Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0030.v1

Article

Evaluating Software Security in the Era of Quantum Computer by Using Fuzzy TOPSIS

Mohd. Nadeem [1,*], Dr. Syed Anas Ansar [2], Masood. Ahmad [1], Dr. Prabhash Chandra Pathak [2], Dr. Rajeev Kumar [3] and Prof. Raees Ahmad Khan [1]

[1] Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow; mohd.nadeem1155@gmail.com
[2] School of Computer Application, Babu Banarasi Das University, Lucknow; syed000anas@gmail.com
[3] Rajeev Kumar, Centre for Innovation and Technology, Administrative Staff College of India; rs0414@gmail.com
* Correspondence: mohd.nadeem1155@gmail.com; Tel.: +91-8318099719

Abstract: The development of quantum computers seeks software developers' attention regarding security in the era of Information Technology, software security is the primary goal for our quantitative assessment of software security in the development cycle of software. Security assessment of software is identifying the key security factors of the software. A security elective provides extensive strategies and calculations to ensure product safety. The security assessment is the key factor in surveying, administering, and controlling security to further enhance the nature of safety. It should be acknowledged that assessing security early on in the development process is beneficial in identifying worms, hazards, flaws, and threats. The definition and portrayal of Quantum Computing (QC) in software security will be discussed in this study. Researchers use cryptography calculations to secure our financial institutions, medical devices, military weaponry, planes, ships, vehicles, and pilots. Here authors of this study use the Fuzzy Technique for Order Preference by Similarity to Ideal Situation (FTOPSIS) to quantitatively assess the weight/rank of the quantum enable security alternatives like (*Diffie-Hellman key-exchange algorithm, Quantum key distribution algorithm, Deutsch-Jozsa Algorithm, Special Deutsch-Jozsa Algorithm, Grover's Algorithm and Quantum key distribution algorithm in GHZ state*) with security factors like (Confidentiality, Integrity, Authentication, Privacy, Reliability, Maintainability, Authorization, Integrity, Possessions, and Availability). Additionally, they critically analyze and select the six alternatives of quantum-based security algorithms. The nature of safety infers the ability to execute a thing on time in this exploration study, specifically 'software security'.

Keywords: Quantum Computing; Software Security; Quantum Algorithm; Quantum Security.

1. Introduction

Nonetheless, when the massive size of (i.e., 100 to 1000 qubit) QC is built, many cryptosystems will likely implode. Google has just promoted the Sycamore Processor 53 qubits. Such developments point to the future advent of massive quantum computers. The current cryptosystem would be rendered obsolete because quantum computers can easily handle cryptographic calculations in a few seconds [1]. As a result, it is critical to focus more on advanced research in regard to existing QC security. Cryptography techniques that satisfy the demands of security alternatives ease of use, and adaptability without jeopardizing the clients' confidence would be the primary challenges in the quantum period. QC is a game-changing advancement in the realm of information technology that can support global efforts in computing and software security. Software with insufficient strength is likely to fail in a highly competitive market; as a result, software development organizations are concentrating more on ensuring the stability of their product. The software development life cycle has several stages, including re-

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0030.v1

quirements planning, planning, coding, testing, investigation, and support. Upkeep is regarded as the final stage of development [2]. To ensure the software security at the developing stages makes the software durable. To attain practicality, programming convenience should be a primary strength. The time span during which developing computer program provides organizations is defined as solidity in a piece of software [3]. The evolving diverse environment of the twenty-first century creates new challenges for everyone, including the advanced computational device known as QC. Quantum security is the management of security throughout the quantum computing phase. Quantum computer innovation is improving at an incredible rate of computing these days. A group of researchers has successfully developed the Sycamore Processor, a fully quantum processor that can plan a quantum circuit in 200 seconds, compared to 10,000 years for an old-style supercomputer [4]. The ongoing design of encryption or security strategies for various organizations, web applications, software, monetary construction of encryption, security in privacy, and everything else that relies on a computer network is in question, and the sturdiness of software is also influenced by a quantum computer. The present safety measures used in the classic computer are symmetrical and lopsided. A comparable key is used to scramble and decode information in a symmetric approach. Different keys are employed in the imbalanced methodology. The security is entirely based on the security key, which is a number calculated by Shor Algorithm. The enormous quantity of size 2042 pieces can be reduced to a single number [5]. The total time consumed by the old-style computing device can be factored out over a long period of time. However, utilizing quantum peculiarity can be separated in a matter of minutes or less.

2. Software Security Factors and Quantum Computing Alternatives

Software security is a major concern in the field of information technology. The rapid progress in Quantum computing technology will require inventive and highly efficacious approaches in software security. The encryption and decryption methods can easily be matched by the qubits combination at the same time. The security assessment is the need of time. We selected the factors of software security and the different quantum-enabled security approach for evaluating software security. The hierarchy of software security is shown in figure 1.

