Acta Scientiarum

http://periodicos.uem.br/ojs/acta
ISSN on-line: 1807-8664
Doi: 10.4025/actascitechnol.v47i1.71128

Evaluating the Security of a “Blind Quantum Algorithm-centered Medical Privacy Data Sharing Model” Using the DHGF Method

Lijuan Wu*, Jin Wei and Hui Jiang

Department of Computer Teaching, Changzhi Medical College, Changzhi, Shanxi, 046000, China. *Author for correspondence E-mail: wulj@czmc.edu.cn

ABSTRACT. This research addresses the academic challenge of lacking security verification methods for quantum computing models. It innovatively introduces the DHGF comprehensive evaluation method into the quantum security field, successfully overcoming the adaptability bottleneck of traditional evaluation methods in quantum scenarios. The research proposes a cross-verification method between a classical algorithm-based evaluation system and a quantum security model, constructing a methodological framework for cross-validation between classical algorithms and quantum technology. This enables dynamic evaluation of blind quantum computing protocols using the DHGF comprehensive evaluation method. Taking a "Blind Quantum Algorithm-centered Medical Privacy Data Sharing Model" as an example, the research demonstrates the entire process of evaluating the security of a privacy data model built on quantum algorithms and technology using the classical DHGF comprehensive evaluation method. The evaluation process integrates the Delphi method, Analytic Hierarchy Process, Grey System Theory, and Fuzzy Comprehensive Evaluation. The Delphi method is used to determine the evaluation indicator set based on expert opinions; the Analytic Hierarchy Process is employed to determine the weights of the evaluation indicators; and then the evaluation is conducted using the Grey System Theory and Fuzzy Comprehensive Evaluation. This research leverages mature and reliable classical algorithms to validate the security of a model built using quantum algorithms and technologies as its core. This approach establishes a cross-validation system integrating classical and quantum techniques, resulting in a dynamically scalable paradigm for quantum security assessment. This represents a bold extension of classical algorithms into the quantum domain. The comprehensive evaluation score Z from the research results demonstrates the algorithm's ability to accurately and quantitatively describe the dynamic security of the model, providing a novel solution for security analysis of complex and uncertain models and holding significant practical value.

Keywords: safety evaluation; integrated algorithm; quantitative analysis; Index system.

Received on January 29, 2024.
Accepted on February 19, 2025.

Introduction

With the rapid advancement of quantum technology, numerous quantum algorithms have been proposed (Montanaro, 2016). In order to verify the correctness of these quantum algorithms, researchers have continually attempted various methods. Chapter 8 of the referenced literature (Nielsen & Chuang, 2010) presents various techniques for validating quantum algorithms. This chapter discusses the methods for verifying and validating quantum algorithms. After analyzing the literature, three typical methods for validating quantum algorithms can be identified. The initial approach involves validating quantum algorithms through mathematical means. Researchers will strictly derive and analyze each process and step in the quantum algorithm to ensure that the algorithm can reach the correct conclusion in all cases. Literature (Nakahara & Ohmi, 2008) provides a detailed exposition of the mathematical foundations of quantum computing and algorithm validation methods. Paper (Xie et al., 2021) introduces the quantum search algorithm and substantiates its accuracy through mathematical theory. In literature (Qu et al., 2021), a comprehensive safety analysis of the proposed model is conducted through mathematical derivation and proof.

Another approach involves validating the accuracy of the quantum algorithm through simulation on a classical computer. Due to the current early stage of development of quantum computers and their lack of practical application, researchers validate quantum algorithms by creating simulation environments on classical computers. Reference (Hu et al., 2020) describes the simulation of the algorithm on amplitude-damped channels using the IBM Qiskit quantum simulator and the IBM q5 Tenerife quantum device. (Gong et al., 2023) The proposed model was simulated using a simulation method.

The third approach involves researchers validating the accuracy of quantum algorithms through laboratory experiments using experimental equipment. In article (Abhijith et al., 2022), quantum computing algorithms and their implementation on real quantum hardware are detailed. Additionally, it provides guidance on implementing these algorithms on IBM's quantum computer and discusses the distinctions between simulators and real hardware operation. Reference (Lanyon et al., 2007) offers detailed insight into the process of experimental design and implementation, along with verification of the results of experimental validation of quantum algorithms. Reference (Vandersypen et al., 2001) describes the experimental process of implementing the quantum Shor algorithm using nuclear magnetic resonance technology and discusses the experimental results and the verification of the algorithm's correctness. Reference (Chuang et al., 1998) introduces a method for experimentally verifying the quantum Deutsch-Jozsa algorithm. In the practical application of the aforementioned three verification methods, we have found that for algorithms with relatively simple structures and smaller scales, experimental verification and the use of simulation and modeling methods are feasible. However, for algorithms with more complex architectures, larger scales, and multiple modules, it is generally only possible to use mathematical tools and quantum-related theories to complete the verification of the algorithm. In earlier research, we introduced a “Blind Quantum Algorithm-centered Medical Privacy Data Sharing Model” (Wei et al., 2023) (hereinafter referred to as the "sharing model"). The model centered around the blind quantum algorithm and incorporating classical networks, quantum transmission channels, and quantum computers to ensure the secure transmission, sharing, and computations of private data. Currently, quantum computers and quantum communication are still in the research, development, and trial stages. Thus, it would be impractical to validate the model scheme's security solely through simulation or construction of a large-scale quantum network and quantum computer. In this context, we rely on pertinent quantum theory and mathematical tools to substantiate, derive, and assess the model's robustness. Given the extensive nature of the model and its numerous components, demonstrating the overall model's security entails individually verifying the security of each part. Subsequently, we can infer and evaluate the model's security based on the security evaluation outcomes of each component.

During the verification process, we uncovered two significant issues: inefficient verification and an inadequate level of rigor in the process. Firstly, because each component must be individually subjected to security verification, the time spent and the steps executed are numerous, leading to low verification efficiency. Secondly, to more closely approximate the actual application environment, we prefer the model to be in a dynamic operational state, conducting security verification on dynamic indicators such as the model's operational process, operational steps, and the collaborative working state of each component. Only in this way can it hold genuine significance.

As a result, our research team endeavored to identify an alternative verification method. The present paper illustrates the comprehensive process of assessing the security of the” Blind Quantum Algorithm-centered Medical Privacy Data Sharing Model" using the DHGF classical algorithm. It aims to confirm the viability of evaluating quantum algorithms using classical algorithms and to present a novel perspective and methodology for authenticating quantum algorithms. The DHGF comprehensive evaluation method (Xin et al., 2023) (hereinafter referred to as the "the DHGF method") is relatively mature and boasts wide applicability due to its ability to integrate qualitative and quantitative information and handle ambiguity and uncertainty. It has been successfully applied in various fields, including risk assessment, decision support, resource allocation and optimization, evaluation and prediction, as well as environmental assessment, healthcare, and military applications (Xu et al., 2022). Therefore, applying the DHGF method to the field of quantum technology and quantum algorithms is a bold and worthwhile endeavor. This provides a novel approach and valuable experience for the security evaluation of this type of model.

