COVID-19 Crises: Imposter Open Innovation and Openness in Data. IEEE Engineering Management Review, 2020, 48(4):46-54

[3] Hugues Turbé, Victor G. Ruiz, Mina Bjelogrlic, Jessica Rochat, Christian Lovis. Communicating on Multivariate and Geospatial Data supported by ergonomics criteria: COVID-19 case. 2020 Workshop on Visual Analytics in Healthcare (VAHC), MD, USA,2020, pp. 4-16

[4] Michael Veale, Reuben Binns, Jef Ausloos. When data protection by design and data subject rights clash. International Data Privacy Law, 2018, 8(2):105-123

[5] Parushi Malhotra, Yashwant Singh, Pooja Anand, Deep K. Bangotra, Pradeep K. Singh, Wei-Chiang Hong. Internet of Things: Evolution, Concerns and Security Challenges. Sensors, 2021, 21(5):1809

[6] Muhammad S. Hajar, M. O. Al-Kadri, Harsha K. Kalutarage. A survey on wireless body area networks: architecture, security challenges and research opportunities. Computers & Security, 2021, 104:102211

[7] Ali Ghubaish, Tara Salman, Maede Zolanvari, Devrim Unal, Abdulla Al-Ali, Raj Jain. Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security. IEEE Internet of Things Journal, 2021, 8(11): 8707-8718

[8] Ali Nirabi, Shihab A. Hameed. Mobile Cloud Computing For Emergency Healthcare Model:Framework. 2018 7th International Conference on Computer and Communication Engineering (ICCCE), Kuala Lumpur, Malaysia, 2018, pp. 375-379

[9] Hai Taoa, Md Z. Bhuiyanb, Md A. Rahman, Guojun Wangd, Tian Wange, Md. M. Ahmed, et al. Economic Perspective Analysis of Protecting Big Data Security and Privacy.Future Generation Computer Systems, 2019, 98:660-671

[10] Chanapha Butpheng, Kuo-Hui Yeh, Hu Xiong. Security and Privacy in IoT-Cloud-Based e-Health Systems—A Comprehensive Review. Symmetry, 2020, 12(7):1191

[11] Orestis Akrivopoulos, Ioannis Chatzigiannakis, Christos Tselios, Athanasios Antoniou. On the Deployment of

Healthcare Applications over Fog Computing Infrastructure. 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), Turin, Italy,2017, pp. 288-293

[12] Jayesh Patel. An Effective and Scalable Data Modeling for Enterprise Big Data Platform. 2019 IEEE International Conference on Big Data (Big Data),Los Angeles, CA, USA, 2019, pp. 2691-2697

[13] Tehsin Kanwal, Adeel Anjum, Abid Khan. Privacy preservation in e-health cloud: taxonomy, privacy requirements, feasibility analysis, and opportunities, Cluster Computing, 2021, 24(1):293-317

[14] Hao Jin, Yan Luo, Peilong Li, Jomol Mathew. A Review of Secure and Privacy-Preserving Medical Data Sharing, IEEE Access, 2019, 7:61656-61669

[15] Ayyoob Sharifi, Amir R. Khavarian-Garmsir, Rama K. R. Kummitha. Contributions of Smart City Solutions and Technologies to Resilience against the COVID-19 Pandemic : A Literature Review. sustainability journal, 2021, 13(14):8018

[16] Mehedi Masud, Gurjot S. Gaba, Karanjeet Choudhary, Roobaea Alroobaea, M. S. Hossain, A.M. Shamim. A robust and lightweight secure access scheme for cloud based E-healthcare. servicesPeer-to-Peer Networking and Applications, 2021, 14:3043-3057

[17] Qinlong Huang, Wei Yue, Yue He, Yixian Yang. Secure Identity-based Data Sharing and Profile Matching for Mobile Healthcare Social Networks in Cloud Computing. IEEE Access, 2018, 6:36584-36594

[18] M. S.Hossain, Ghulam Muhammad, Nadra Guizani. Explainable AI and Mass Surveillance System-based Healthcare Framework to Combat COVID-19 like Pandemics, IEEE Network, 2020, 34(4):126-132

[19] Long Hu, Meikang Qiu, Jeungeun Song, M. S. Hossain, Ahmed Ghoneim. Software defined healthcare networks. IEEE Wireless Communications, 2015, 22(6):67-75