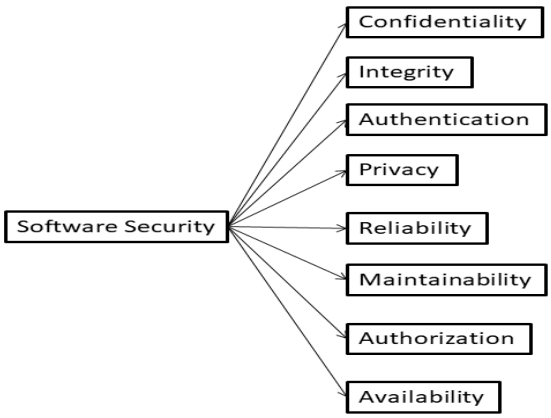

Figure 1. Hierarchy of Software Security

A. Factors

Confidentiality [C1] The term confidentiality refers to enforcing agreed-upon restrictions on access and disclosure and protecting individual privacy and proprietary information [4].

Integrity [C2] the term software integrity refers to the source code of a product. Furthermore, software quality is critical since it determines how safe, secure, and solid the software is. Here, we'll look at what software uprightness is, why it's vital, and how the correct gadgets can help you improve your product's respectability [6].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0030.v1

Authentication [C3] the most prevalent method of assessing a client's character is authentication. It is a partner's instrument for approaching a solicitation with a number of distinct conditions. The authentication provided is compared to those on a document in a data set of the permitted client's data on a nearby working framework or within a verification server [7].

Privacy [C4] Software security is created with the goal of ensuring the safety of its users. The product is typically used in connection with Internet usage to regulate or limit the amount of data made available to outsiders. The software can do several types of encryption and sorting [8].

Reliability [C5] the reliability quality is to be anticipated for the testing stage or activity stage, different measures ought to be utilized. Reliability quality idea will prompt different dependability values got, and it will additionally prompt different dependability-based choices made [9].

Maintainability [C6] the degree to which an application is perceived, fixed, or improved is referred to as software maintainability. Software maintainability is critical because it accounts for around 75% of a project's cost! Finding strategies to estimate this important variable reduces designer effort, lowers costs, and increases assets. Understanding software maintainability allows organizations to identify areas for improvement and determine the value given by present applications or during development adjustments [10].

Authorization [C7] the most typical method of granting a client or machine access credentials is through software authorization. Normally, approval is accomplished using a code generated by client computers and recognized by the server. The administrator can also use the server-client to approve or set permissions for certain clients or workstations [11].

Availability [C8] Availability refers to the fact that software is always present and ready to perform its task when needed. This broad perspective includes what is commonly referred to as reliability, as well as additional considerations such as margin time due to intermittent upkeep. In reality, accessibility broadens the concept of dependability by including the idea of recovery — that is, when the system breaks, it automatically repairs itself. Fixing can be accomplished in a variety of ways [12].

B. Alternatives

Diffie-Hellman key-exchange algorithm [A1]- [13] is a protected calculation that offers elite execution, permitting two systems to trade a common worth without utilizing information encryption freely. The traded keying material that is shared by the two systems can be founded on 768, 1024, or 2048 pieces of keying material, known as Diffie-Hellman bunches 1, 2, and 2048, separately. For assurance against man-in-the-center security threats, characters are validated later the Diffie-Hellman trade happens. Diffie Hellman algorithm is a symmetric cryptographic method for the transmission of secure data [14]. An evident imperfection has forever been the trouble in offering the imperative encryption key to the recipient of the message. It can catch any hacker sent over an uncertain channel by programmers, who can then utilize a similar key to decode the scrambled cipher texts. In this kind of SSA, the Diffie Hellman algorithm has the property to solve the hacking problem of keys by using a one-way function. The communication between the sender and receiver only decrypts the message by the secure key. One-way function follows a sort of calculation where you can compute a result for information [15]. Notwithstanding, it is hypothetically difficult to get the individual contribution from an arbitrary outcome. Diffie-Hellman key transfer method helps us to find arbitrary outcome.

Quantum key distribution algorithm [A2]-Quantum Key Distribution (QKD) algorithm has a bidirectional quantum channel for communication. The first QKD is BB84 is given by Charles Bennett and Gilles Brassard [16]. The QKD methods send data more than once between the users, and they will compute the quantum bit error rate. The algorithms have ten steps, and every step has twenty rounds. After the repeated rounds, the shifting

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0030.v1

of key processes is applied in QKD between the users [17]. To secure the software, web application, network, etc., several protocols are created sequentially with the same or different mechanism against the well-known quantum attack. In QKD depends on three algorithms BB84, B92, and EPR [18]. Quantum cryptography is guaranteed by the law of physics demonstrated by the non-cloning theory that supports the secure key unconditionally and detects eavesdropping on the quantum-based communication channel.