Model structure

Our team proposed the "Blind Quantum Algorithm-centered Medical Privacy Data Sharing Model". This model comprises three main components: data retrieval, data transmission, and data scientific computation. As the research progresses further, we have identified issues such as high conversion costs and significant resource investment in transforming classical client information into quantum information. Consequently, we have revised the relevant sections of the model concerning the conversion of classical-to- quantum information. The Trusted Central Proxy Server (TCPS) has been redesigned into a distributed architecture, meaning that multiple TCPS servers now exist within the network. These TCPS servers are responsible for converting classical information sent by medical institutions into quantum information, thereby achieving complete classicization on the client side. The revised model is depicted in Figure 1.

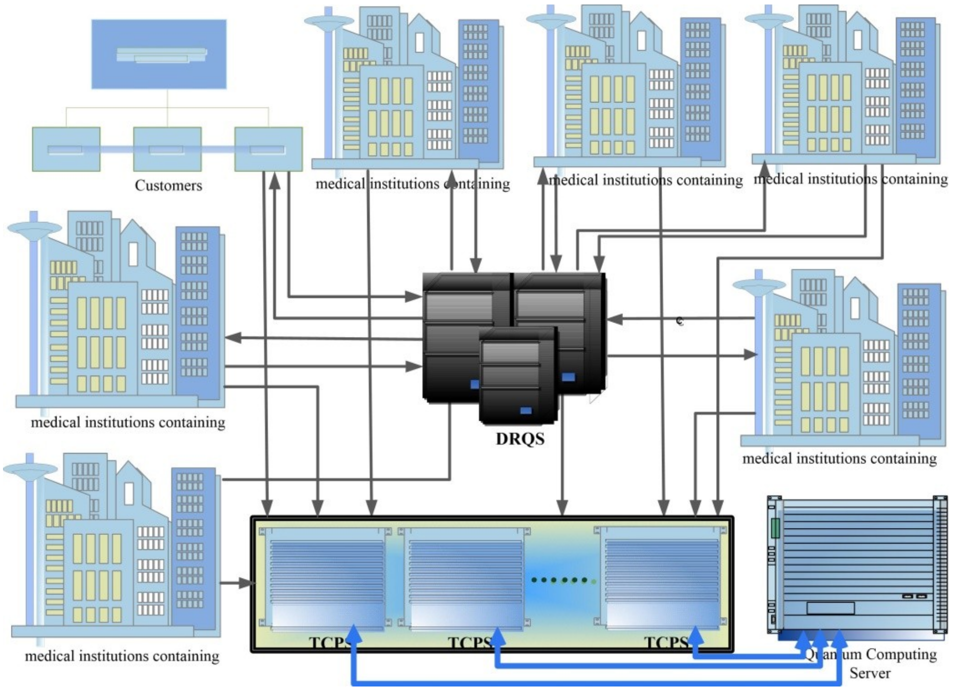
Customers
medical institutions containing
medical institutions containing
medical institutions containing
medical institutions containing
medical institutions containing
medical institutions containing
DRQS
TCPS
TCPS
TCPS
Quantum Computing Server

Figure 1. Structure of the Medical Privacy Data Sharing model

Model the business process

The business process of the privacy data sharing model is divided into five stages: data sharing request, data resource retrieval, data transmission, data computation, and data result querying. The business process is illustrated in Figure 2. (Wei et al., 2023).

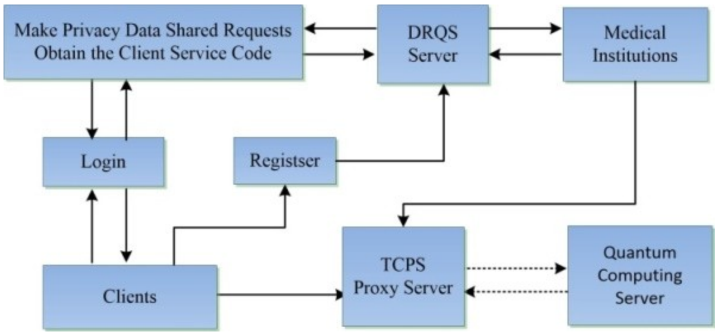

Figure 2. Privacy sharing model business process

Registered clients submit medical privacy data sharing requests to the Data Resource Query Server (DRQS). The DRQS generates a client service code and uses the request content to search its data resource directory, identifying data sources and affiliated institutions. Based on the search results, the DRQS sends data sharing requests, along with the client service code, to multiple medical institution servers that store the user's requested information. Each medical institution's data server corresponds to the client service code. Following the data directory sent by the DRQS, the data is aggregated and organized within a closed network and then transmitted, along with the client service code, to the TCPS via a dedicated classical channel.

The TCPS consolidates the received client service codes and classical information from different medical institutions, converting the classical information into quantum data. Subsequently, it queues the quantum information for transmission to the blind quantum computing server.

During the privacy data scientific computation phase, the blind quantum server creates a brickwork and carries out the blind quantum computing protocol in two sequential stages: data preparation and data computation, aimed at performing scientific computations on the data. Following the completion of the computation, both the TCPS and the quantum server will erase the original data and subsequently transmit the client service code along with the associated computation results to the TCPS server. Customers can access the computation results by logging in to the TCPS proxy server and entering the service code. The TCPS proxy server will regularly conduct a comprehensive removal of the completed computation tasks and their respective data.

Material and methods

This paper employs the DHGF method to demonstrate a security analysis and evaluation process for a “Blind Quantum Algorithm-centered Medical Privacy Data Sharing Model”. The DHGF method is based on Professor Qian Xuesen's proposed comprehensive integration method from qualitative to quantitative analysis and Professor Gu Jifa's research on the WSR method (Xu et al.). It integrates four different algorithms: the Delphi Method, the Analytic Hierarchy Process (AHP), Grey System Theory (GST), and Fuzzy Comprehensive Evaluation (FCE). These algorithms complement each other, realizing a comprehensive evaluation method that transforms qualitative analysis into quantitative analysis. The flow chart of the DHGF method is shown in Figure 3. First, the Delphi method is used to determine the security indicator set. Then, AHP is used to construct the indicator system and obtain weight values (Gao & Bernstein, 2025), while GST analyzes the correlation among the indicators. Finally, the evaluation results are obtained using FCE. Based on the above analysis results, a comprehensive security score for the model is calculated and analyzed. Throughout the algorithm, the Delphi method is not an independent algorithmic step but rather an expert consultation mechanism integrated throughout the DHGF method. It plays a crucial role in determining the indicator set, indicator system, weights, sample matrix, and grey levels for the sharing model, thus improving the accuracy and reliability of the comprehensive evaluation. Data was collected via an online survey tool. Upon completion, the survey data was exported to a database. After data cleaning and formatting, the database was used for the research presented in this paper.