[20] Swapnil Paliwal, Ch. A. Kumar. A Novel Multi-party Key Exchange Protocol. Advances in Intelligent Systems and Computin, 2018, pp.597-607, Springer, Cham

[21] Ashish Singh, Kakali Chatterjee. A Mutual Trust Based Access Control Framework for Securing Electronic Healthcare System. 2017 14th IEEE India Council International Conference (INDICON), Roorkee, India, 2017, pp. 1-6

[22] Xiong Li, Jianwei Niu, Md Z. Bhuiyan, Fan Wu, Marimuthu Karuppiah, Saru Kumari. A Robust ECC based Provable Secure Authentication Protocol with Privacy Preserving for Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 2017,14(8): 3599-3609

[23] Swapnil Paliwal, Ch. A. Kumar. A Novel Multi-party Key Exchange Protocol. Advances in Intelligent Systems and Computing, 2018, pp.597-607, Springer, Cham

[24] Sundara V. Karuppiah, Geetha Gurunathan. Secured storage and disease prediction of E-health data in cloud. Journal of Ambient Intelligence and Humanized Computing, 2021, 12:6295-306.

[25] A. Abdel-Monem and M. Abouhawwash, "A Machine Learning Solution for Securing the Internet of Things Infrastructures: https://doi. org/10.61185/SMIJ. HPAO9103," *Sustainable Machine Intelligence Journal*, vol. 1, 2022.

[26] J. Reig-Mullor, A. Garcia-Bernabeu, D. Pla-Santamaria, and M. Vercher-Ferrandiz, "Evaluating ESG corporate performance using a new neutrosophic AHP-TOPSIS based approach," *Technological and Economic*

Development of Economy, vol. 28, no. 5, pp. 1242–1266, 2022.

[27] E. Bolturk and C. Kahraman, "A novel interval-valued neutrosophic AHP with cosine similarity measure," *Soft Computing*, vol. 22, pp. 4941–4958, 2018.

[28] A. Sleem and I. Elhenawy, "Energy Efficiency and Material Cost Savings by Evolution of Solar Panels Used in Photovoltaic Systems under Neutrosophic Model," *Neutrosophic Systems with Applications*, vol. 5, pp. 36–43, 2023.

[29] P. Gulum, E. Ayyildiz, and A. T. Gumus, "A two level interval valued neutrosophic AHP integrated TOPSIS methodology for post-earthquake fire risk assessment: An application for Istanbul," *International Journal of Disaster Risk Reduction*, vol. 61, p. 102330, 2021.

[30] E. Eryarsoy, H. S. Kilic, S. Zaim, and M. Doszhanova, "Assessing IoT challenges in supply chain: A comparative study before and during-COVID-19 using interval valued neutrosophic analytical hierarchy process," *Journal of Business Research*, vol. 147, pp. 108–123, 2022.

[31] A. Abdelhafeez, H. Mahmoud, and A. S. Aziz, "Identify the most Productive Crop to Encourage Sustainable Farming Methods in Smart Farming using Neutrosophic Environment," *Neutrosophic Systems with Applications*, vol. 6, pp. 17–24, 2023.

[32] E. Ayyildiz and A. Taskin, "A Novel Interval Valued Neutrosophic AHP-WASPAS Methodology for Emergency Supply Depot Location Selection Problems," in *Multi-Criteria Decision Analysis*, CRC Press, 2022, pp. 251–266.

[33] N. Cizmecioglu, H. S. Kilic, Z. T. Kalender, and G. Tuzkaya, "Selection of the Best Software Project Management Model via Interval-Valued Neutrosophic AHP," in *Intelligent and Fuzzy Techniques for Emerging Conditions and Digital Transformation: Proceedings of the INFUS 2021 Conference, held August 24-26, 2021. Volume 2*, Springer, 2022, pp. 388–396.

[34] F. Kutlu Gündoğdu and C. Kahraman, "Hospital performance assessment using interval-valued spherical fuzzy analytic hierarchy process," *Decision Making with Spherical Fuzzy Sets: Theory and Applications*, pp. 349–373, 2021.

[35] B. Y. Kavus, P. G. Tas, E. Ayyildiz, and A. Taskin, "A three-level framework to evaluate airline service quality based on interval valued neutrosophic AHP considering the new dimensions," *Journal of Air Transport Management*, vol. 99, p. 102179, 2022.

Received: June 3, 2023. Accepted: Sep 27, 2023