Deutsch-Jozsa Algorithm [A3]-Deutsch-Jozsa Algorithm [19], let us consider the function $f: \{0,1\}^n \rightarrow \{0,1\}$ accepts the n sequence of 0's and 1's and outputs as a 0 or 1. The domain of the function might be 2^{n-1} [20]. The function is called the *balance* when half of the input is 0, and the other half is 1. The function is called constant when all the input is 0 or 1. The Deutsch-Jozsa algorithm resolved the accompanying issue: assume that function which we can assess yet can't see the manner in which it is characterized [21]. Here, we are guaranteed that the function is either balanced/adjusted for constant/steady; let us decide if the function is adjusted or then again consistent. Traditionally, this calculation can be addressed by assessing the function of various inputs. In the best case, when we realize that precisely two distinct data sources give two unique yields, we can guarantee that the function is adjusted. Interestingly, to guarantee that the work is steady, the capacity should be assessed the capacity on the greater part of the potential information sources [19]. Accordingly, the direct outcome imaginable requires function assessment.

Special Deutsch-Jozsa Algorithm [A4]- Special Deutsch-Jozsa Algorithm assesses the balanced and constant values of the binary bits of the function. First of all, the function is one of either balanced that is equal to 1 for exactly half of the other possible$x$ and 0 for the other half Function is constant for all values of x either 1 or 0 [22].

Grover's Algorithm [A5]-Grover's algorithm's major application is the unstructured search problem. The Grover's algorithm is fast, and working quadratic way also enhance the run time for a variety of other algorithm. The application of Grover's algorithm is beyond the search application [23]. In quantum computing, the algorithm search phenomenon can be understood by the procedure of the search problem. Let us consider a set of items which have same colour accepts one. The number of items is N, in the classical way $\frac{N}{2}$ steps are followed, and the different item can be identified or searched, in worst case all the N steps follows but in Grover's Algorithm $\sqrt{N}$ steps are follows and the item will be selected. This phenomenon provides the quadratic quantum speed up for the large classical problems. This is called the amplitude amplification method [24].

Quantum key distribution algorithm in GHZ state [A6]- Let's examine the way that the exceptional Deutsch-Jozsa algorithm can be utilized for quantum key distribution by utilizing a GHZ state [25]. We utilize function, which is of one of two sorts; either the input of the function is balanced or constant. It is confidential. Security objective is to decide with sureness whether they have picked a consistent or a fair function without information of the function. If the function is consistent, the result qubits are fully snared (GHZ state), in any case distinct state. For the security estimation, let's share one mystery bit if they decide the function by getting a reasonable estimation result. The existence of share made the entangled state fully destroyed into a separable state [26].

3. Methodology and Numerical Analysis

The FTOPSIS is a one-of-a-kind process for evaluating the rank/weight of the alternatives associated with quantum enable software security. TOPSIS divides a decision problem into several levels, each addressing a broad goal, a set of options, and a set of algorithms. The FTOPSIS speculates on this. It has been determined what software security strategy should be in the era of quantum computer. FTOPSIS was used to examine the rank/weight of the alternatives associated to the software security in the era of quantum computing.

A. Fuzzy TOPSIS Methodology

FTOPSIS is a method for evaluating the rank of alternatives, security factors and with the concerns of quantum enable security algorithm. It is based on the attributes and

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0030.v1

alternatives that are fundamentally linked to those characteristics. The FTOPSIS have philological standings, and their assessment systems are based on fuzzy numbers. As indicated in table 1, the philological ranks have a thing for fuzzy numbers.

Table 1. Fuzzy Comparison Measures (FCM).

Linguistic Terms	FCM
Equal	(1 ,1, 1)
Not Bad	(2 ,3, 4)
Good	(4,5, 6)
Very Good	(6 ,7, 8)
Perfect	(9 ,9, 9)
Weak Advantage	(1 ,2, 3)
Preferable	(3 ,4, 5)
Fairly Good	(5 ,6, 7)
Absolute	(7 ,8, 9)

From there on FTOPSIS framework is an overview of every individual substance given by the inspector. The resulting progresses are concluding the Fuzzy Comparison Measures (FCM) from the hierarchal plan. The effect of the part and its decision are with one measure to various elective standards has a pair-wise relationship of individual variable, which acknowledges a basic part altogether.

The "M" choice in the numerical mathematical mean arrangement, together with the "M" point and "N" layered area FTOPSIS system, are utilized in the multi-measures decision for locating. The foundation of the FTOPSIS methods is the possibility of the absolute and furthest division from the positive ideal preparation, unfavorable ideal solution for the ideal and least ideal plan, respectively [27]. The effectiveness of the other option and component in regard to the rules can be evaluated using the FTOPSIS approach. The tendency suggests that FTOPSIS addresses the significance of models and assigns fuzzy numbers to ensure consistency in a fuzzy environment. We choose the strategy of Fuzzified TOPSIS approach to apply the aggregate decision dynamic methodology in a fuzzy environment. The means are given under:

Stage 1: To drive the enrolment work from the three-sided fuzzy number, which disperse the yes or no rationale in many sub-values in table 1 and participation work 'μ', as displayed in condition 1.