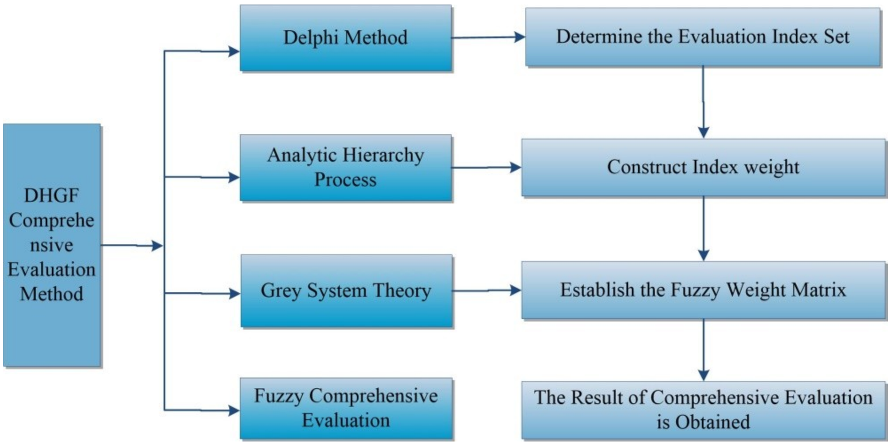
DHGF Comprehensive Evaluation Method
Delphi Method
Analytic Hierarchy Process
Grey System Theory
Fuzzy Comprehensive Evaluation
Determine the Evaluation Index Set
Construct Index weight
Establish the Fuzzy Weight Matrix
The Result of Comprehensive Evaluation is Obtained

Figure 3. The flow chart of the DHGF Method

Delphi Method

The Delphi method, also known as the expert survey method, underpins the security analysis and evaluation of sharing models in this study. We employed this method to construct a security evaluation indicator set for sharing models. Initially, a panel of qualified experts was selected. A structured questionnaire was then designed to facilitate expert judgment and model building. Multiple rounds of anonymous (Makhmutov, 2021) online surveys were conducted to collect expert assessments of sharing model security. The results of each round were aggregated, analyzed, and fed back to the experts, who then revised their opinions based on the previous round's findings. This iterative process continued until a consensus was reached, resulting in a security evaluation indicator set (Zhang & Xi, 2020), $U = (u_1, u_2, \ldots u_n)$. This approach minimizes subjective bias. The detailed procedure is shown in Figure 4.

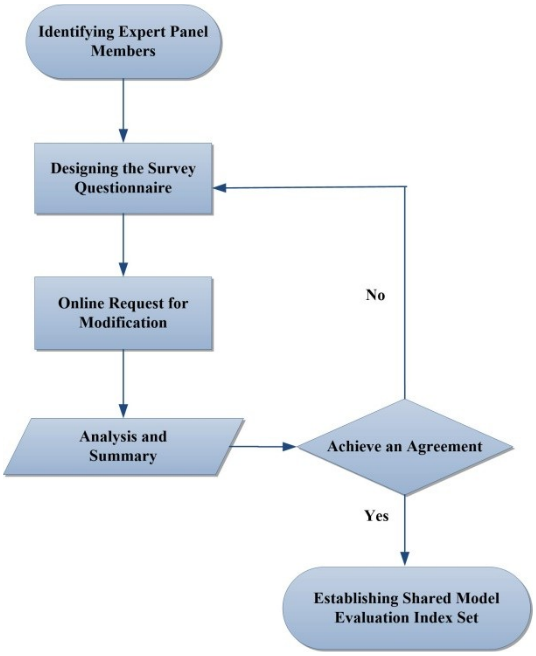
Identifying Expert Panel Members
Designing the Survey Questionnaire
Online Request for Modification
Analysis and Summary
Achieve an Agreement
No
Yes
Establishing Shared Model Evaluation Index Set

Figure 4. Delphi Method Process Diagram

Analytic Hierarchy Process (AHP)

AHP formally introduced by Thomas L. Saaty in 1980, is a widely used decision-making method and prioritization tool (Shekar & Mathew, 2023). AHP structures the problem hierarchically, linking influencing factors to create an analytical framework. This study employs AHP to construct a hierarchical model of the evaluation indicators (U) for the sharing model. Pairwise comparisons are used to determine the relative importance of indicators at each level. Expert panelists provide pairwise comparisons, generating judgment matrices that undergo consistency checks (Saini et al., 2022). Matrices passing these checks are used to calculate the weights of each indicator, ultimately yielding the weights for the sharing model's evaluation indicators. The detailed procedure is shown in Figure 5. (Zhu, 2022)

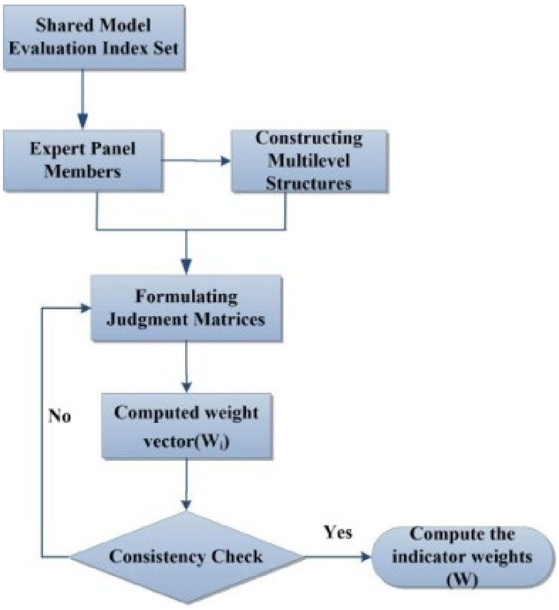
Shared Model Evaluation Index Set
Expert Panel Members
Constructing Multilevel Structures
Formulating Judgment Matrices
Computed weight vector(W_i)
No
Consistency Check
Yes
Compute the indicator weights (W)

Figure 5. AHP Method Process Diagram

Constructing Multilevel Structures

This study employs a three-level hierarchical structure to evaluate the security of the sharing model (Im et al., 2021). This structure comprises a Target Layer, a Criterion Layer, and an Indicator Layer. As shown in Figure 6 (Chong et al., 2017). The Target Layer defines the overall objective of the security evaluation. The

Criterion Layer consists of five key criteria directly influencing security: B_1-B_5. These criteria are further decomposed into 18 indicators (B_{11}, B_{12}, B_{21}...B_{54}) at the Indicator Layer. This hierarchical structure facilitates a hierarchical decomposition of the sharing model's security evaluation, effectively reflecting the hierarchical and systematic nature of the evaluation criteria.