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

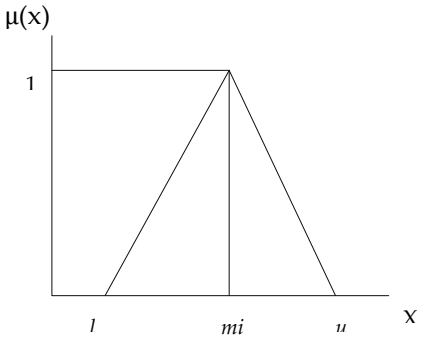

Figure 3. Fuzzy Comparison Measures

Let us consider or choose 'l' least worth, 'mi' center worth, and 'u' upper most qualities as displayed in the figure. 2.

Stage 2: In FTOPSIS, first and foremost, determine the table for the phonetic terms utilized in the influencing variables and choices from the table 1 as referenced underneath. Further, we utilized the fuzzy choice framework with the assistance of condition 2, and assessed the grid.

$$C_1 \quad \ldots\ldots \quad C_n$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0030.v1

$$\widetilde{K} = \begin{matrix} A_1 \\ \dots \\ A_m \end{matrix} \begin{bmatrix} \tilde{x}_{11} & \cdots & \tilde{x}_{1n} \\ \cdots & \ddots & \cdots \\ \tilde{x}_{m1} & \cdots & \tilde{x}_{mn} \end{bmatrix} \quad (2)$$

Here, $\tilde{x}_{ij} = \frac{1}{D}\left(\tilde{x}_{ij}^{1} \cdots \oplus \tilde{x}_{ij}^{d} \oplus \cdots \tilde{x}_{ij}^{D}\right)$, $\tilde{x}_{ij}^{d}$, is used to calculate the ranking of quantum enable security alternativeA_i, the factors C_j is evaluated by the d^{th} practitioner $\tilde{x}_{ij}^{d} = (l_{ij}^{d}, mi_{ij}^{d}, u_{ij}^{d})$.

Stage 3: The standardized fuzzy choice grids are assessed by the situation 3, addressed by ($\tilde{P}$). The standardization is determined by the situation 4.

$$\tilde{P} = \left[\tilde{p}_{ij}\right]_{m\times n} \quad (3)$$

$$\tilde{p}_{ij} = \left(\frac{l_{ij}}{u_j^+}, \frac{mi_{ij}}{u_j^+}, \frac{u_{ij}}{u_j^+}\right), u_j^+ = max\{u_{ij}, i = 1,2,3..n\} \quad (4)$$

The most expected level u_j^+ is 1 and the most exceedingly terrible is 0. The standardization cycles of FCMs are determined by the comparable advances.

Stage 4: Further, the weighted standardized fuzzy choice framework ($\tilde{Q}$) is measured by the situation 5.

$$\tilde{Q} = \left[\tilde{q}_{ij}\right]_{m\times n} i = 1,2,..m;\ j = 1,2,3 \dots n \quad (5)$$

Where, $\tilde{q}_{ij} = \tilde{p}_{ij} \otimes \tilde{w}_{ij}$

Stage 5: The fuzzy positive ideal explanation, 'A^+' and fuzzy negative ideal explanation 'A^-' are determined; awesome and most terrible arrangement, separately, by the situation 6 and 7. This should be possible by staying away from the sporadic inconvenience of estimation.

$$A^+ = \left(\tilde{q}_{1,\cdots\dots}^{*} \tilde{q}_{j,\cdots\dots}^{*} \tilde{q}_{n,}^{*}\right) \quad (6)$$

$$A^- = \left(\tilde{q}_{1,\cdots\dots}^{*} \tilde{q}_{j,\cdots\dots}^{*} \tilde{q}_{n,}^{*}\right) \quad (7)$$

The units of option are determined by the situations 8 and 9, separately.

$$\tilde{d}_i^+ = \sum_{j=1}^{n} d\left(\tilde{q}_{ij}, \tilde{q}_{ij}^{*}\right), \quad i = 1,2,..m;\ j = 1,2,3 \dots n \quad (8)$$

$$\tilde{d}_i^- = \sum_{j=1}^{n} d\left(\tilde{q}_{ij}, \tilde{q}_{ij}^{*}\right), \quad i = 1,2,..m;\ j = 1,2,3 \dots n \quad (9)$$

Stage 6: Further, to work out the Closeness Coefficient, it is addressed by '$C\tilde{C}_i$', it is characterized as the general close level of the options utilized in security of software in the era of quantum computer. It is addressed here by condition 10. The closeness coefficients decide the ideal levels of its closeness. The closeness coefficients assess the fuzzy holes level at the beginning of fuzzy closeness to recuperate the choices [28]. The units of the best and the most unbearably awful degree of choices have been determined.

$$C\tilde{C}_i = \frac{\tilde{k}_i^-}{\tilde{k}_i^+ + \tilde{k}_i^-} = 1 - \frac{\tilde{k}_i^+}{\tilde{k}_i^+ + k_i^-}, i = 1,2, \dots., m \quad (10)$$

The positions of the still up in the air by the situation 10 are utilizing the separations. Further, the computation of quantum enable security approaches and security factors are chosen options are done and the mathematical investigations are made sense of in next part of the paper.

The ranks of the alternatives are determined by the equation 10 by using the detachments. Further, the calculation of security of software in quantum era of computing perspective with the help of factors and its selected alternatives are done and the numerical analysis is explained in next section of the paper.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0030.v1

B. Data Analysis

The result of the given evaluation are tabulated in this section, the different values (linguistic terms are changed into its numerical value by the set of literature) are shown in the table given below:

Table 2. subjective cognition results of linguistic terms of factors.

C1	C2	C3	C4	C5	C6	C7	C8
1.000000	1.874000	1.476000	1.486400	0.457000	0.304100	0.226600	0.550000
1.000000	2.547000	1.678000	2.454000	0.567000	0.397000	0.276400	0.750000
1.000000	3.241000	1.957000	3.386650	0.795000	0.561700	0.357300	0.953000
	1.000000	0.615000	0.757100	0.165000	0.550000	0.304100	0.226600
-	1.000000	0.785000	0.955000	0.250000	0.750000	0.397000	0.276400
	1.000000	1.036000	1.254000	0.25000	0.953000	0.561700	0.357300
		1.000000	0.767000	0.214000	0.550000,	0.226600,	0.304100
-	-	1.000000	1.054000	0.257000	0.750000,	0.276400,	0.397000
		1.000000	1.364000	0.310700	0.953000	0.357300	0.561700
			1.000000	0.250000,	0.226600,	0.550000,	0.304100
-	-	-	1.000000	0.2354000,	0.276400,	0.750000,	0.397001
			1.000000	0.290400	0.357300	0.953000	0.561700
				1.000000,	0.226600,	0.304100,	0.550000,
-	-	-	-	1.000000,	0.276400,	0.397000,	0.750000,
				1.000000	0.357300	0.561700	0.953000
					1.000000,	0.550000,	0.226600,
-	-	-	-	-	1.000000,	0.750000,	0.276400,
					1.000000	0.953000	0.357300
						1.000000,	0.304100,
-	-	-	-	-	-	1.000000,	0.397000,
						1.000000	0.561700

Table 3. Weighted normalized fuzzy decision matrix of factors and alternatives.

	A1	A2	A3	A4	A5	A6
C1	0.7300, 2.2700, 4.2700	2.8200, 4.8200, 6.7300	2.9100, 4.8200, 6.7300	0.7300, 2.2700, 4.2700	2.8200, 4.8200, 6.7300	2.8200, 4.8200, 6.7300
C2	4.4500, 6.4500, 8.1800	1.6400, 3.3600, 5.3600	0.7300, 2.2700, 4.2700	4.4500, 6.4500, 8.1800	0.7300, 2.2700, 4.2700	2.8200, 4.8200, 6.7300
C3	2.8200, 4.8200, 6.7300	0.7300, 2.2700, 4.2700	4.4500, 6.4500, 8.1800	0.7300, 2.2700, 4.2700	2.8200, 4.8200, 6.7300	1.6400, 3.3600, 5.3600
C4	0.7300, 2.2700, 4.2700	0.7300, 2.2700, 4.2700	0.7300, 2.2700, 4.2700	4.4500, 6.4500, 8.1800	1.6400, 3.3600, 5.3600	1.0000, 2.6400, 4.6400
C5	4.4500, 6.4500, 8.1800	4.4500, 6.4500, 8.1800	4.4500, 6.4500, 8.1800	2.8200, 4.8200, 6.7300	0.7300, 2.2700, 4.2700	2.8200, 4.8200, 6.7300
C6	0.7300, 2.2700, 4.2700	0.7300, 2.2700, 4.2700	0.7300, 2.2700, 4.2700	0.7300, 2.2700, 4.2700	0.7300, 2.2700, 4.2700	2.8200, 4.8200, 6.7300
C7	4.4500, 6.4500, 8.1800	4.4500, 6.4500, 8.1800	4.4500, 6.4500, 8.1800	4.4500, 6.4500, 8.1800	4.4500, 6.4500, 8.1800	1.6400, 3.3600, 5.3600
C8	2.8200, 4.8200, 6.7300	2.8200, 4.8200, 6.7300	2.8200, 4.8200, 6.7300	2.8200, 4.8200, 6.7300	0.7300, 2.2700, 4.2700	2.8200, 4.8200, 6.7300

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0030.v1

Table 4. Weighted pairwise normalized fuzzy decision matrix.