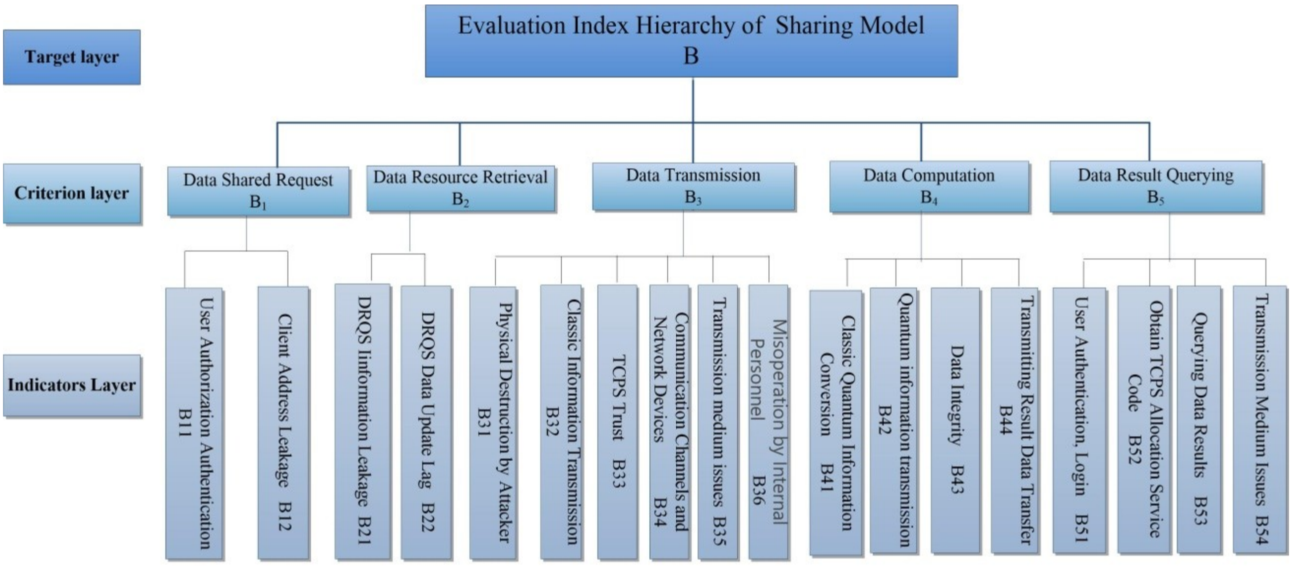
Target layer
Evaluation Index Hierarchy of Sharing Model B
Criterion layer
Data Shared Request B1
Data Resource Retrieval B2
Data Transmission B3
Data Computation B4
Data Result Querying B5
Indicators Layer
User Authorization Authentication B11
Client Address Leakage B12
DRQS Information Leakage B21
DRQS Data Update Lag B22
Physical Destruction by Attacker B31
Classic Information Transmission B32
TCPS Trust B33
Communication Channels and Network Devices B34
Transmission medium issues B35
Misoperation by Internal Personnel B36
Classic Quantum Information Conversion B41
Quantum information transmission B42
Data Integrity B43
Transmitting Result Data Transfer B44
User Authentication, Login B51
Obtain TCPS Allocation Service Code B52
Querying Data Results B53
Transmission Medium Issues B54

Figure 6. Evaluation Index Hierarchy of Sharing Model

Formulating Judgment Matrices

Experts leveraging their professional knowledge and experience, used Professor Saaty's 1-9 scale in Table 1 (Shekar & Mathew, 2023) to construct an n×n judgment matrix B. Each element, B_{ij}, represents the relative importance of criterion i to criterion j, judgment Matrix satisfies properties (Fan et al., 2022): $a_{ij} = {}^{1}/_{a_{ji}}$

Table 1. Meaning of the 1-9 Scale

Scale	Definition	Explain
1	Equal importance	Two activities contribute equally to the objective
3	Moderate importance	Experience and judgment slightly favor one activity over another
5	Strong importance	Experience and judgment strongly favor one activity over another
7	Very strong	An activity is favored very strongly over another
9	Extreme importance	The evidence favoring one activity over another is of the highest possible order of affirmation
Intermediate values: 2,4,6,8 is between the quantitative scale grades when the compromise is between two adjacent criteria		

For example, through expert consultation on the sharing model, the elements of the criterion layer were compared pairwise in terms of their importance relative to the elements of the target layer ,The judgment matrix B for the criterion layer-target layer was constructed (Harsha et al., 2022), as shown in Matrix 1 below: experts considered data resource retrieval B2 to be more important relative to data sharing request B1, assigning it a scale of 5.

Matrix 1 Criterion-Target Layer Judgment Matrix B

$$
\mathrm{B} = \begin{bmatrix} B & B_1 & B_2 & B_3 & B_4 & B_5 \\ B_1 & 1 & {}^{1}/_{5} & {}^{1}/_{6} & {}^{1}/_{9} & {}^{1}/_{3} \\ B_2 & 5 & 1 & {}^{1}/_{2} & {}^{1}/_{5} & 3 \\ B_3 & 6 & 2 & 1 & {}^{1}/_{4} & 2 \\ B_4 & 9 & 5 & 4 & 1 & 8 \\ B_5 & 3 & {}^{1}/_{3} & {}^{1}/_{2} & {}^{1}/_{8} & 1 \end{bmatrix}
$$

Using the same method, the judgment matrices B_1, B_2, B_3, B_4, and B_5 for the indicator layer-criterion layer were established, as shown in Matrix 2.

Matrix 2 Indicators-Criterion Layer Judgment Matrix B_1-B_5

$$B_1 = \left[\begin{array}{ccc} B_1 & B_{11} & B_{12} \\ B_{11} & 1 & 3 \\ B_{12} & {}^{1}/_{3} & 1 \end{array}\right] \quad B_2 = \left[\begin{array}{ccc} B_2 & B_{21} & B_{22} \\ B_{21} & 1 & {}^{1}/_{8} \\ B_{22} & 8 & 1 \end{array}\right]$$

$$B_3 = \left[\begin{array}{ccccccc} B_3 & B_{31} & B_{32} & B_{33} & B_{34} & B_{35} & B_{36} \\ B_{31} & 1 & {}^{1}/_{2} & {}^{1}/_{8} & 1 & 3 & {}^{1}/_{2} \\ B_{32} & 2 & 1 & {}^{1}/_{3} & 4 & 8 & 5 \\ B_{33} & 8 & 3 & 1 & 7 & 8 & 4 \\ B_{34} & 1 & {}^{1}/_{4} & {}^{1}/_{7} & 1 & 6 & {}^{1}/_{3} \\ B_{35} & {}^{1}/_{3} & {}^{1}/_{8} & {}^{1}/_{8} & {}^{1}/_{6} & 1 & {}^{1}/_{6} \\ B_{36} & 2 & {}^{1}/_{5} & {}^{1}/_{4} & 3 & 6 & 1 \end{array}\right]$$

$$B_4 = \left[\begin{array}{ccccc} B_4 & B_{41} & B_{42} & B_{43} & B_{44} \\ B_{41} & 1 & 3 & 4 & 7 \\ B_{42} & {}^{1}/_{3} & 1 & 4 & 3 \\ B_{43} & {}^{1}/_{4} & {}^{1}/_{4} & 1 & 8 \\ B_{44} & {}^{1}/_{7} & {}^{1}/_{3} & {}^{1}/_{8} & 1 \end{array}\right] \quad B_5 = \left[\begin{array}{ccccc} B_5 & B_{51} & B_{52} & B_{53} & B_{54} \\ B_{51} & 1 & {}^{1}/_{5} & {}^{1}/_{4} & 7 \\ B_{52} & 5 & 1 & 1 & 7 \\ B_{53} & 4 & 1 & 1 & 9 \\ B_{54} & {}^{1}/_{7} & {}^{1}/_{7} & {}^{1}/_{9} & 1 \end{array}\right]$$

Computed weight vector

The weight vector can quantitatively express the relative importance among different indicators, transforming qualitative judgments into quantitative weight values. Based on the numerical values of the elements in the judgment matrix, the weight vector is calculated. There are many methods for calculating the weight vector, and this study employs the geometric mean method. According to formula (1), the m-th root of the product of the row vectors of the judgment matrix is obtained, denoted as $\bar{W_i}$.Normalization, as shown in formula (2), yields the weight vector W_i.

$$\bar{W_i} = \sqrt[m]{\prod_{j=1}^{m} a_{ij}} \text{ (1) } W_i = \frac{\bar{W_i}}{\sum \bar{W_i}} \text{ (2)}$$