	A1	A2	A3	A4	A5	A6
C1	0.4600, 0.6700, 0.8600	0.6100, 0.8200, 0.9800	0.4600, 0.6700, 0.8600	0.4600, 0.6700, 0.8600	0.6100, 0.8200, 0.9800	0.5200, 0.7400, 0.9200
C2	0.4600, 0.6700, 0.8600	0.4600, 0.6700, 0.8600	0.4600, 0.6700, 0.8600	0.4600, 0.6700, 0.8600	0.6100, 0.8200, 0.9800	0.4600, 0.6700, 0.8600
C3	0.3800, 0.6000, 0.8000	0.4600, 0.6700, 0.8600	0.3800, 0.6000, 0.8000	0.3800, 0.6000, 0.8000	0.4600, 0.6700, 0.8600	0.6100, 0.8200, 0.9800
C4	0.4600, 0.6700, 0.8600	0.4600, 0.6700, 0.8600	0.4600, 0.6700, 0.8600	0.6100, 0.8200, 0.9800	0.4600, 0.6700, 0.8600	0.5400, 0.7500, 0.9200
C5	0.4600, 0.6700, 0.8600	0.3800, 0.6000, 0.8000	0.3800, 0.6000, 0.8000	0.4600, 0.6700, 0.8600	0.6100, 0.8200, 0.9800	0.4600, 0.6700, 0.8600
C6	0.6100, 0.8200, 0.9800	0.4600, 0.6700, 0.8600	0.4600, 0.6700, 0.8600	0.4600, 0.6700, 0.8600	0.4600, 0.6700, 0.8600	0.6100, 0.8200, 0.9800
C7	0.6100, 0.8200, 0.9800	0.4600, 0.6700, 0.8600	0.4600, 0.6700, 0.8600	0.3800, 0.6000, 0.8000	0.3800, 0.6000, 0.8000	0.4600, 0.6700, 0.8600
C8	0.3800, 0.6000, 0.8000	0.3800, 0.6000, 0.8000	0.6100, 0.8200, 0.9800	0.4600, 0.6700, 0.8600	0.6100, 0.8200, 0.9800	0.5200, 0.7400, 0.9200

Table 5. Weighted pairwise normalized fuzzy decision matrix.

	A1	A2	A3	A4	A5	A6
C1	0.0020, 0.0100, 0.0390	0.0020, 0.0080, 0.0250	0.0020, 0.0080, 0.0250	0.0020, 0.0100, 0.0390	0.0020, 0.0100, 0.0390	0.0020, 0.0060, 0.0200
C2	0.0020, 0.0080, 0.0250	0.0020, 0.0080, 0.0250	0.0020, 0.0070, 0.0220	0.0010, 0.0040, 0.0170	0.0010, 0.0040, 0.0170	0.0030, 0.0120, 0.0420
C3	0.0020, 0.0070, 0.0220	0.0020, 0.0070, 0.0220	0.0030, 0.0120, 0.0420	0.0020, 0.0080, 0.0250	0.0020, 0.0080, 0.0250	0.0020, 0.0070, 0.0220
C4	0.0030, 0.0120, 0.0420	0.0030, 0.0120, 0.0420	0.0020, 0.0080, 0.0250	0.0020, 0.0070, 0.0220	0.0020, 0.0070, 0.0220	0.0030, 0.0120, 0.0420
C5	0.0030, 0.0120, 0.0420	0.0020, 0.0080, 0.0250	0.0020, 0.0080, 0.0250	0.0030, 0.0120, 0.0420	0.0030, 0.0120, 0.0420	0.0020, 0.0080, 0.0250
C6	0.0020, 0.0070, 0.0220	0.0030, 0.0120, 0.0420	0.0020, 0.0070, 0.0220	0.0030, 0.0120, 0.0420	0.0020, 0.0080, 0.0250	0.0020, 0.0080, 0.0250
C7	0.0020, 0.0080, 0.0250	0.0020, 0.0080, 0.0250	0.0020, 0.0080, 0.0250	0.0020, 0.0080, 0.0250	0.0020, 0.0070, 0.0220	0.0020, 0.0070, 0.0220
C8	0.0020, 0.0070, 0.0220	0.0020, 0.0070, 0.0220	0.0020, 0.0070, 0.0220	0.0020, 0.0070, 0.0220	0.0030, 0.0120, 0.0420	0.0030, 0.0120, 0.0420

Table 6. Closeness coefficient of the detachment level of the alternatives.

Alternatives	$dist^{+i}$	$dist^{-i}$	Gap Degree of CC^{+i}	Satisfaction Degree of CC^{-i}
A1	0.0515245	0.038569	0.3655859	0.62585971
A2	0.0655254	0.037589	0.5248597	0.64446598
A3	0.0475698	0.058564	0.5698569	0.44458799
A4	0.0457584	0.038697	0.2562567	0.52112533
A5	0.4518574	0.055988	0.5656599	0.46689221
A6	0.0452859	0.055857	0.6125874	0.38888923

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 October 2022 doi:10.20944/preprints202210.0030.v1

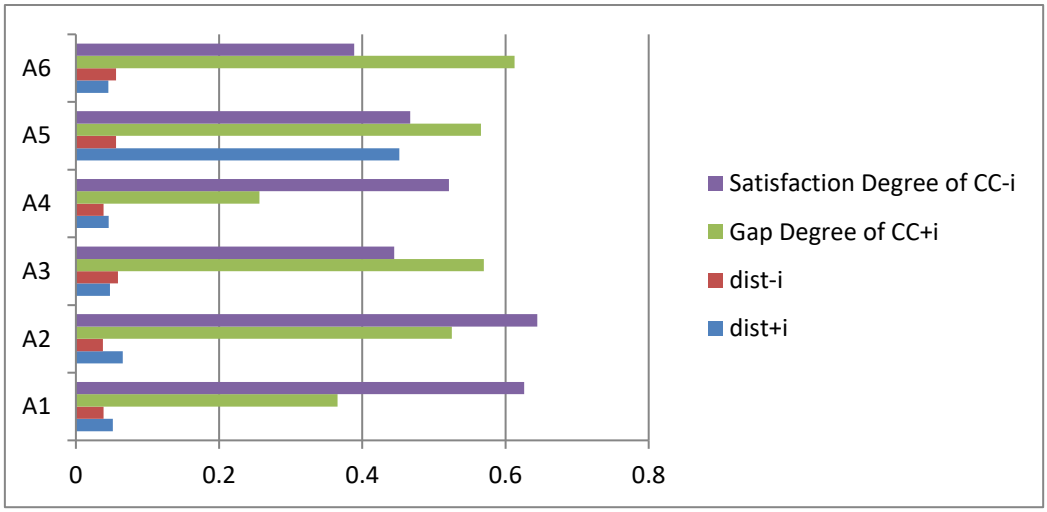

Figure 2. Closeness coefficient of the detachment level of the alternatives.

4. Result and Conclusion

The growth of Quantum Computer that is safe and trustworthy requires immediate attention from software developers, experts, and specialists. This research aims to improve the security of software in the era Quantum Computer. The technique requires the parameters for selection based on their impact on the security of software. Furthermore, according to this research, variables of appropriate security of software should be completed during the early stages of improvement. Symmetric comprehension and point-of-view evaluation are expected to fix this difficulty in the current managed security of software growth, which is becoming increasingly perplexing. We investigated this cause and made quantitative predictions about the possible long-term security of software power that may be a robust system.

Furthermore, the ideal solution to reduce the assortment issue is to take care of the maintainability of environmentally friendly power advancement underhanded nature. The proposed study will be capable of achieving the goal of security of software concerns by dealing with and looking at its many sources and expected inexact assortment. Furthermore, in the first research on the security of software, FTOPSIS procedure for practical security of software, the weight of the factors according to the alternatives are "Quantum Key Distribution" got the highest weight and "Grover's Algorithm" got the least.

Our assessment approach will aid the maker or sketcher in creating the item with adequate improvement in the movement life depiction of software security that may be maintained. The findings of this study can be used to assess reasonable development of the software and will aid decision-makers in achieving benefits and drawbacks reduction and other related plans for large-scale feasible security issues in software development, as well as providing full versatility of supportable development. FAHP philosophy indicates the importance of variables that support the development of secure software.

This investigation would aid experts in learning more about the plan for developing secure software that is manageable. Improvement guidelines might be offered over this evaluation to assist specialists in re-fining the development of success by utilizing high organized concentrations of concern. There may be a few delimits in this evaluation that should be kept in mind in future assessments. The following are the outcomes' breaking points:

- *The data gathered for security factors of the software that can be sustained is essential for progress. The outcomes may make it difficult to comprehend that the data is massive.*
- *There may be more maintainable security factors not included in this study.*

The goal is to reduce the need for assistance for a long time while maintaining secure software. Focusing on improving the thing's security of software from the start of the improvement cycle will increase the item's tremendous value. We can lessen the complex

design of computation in the future by using cross-segment-based feasible sustainable power estimation. This quantitative study assessment is based on ongoing supportable security of software, as well as future difficulties that must be considered. We have depicted future challenges and are attempting to successfully review the issues utilizing a combined strategy of multi models autonomous bearing "FAHP and FTOPSIS."

Author Contributions: The research article RA gives the concept and idea of the research, MN worked on this topic from last three year and identifying the factors and alternatives, RK and PCP helps in identification, SA gives the approach of decision making, MN works on the methodology and evaluates the result by using the questionnaire. MN works with the Specialist to identify the impact of the factors and alternatives with the help of RA.