The 5th root of the product of the first row vector in the criterion-target layer judgment matrix

$$\text{B: } \bar{W}_B = \sqrt[5]{1 \times {}^{1}/_{5} \times {}^{1}/_{6} \times {}^{1}/_{9} \times {}^{1}/_{3}} = 0.2620$$

Sequentially compute the other row vectors of the Criterion-Target Layer judgment matrix B to form a vector matrix:

$$\bar{W_B} = [0.2620,1.0845,1.4310,4.2823,0.5743]$$

After normalization, we find the weights of the Criterion-Target Layer judgment matrix:

$$W_B = [0.0343,0.1421,0.1874,0.5609,0.0752]$$

Same method, we find the weight of Indicators-Criterion Layer judgment matrix:

$$W_{B_1} = [0.7500,0.2500] \quad W_{B_2} = [0.1111,0.8889] \quad W_{B_3} = [0.0748,0.2416,0.4544,0.0715,0.0254,0.1224]$$
$$W_{B_4} = [0.6309,0.2287,0.1143,0.0261] \quad W_{B_5} = [0.1361,0.4304,0.4335,0.0386$$

Consistency check

The inherent subjectivity in expert understanding of decision criteria can lead to inconsistencies in the judgment matrix. Therefore, a consistency check is crucial in the AHP process to ensure the logical soundness of the matrix. This check uses the Consistency Ratio (C.R.), as shown in formula (3). C.R. $\leqslant 0.1$ indicates acceptable consistency, allowing the AHP calculations to proceed. Conversely, C.R. > 0.1 signifies significant inconsistency, necessitating matrix revision and a repeated consistency check. (Batool et al., 2023; Neto et al., 2024).

$$\text{C.R.} = \frac{\text{C.I.}}{\text{R.I.}} \text{ (3)}$$

Among them:

$$\mathrm{C.I.} = \frac{\lambda_{max}-n}{n-1} \quad (4)$$

$$\lambda_{max} = \frac{1}{n}\sum_{i=1}^{n}\frac{\sum_{j=1}^{n} a_{ij}w_j}{w_i} \quad (5)$$

R.I. (Random Consistency Index) : The average random consistency index for a judgment matrix of a given size, obtained from Table 2 (Ghimire & Kim, 2018).

C.I. (Consistency Index): A measure of inconsistency in the judgment matrix, calculated using formula (4). The smaller the C.I. value, the better the consistency. When C.I. = 0, it indicates a perfectly consistent judgment matrix.

λ_{max}: The maximum eigenvalue of the judgment matrix, calculated using formula (5). For a perfectly consistent matrix, $\lambda_{max} = n$ (n is the matrix order). The greater the difference between λ_{max} and *n*, the more inconsistent the judgment matrix.

Table 2. Comparison table of average random consistency index

n	1	2	3	4	5	6	7	8	9	10
R.I.	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49

Compute the indicator weights W

Once the judgment matrix has passed a consistency check, the calculated indicator weights (W_i) are multiplied by the corresponding criterion weights (W_B) to produce the weight.

For example: The weight for the index layer "User Authorization Authentication B_{11}" is:

$$W_{11} = W_{B11} \times W_B = 0.7500 \times 0.343 = 0.0257$$

Same method, the remaining weights are calculated to form the weight matrix W:

W = [0.0257,0.0086,0.0158,0.1263,0.0140,0.0453,0.0870,0.0134,0.0048,0.0229,0.3539,0.1283,0.0641, 0.0146,0.0102,0.0324,0.0326,0.0029]

Grey System Theory (GST)

Grey System Theory is an analytical method based on incomplete and uncertain information. It can be used for effective prediction, decision-making, and evaluation under conditions of insufficient or uncertain data (Ghosh & Banerjee, 2021). The specific steps are shown in Figure 7.

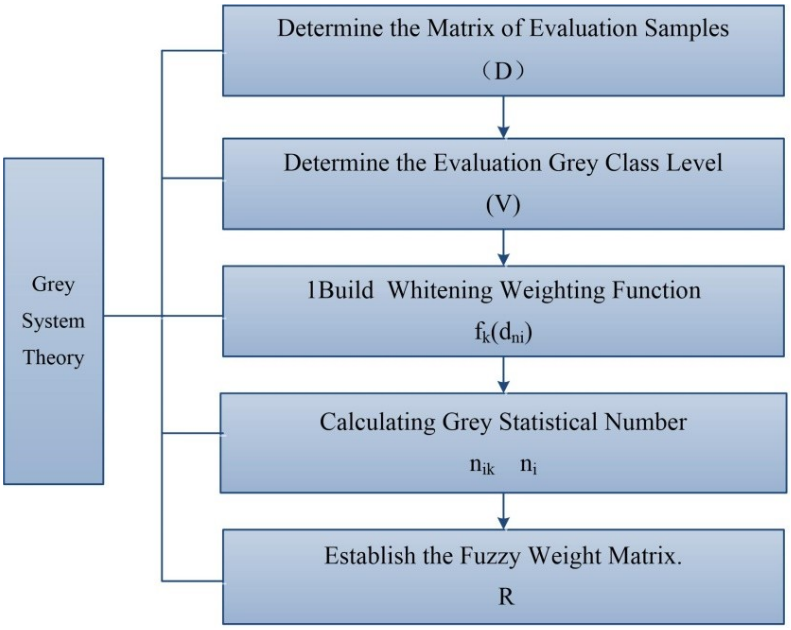
Grey System Theory
Determine the Matrix of Evaluation Samples (D)
Determine the Evaluation Grey Class Level (V)
1Build Whitening Weighting Function $f_k(d_{ni})$
Calculating Grey Statistical Number n_{ik} n_i
Establish the Fuzzy Weight Matrix. R

Figure 7. Grey System Theory Process Diagram

Specify the evaluation sample matrix D

The sample matrix D is fundamental. This matrix organizes and presents data from multiple samples across multiple evaluation criteria. In sample matrix D, rows represent evaluation indicators, and columns represent expert samples. d_{ij} represents the value of the j-th expert on the i-th evaluation indicator.

$$\mathrm{D} = d_{ij} = \begin{bmatrix} d_{11} & d_{12} & \cdots & d_{1m} \\ d_{21} & d_{22} & & d_{2m} \\ \vdots & & \ddots & \vdots \\ d_{n1} & d_{n2} & \cdots & d_{nm} \end{bmatrix}$$

To address the needs of the shared model, we invited 10 experts, s_1, s_2, ..., s_{10}, to individually score the impact of each indicator in the indicator layer on security. This resulted in a sample matrix D, as shown in Matrix 3.

Matrix 3: Sample Matrix D for Sharing Model

$$\mathrm{D} = \begin{bmatrix} 7 & 6 & 6 & 5 & 4 & 6 & 4 & 6 & 6 & 5 \\ 4 & 5 & 8 & 4 & 5 & 3 & 7 & 4 & 8 & 9 \\ 6 & 7 & 6 & 5 & 6 & 7 & 7 & 7 & 9 & 8 \\ 6 & 8 & 9 & 8 & 9 & 7 & 9 & 8 & 9 & 6 \\ 3 & 4 & 5 & 4 & 3 & 5 & 6 & 9 & 5 & 7 \\ 8 & 8 & 5 & 7 & 6 & 8 & 8 & 6 & 7 & 9 \\ 7 & 5 & 8 & 6 & 6 & 6 & 6 & 9 & 6 & 8 \\ 5 & 4 & 8 & 6 & 7 & 4 & 8 & 7 & 5 & 5 \\ 3 & 2 & 6 & 4 & 2 & 4 & 5 & 5 & 5 & 6 \\ 5 & 5 & 7 & 2 & 5 & 5 & 7 & 5 & 6 & 2 \\ 8 & 9 & 6 & 7 & 8 & 8 & 5 & 8 & 8 & 6 \\ 8 & 9 & 8 & 8 & 7 & 7 & 8 & 9 & 7 & 3 \\ 7 & 6 & 7 & 6 & 9 & 6 & 4 & 9 & 9 & 8 \\ 8 & 7 & 7 & 6 & 5 & 5 & 6 & 9 & 9 & 9 \\ 5 & 3 & 2 & 3 & 4 & 5 & 9 & 7 & 9 & 9 \\ 6 & 9 & 4 & 5 & 5 & 8 & 3 & 8 & 9 & 5 \\ 7 & 3 & 6 & 5 & 6 & 6 & 4 & 9 & 6 & 8 \\ 4 & 2 & 3 & 4 & 3 & 3 & 6 & 5 & 6 & 2 \end{bmatrix}$$

Determine evaluation grade

Based on measurement theory and expert opinions, an empirical analysis of the shared model's security aspects was conducted. Experts categorized the security assessment of the shared model into four levels: Excellent, Good, Medium, and Poor. Within a 0-10 range, the set of evaluation levels is represented as:

$V = [v_1, v_2, v_3, v_4] = [9, 7, 5, 3]$.

Constructing whitening weight function

The threshold method is used to determine the maximum, median, and minimum values of the sample matrix D. Based on the evaluation grey class grade V, the whitenization weight function is determined (Tan et al., 2016).

(1) For the first grey class ‘excellent’, gray number$\otimes \in [9, +\infty]$, its whitening weight function is shown in formula (6).

$$f_1(d_{ij}) = \begin{cases} \frac{d_{ij}}{9} \; d_{ij} \in [0,9] \\ 1 \; d_{ij} \in (9, +\infty) \\ 0 \; d_{ij} \in (-\infty, 0) \end{cases} (6)$$

（2）For the second grey class ‘good’, gray number$\otimes \in [0,7,14]$,its whitening weight function is shown in formula (7):

$$f_2(d_{ij}) = \begin{cases} \frac{d_{ij}}{7} \; d_{ij} \in [0,7) \\ 2 - \frac{d_{ij}}{7} \; d_{ij} \in [7,14] \\ 0 \; d_{ij} \notin [0,14) \end{cases} (7)$$

(3) For the third grey class ‘medium’, gray number⊗ ∈ [0,5,10],its whitening weight function is shown in formula (8):

$$f_3(d_{ij}) = \begin{cases} \frac{d_{ij}}{5} \; d_{ij} \in [0,5) \\ 2 - \frac{d_{ij}}{5} \; d_{ij} \in [5,10] \\ 0 \; d_{ij} \notin [0,10) \end{cases} (8)$$

(4) For the fourth grey class ‘poor’, gray number⊗ ∈ [0,3,6], its whitening weight function is shown in formula (9):

$$f_4(d_{ij}) = \begin{cases} 2 - \frac{d_{ij}}{3} \; d_{ij} \in [3,6) \\ 1 \; d_{ij} \in [0,3] \\ 0 \; d_{ij} \notin [0,6) \end{cases} \quad (9)$$

Calculating grey statistical number

According to grey theory, the whitening weight function can determine the weight $f_k\ (d_{ij})$ of each expert's score d_{ij} within the k-th category evaluation grey class, and represent it as n_{ik}. Thus, formula (10) is obtained by computing the grey statistics of each indicator associated with the k-th category evaluation grey class. The total grey statistical number (n_i) for each evaluation indicator is shown in formula (11).

$$n_{ik} = \sum_{i=1}^{10} f_k\left(d_{ij}\right) (10) \; n_i = \sum_{k=1}^{4} n_{ik} \; (11)$$

Calculate the grey statistical for n_{11} according to Formula (10).

$$n_{11} = f_1(7) + f_1(6) + f_1(6) \cdots f_1(5) = 6.111$$

The same can be calculated: $n_{12} = 7.857$, $n_{13} = 8.200$, $n_{14} = 2.000$

From Equation (11), The total grey statistical number for n1:

$n_1 = n_{11}+n_{12}+n_{13}+n_{14} = 24.168$

Similarly, calculating the grey statistical n_{ik} for the remaining 17 indications and the total grey statistical counts n_i results in the following matrix (Kong et al., 2024).

$$n_{ik} = \begin{bmatrix} 6.111 & 7.857 & 8.200 & 2.000 \\ 6.333 & 7.000 & 6.600 & 3.667 \\ 7.556 & 8.857 & 6.400 & 0.333 \\ 8.778 & 8.143 & 4.200 & 1.000 \\ 5.667 & 6.714 & 7.400 & 4.333 \\ 8.000 & 8.571 & 5.600 & 0.333 \\ 7.444 & 8.429 & 6.600 & 0.333 \\ 6.556 & 7.857 & 7.400 & 2.333 \\ 4.667 & 6.000 & 7.600 & 5.333 \\ 5.444 & 7.000 & 7.800 & 3.667 \\ 8.111 & 8.429 & 5.400 & 0.333 \\ 8.222 & 8.286 & 4.400 & 1.000 \\ 7.889 & 8.143 & 5.400 & 0.667 \\ 7.889 & 8.143 & 5.800 & 0.667 \\ 6.222 & 8.286 & 5.600 & 4.333 \\ 6.889 & 7.143 & 6.400 & 2.667 \\ 6.667 & 7.714 & 6.800 & 2.000 \\ 4.222 & 5.429 & 6.800 & 6.667 \end{bmatrix} n_i = \begin{bmatrix} 24.168 \\ 23.600 \\ 23.146 \\ 22.121 \\ 24.114 \\ 22.505 \\ 22.806 \\ 24.146 \\ 23.600 \\ 23.911 \\ 22.273 \\ 21.908 \\ 22.099 \\ 22.499 \\ 22.441 \\ 23.099 \\ 23.181 \\ 23.118 \end{bmatrix}$$

Establish the fuzzy weight matrix

The grey weight of the i-th evaluation factor under criterion k is given by r_{ij}. These values constitute the fuzzy weight matrix $R = (r_{ij})_{18\times4}$. As shown in Equation (12). The fuzzy weight values for the sharing model are shown in Figure 8

$$R = r_{ij} = \frac{n_{ik}}{n_i} (12)$$

$$R = \begin{bmatrix} 0.253 & 0.325 & 0.339 & 0.083 \\ 0.268 & 0.297 & 0.280 & 0.155 \\ 0.326 & 0.383 & 0.277 & 0.014 \\ 0.397 & 0.368 & 0.190 & 0.045 \\ 0.235 & 0.278 & 0.307 & 0.180 \\ 0.355 & 0.381 & 0.249 & 0.015 \\ 0.326 & 0.370 & 0.289 & 0.015 \\ 0.271 & 0.325 & 0.306 & 0.097 \\ 0.198 & 0.254 & 0.322 & 0.226 \\ 0.228 & 0.293 & 0.326 & 0.153 \\ 0.364 & 0.378 & 0.242 & 0.015 \\ 0.375 & 0.378 & 0.201 & 0.046 \\ 0.357 & 0.368 & 0.244 & 0.030 \\ 0.351 & 0.362 & 0.258 & 0.030 \\ 0.277 & 0.280 & 0.250 & 0.193 \\ 0.298 & 0.309 & 0.277 & 0.115 \\ 0.288 & 0.333 & 0.293 & 0.086 \\ 0.183 & 0.235 & 0.294 & 0.288 \end{bmatrix}$$

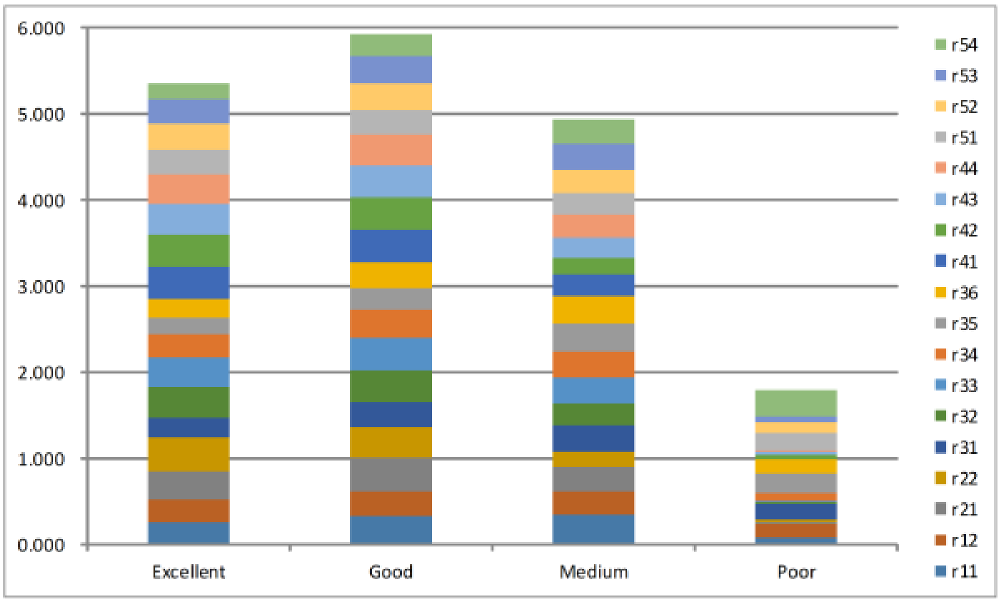

Figure 8. Diagram of Fuzzy Weights for the Sharing Model.

Fuzzy comprehensive method

Fuzzy comprehensive evaluation provides a means of assessing information characterized by fuzziness and uncertainty (Hou et al., 2024). In the context of sharing model security verification, this method entails the computation of a fuzzy evaluation matrix B, derived from a composite calculation of the previously defined fuzzy weight matrix R and the indicator weight matrix W. As shown in Equation (13).

$$B = W \cdot R \ (13)$$

The comprehensive evaluation matrix for the sharing model is:

$$B = [0.3491, 0.3648, 0.2463, 0.0426]$$

Finally, the fuzzy comprehensive assessment matrix B is multiplied by the evaluation grey class level V^T, as indicated in the following formula (14).

$$Z = B \cdot V^T \ (14)$$

The fuzzy comprehensive evaluation value for the sharing model:

$$Z = [0.3491, 0.3648, 0.2463, 0.0426] \cdot \begin{bmatrix} 9 \\ 7 \\ 5 \\ 3 \end{bmatrix} = 7.0553$$

Results and discussion

The magnitude of the comprehensive evaluation value Z reflects the security of the sharing model, with a larger Z value indicating better security. Based on the four security levels of the sharing model—excellent, good, fair, and poor—represented by the set V = [v1, v2, v3, v4] = [9, 7, 5, 3], the research result shows Z = 7.0553, Z∈ (7, 9). This indicates that the security of the medical privacy data sharing model based on blind quantum computation is generally at a 'good' level.

A comprehensive evaluation model, based on the DHGF method, was developed using a "Evaluating the Security of a 'Blind Quantum Algorithm-centered Medical Privacy Data Sharing Model' Using the DHGF Method" as a case study. This model leverages the strengths of multiple evaluation algorithms to holistically assess the complex indicators of the data sharing model, providing both qualitative and quantitative evaluations. By transcending the limitations of single-algorithm approaches, it offers practical applicability and ensures a more comprehensive and balanced assessment. The resulting evaluation is characterized by its comprehensiveness, reliability, ability to handle uncertainty, and strong interpretability and generality.

This study introduces the DHGF method for evaluating the security of a blind quantum-based medical privacy data sharing model. This approach, however, is not limited to medical applications; its framework and evaluation process offer broad applicability and significant potential in other domains requiring sensitive data security assessment, including finance and the Internet of Things (Ghosh & Banerjee, 2021) and the evaluation of blind quantum computation-based data sharing platforms. The high privacy sensitivity of these areas underscores the significant value of this method for assessing data breach risks.

This study has limitations, including localized data collection, potential bias in expert opinions, and the grey theory's prediction accuracy being sensitive to sample. Future work will focus on optimizing the model architecture, diversifying the data, and exploring hybrid methods to enhance predictive accuracy.

Conclusion

This study investigates the application of the DHGF algorithm in the security evaluation of a "Blind Quantum Algorithm-centered Medical Privacy Data Sharing Model" The results show that the model achieves a 'good' level in security analysis.

The innovation of this research lies in the introduction of the DHGF algorithm, which overcomes the limitations of traditional single-dimensional and static evaluations. It achieves a paradigm shift from single-dimensional static testing to multi-modal dynamic verification, validating the irreplaceable engineering value of classical algorithms in quantum security verification. This provides new insights for the security assessment of quantum computing technologies in practical applications and demonstrates the innovative potential of integrating classical and quantum technologies. In the future, we will focus on validating the model with real data and exploring the integration of other advanced security technologies to further enhance the robustness of the proposed framework.

Acknowledgements

The authors thank the funding Research Project Supported by Shanxi Scholarship Council of China.

References

Abhijith, J., Adedoyin, A., Ambrosiano, J., Anisimov, P., Casper, W., Chennupati, G., Lokhov, A. Y. (2022). Quantum Algorithm Implementations for Beginners. *ACM Transactions on Quantum Computing*, *3* (4), 1-92. https://doi.org/10.1145/3517340

Ashley, M. (2016). Quantum algorithms: An overview. *npj Quantum Information*, *2* (1). https://doi.org/10.1038/npjqi.2015.23

Batool, K., Zhao, Z.-Y., Nureen, N., & Irfan, M. (2023). Assessing and prioritizing biogas barriers to alleviate energy poverty in Pakistan: An integrated AHP and G-TOPSIS model. *Environmental Science and Pollution Research*, *30* (41), 94669-94693. https://doi.org/10.1007/s11356-023-28767-4

Chong, T., Yi, S., & Heng, C. (2017). Application of set pair analysis method on occupational hazard of coal mining. *Safety Science*, *92*, 10-16. https://doi.org/10.1016/j.ssci.2016.09.005

Chuang, I. L., Vandersypen, L. M. K., Zhou, X., Leung, D. W., & Lloyd, S. (1998). Experimental realization of a quantum algorithm. *Nature (London), 393* (6681), 143-146. https://doi.org/10.1038/30181

Fan, X., Tian, S., Lu, Z., & Cao, Y. (2022). Quality evaluation of entrepreneurship education in higher education based on CIPP model and AHP-FCE methods. *Frontiers in Psychology*, *13*. https://doi.org/10.3389/fpsyg.2022.973511

Gao, T., & Bernstein, P. (2025). Physical Appearance Design Evaluation of Community Emotional Healing Installations Based on Analytic Hierarchy Process–Fuzzy Comprehensive Evaluation Method. *Buildings*, *15* (5), 773. https://doi.org/10.3390/buildings15050773

Ghimire, L. P., & Kim, Y. (2018). An analysis on barriers to renewable energy development in the context of Nepal using AHP. *Renewable Energy*, *129*, 446-456. https://doi.org/10.1016/j.renene.2018.06.011

Ghosh, N., & Banerjee, I. (2021). IoT-based freezing of gait detection using grey relational analysis. *Internet of Things*, *13*, 100068. https://doi.org/10.1016/j.iot.2019.100068

Gong, C., Zhu, H., Gani, A., & Qi, H. (2023). QGA–QGCNN: A model of quantum gate circuit neural network optimized by quantum genetic algorithm. *The Journal of Supercomputing*, *79* (12), 13421-13441. https://doi.org/10.1007/s11227-023-05158-7

Harsha, G. Anish, T. S., Rajaneesh, A., Prasad, Megha K., Mathew, R., Mammen, P. C., Ajin, R. S., & Kuriakose, S. L. (2022). Dengue risk zone mapping of Thiruvananthapuram district, India: A comparison of the AHP and F-AHP methods. *GeoJournal*, *88* (3), 2449-2470. https://doi.org/10.1007/s10708-022-10757-7

Hou, J., Gao, T., Yang, Y., Wang, X., Yang, Y., & Meng, S. (2024). Battery inconsistency evaluation based on hierarchical weight fusion and fuzzy comprehensive evaluation method. *Journal of Energy Storage*, *84*, 110878. https://doi.org/10.1016/j.est.2024.110878

Hu, Z., Xia, R., & Kais, S. (2020). A quantum algorithm for evolving open quantum dynamics on quantum computing devices. *Scientific Reports*, *10* (1). https://doi.org/10.1038/s41598-020-60321-x

Im, K. H., Kim, W., & Hong, S. J. (2021). A study on single pilot resource management using integral fuzzy analytical hierarchy process. *Safety*, *7* (4), 84. https://doi.org/10.3390/safety7040084

Kong, F., Geng, J., Kang, Y., Jin, X., Hao, S., & Wang, M. (2024, May 17-19). *Evaluation of main responsibility of safety production in power engineering enterprises based on DHGF* [Conference paper]. 2024 4th International Conference on Electrical Power and Energy Technology (ICEPET), Beijing, China. https://doi.org/10.1109/icepet61938.2024.10627512

Lanyon, B. P., Weinhold, T. J., Langford, N. K., Barbieri, M., James, D. F. V., Gilchrist, A., & White, A. G. (2007). Experimental demonstration of a compiled version of Shor's algorithm with quantum entanglement. *Physical Review Letters*, *99* (25). https://doi.org/10.1103/PhysRevLett.99.250505

Makhmutov, R. (2021). The Delphi method at a glance. *Pflege*, *34* (4), 221-221. https://doi.org/10.1024/1012-5302/a000812

Montanaro, A. (2016). Quantum algorithms: An overview. *npj Quantum Information*, *2* (1). https://doi.org/10.1038/npjqi.2015.23

Neto, D. D. H., Figueiredo, M., Moraes, H. B., Campos Filho, L. C. P., & Nelio. (2024). Feasibility analysis of implementing a logistics integration center in amazon region using AHP. *Acta Scientiarum, Technology*, *47* (1), e66976. https://doi.org/10.4025/actascitechnol.v47i1.66976

Nakahara, M., & Ohmi, T. (2008). *Quantum computing: From linear algebra to physical realizations*. CRC Press.

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information* (10th anniversary ed.). Cambridge University Press.

Qu, Z., Wang, K., & Zheng, M. (2021). Secure quantum fog computing model based on blind quantum computation. *Journal of Ambient Intelligence and Humanized Computing*, *13* (8), 3807-3817. https://doi.org/10.1007/s12652-021-03402-7

Saini, V., Li, J., Yang, Y., & Li, J. (2022). Evaluating environmental quality in Rujigou coalfield, China, using analytic hierarchy process. *Environmental Science and Pollution Research*, *30* (1), 1841-1853. https://doi.org/10.1007/s11356-022-22340-1

Shekar, P. R., & Mathew, A. (2023). Integrated assessment of groundwater potential zones and artificial recharge sites using GIS and Fuzzy-AHP: A case study in Peddavagu watershed, India. *Environmental Monitoring and Assessment*, *195* (7). https://doi.org/10.1007/s10661-023-11474-5

Tan, C., Lu, Y., & Zhang, X. (2016). Life extension and repair decision-making of ageing offshore platforms based on DHGF method. *Ocean Engineering*, *117*, 238-245. https://doi.org/10.1016/j.oceaneng.2016.03.048

Vandersypen, L. M. K., Steffen, M., Breyta, G., Yannoni, C. S., Sherwood, M. H., & Chuang, I. L. (2001). Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, *414*, 883-887.

Wei, J., Jiang, H., & Wu, L. (2023). Design of medical privacy data sharing model based on blind quantum computing. *Computer Era*, *(10),* 32-34, 39. https://doi.org/10.16644/j.cnki.cn33-1094/tp.2023.10.007

Xie, X. M., Duan, L. Z., Qiu, T. R., & Kang, X. L. (2021). Search Space Self-adaptive Quantum Search Algorithm. *Xiaoxing Weixing Jisuanji Xitong = Journal of Chinese Computer Systems*, *42* (4), 732.

Xin, J., Wang, C., Tang, Q., Zhang, R., & Yang, T. (2023). An evaluation framework for construction quality of bridge monitoring system using the DHGF method. *Sensors*, *23* (16), 7139. https://doi.org/10.3390/s23167139

Xu, W., Huang, Y., Song, S., Cao, G., Yu, M., Cheng, H., Zhu, Z., Wang, S., Xu, L., & Li, Q. (2022). A bran-new performance evaluation model of coal mill based on GA-IFCM-IDHGF method. *Measurement: Journal of the International Measurement Confederation*, *195*, 110954. https://doi.org/10.1016/j.measurement.2022.110954

Zhang, W. Q., & Xi, Z. L. (2020). Application of Delphi method in screening of indexes for measuring soil pollution value evaluation. *Environmental Science and Pollution Research*, *28* (6), 6561-6571. https://doi.org/10.1007/s11356-020-10919-5

Zhu, Y. (2022). Research on adaptive combined wind speed prediction for each season based on improved gray relational analysis. *Environmental Science and Pollution Research*, *30* (5), 12317-12347. https://doi.org/10.1007/s11356-022-22957-2