References

[1] M. Möller and C. Vuik, "On the impact of quantum computing technology on future developments in high-performance scientific computing," *Ethics Inf. Technol.*, vol. 19, no. 4, pp. 253–269, Dec. 2017, doi: 10.1007/S10676-017-9438-0/FIGURES/2.

[2] N. B. Ruparelia, "Software development lifecycle models," *ACM SIGSOFT Softw. Eng. Notes*, vol. 35, no. 3, pp. 8–13, May 2010, doi: 10.1145/1764810.1764814.

[3] A. M. Davis, E. H. Bersoff, and E. R. Comer, "A Strategy for Comparing Alternative Software Development Life Cycle Models," *IEEE Trans. Softw. Eng.*, vol. 14, no. 10, pp. 1453–1461, 1988, doi: 10.1109/32.6190.

[4] H. Alyami *et al.*, "Analyzing the data of software security life-span: Quantum computing era," *Intell. Autom. Soft Comput.*, vol. 31, no. 2, 2022, doi: 10.32604/iasc.2022.020780.

[5] F. Tabakin, "Model dynamics for quantum computing," *Ann. Phys. (N. Y).*, vol. 383, pp. 33–78, 2017, doi: https://doi.org/10.1016/j.aop.2017.04.013.

[6] F. A. Alzahrani, M. Ahmad, M. Nadeem, R. Kumar, and R. A. Khan, "Integrity Assessment of Medical Devices for Improving Hospital Services," *Comput. Mater. Contin.*, vol. 67, no. 3, 2021, doi: 10.32604/cmc.2021.014869.

[7] M. Nadeem *et al.*, "Multi-level hesitant fuzzy based model for usable-security assessment," *Intell. Autom. Soft Comput.*, vol. 31, no. 1, 2022, doi: 10.32604/IASC.2022.019624.

[8] A. EL Azzaoui, P. K. Sharma, and J. H. Park, "Blockchain-based delegated Quantum Cloud architecture for medical big data security," *J. Netw. Comput. Appl.*, vol. 198, p. 103304, 2022, doi: https://doi.org/10.1016/j.jnca.2021.103304.

[9] R. Bose and H. T. Johnson, "Coulomb interaction energy in optical and quantum computing applications of self-assembled quantum dots," *Microelectron. Eng.*, vol. 75, no. 1, pp. 43–53, 2004, doi: https://doi.org/10.1016/j.mee.2003.11.008.

[10] S. C. Misra, "Modeling Design/Coding Factors That Drive Maintainability of Software Systems," *Softw. Qual. J. 2005 133*, vol. 13, no. 3, pp. 297–320, 2005, doi: 10.1007/S11219-005-1754-7.

[11] A. Midilli, I. Dincer, and M. Ay, "Green energy strategies for sustainable development," *Energy Policy*, vol. 34, no. 18, pp. 3623–3633, Dec. 2006, doi: 10.1016/J.ENPOL.2005.08.003.

[12] M. A. Abdullah, K. M. Muttaqi, and A. P. Agalgaonkar, "Sustainable energy system design with distributed renewable resources considering economic, environmental and uncertainty aspects," *Renew. Energy*, vol. 78, pp. 165–172, Jun. 2015, doi: 10.1016/J.RENENE.2014.12.044.

[13] N. Li, "Research on diffie-hellman key exchange protocol," *ICCET 2010 - 2010 Int. Conf. Comput. Eng. Technol. Proc.*, vol. 4, 2010, doi: 10.1109/ICCET.2010.5485276.

[14] D. Hellman, K. Exchange Algorithm Aditya Kakaraparthi, V. Karthick -Diffie-hellman Protocol on Raspberry pi Yuwen Wang, G. Mogos -, C. Kumar, and D. P. Raj Vincent M, "Enhanced diffie-hellman algorithm for reliable key exchange," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 263, no. 4, p. 042015, Nov. 2017, doi: 10.1088/1757-899X/263/4/042015.

[15] M. Rashid, H. Kumar, S. Z. Khan, I. Bahkali, A. Alhomoud, and Z. Mehmood, "Throughput/Area Optimized Architecture for Elliptic-Curve Diffie-Hellman Protocol," *Appl. Sci. 2022, Vol. 12, Page 4091*, vol. 12, no. 8, p. 4091, Apr. 2022, doi: 10.3390/APP12084091.

[16] L. Bacsardi, "Using quantum computing algorithms in future satellite communication," *Acta Astronaut.*, vol. 57, no. 2, pp. 224–229, 2005, doi: https://doi.org/10.1016/j.actaastro.2005.03.023.

[17] J. Fang *et al.*, "Improved polar-code-based efficient post-processing algorithm for quantum key distribution," *Sci. Reports 2022 121*, vol. 12, no. 1, pp. 1–11, Jun. 2022, doi: 10.1038/s41598-022-14145-6.

[18] A. Adu-Kyere, E. Nigussie, and J. Isoaho, "Quantum Key Distribution: Modeling and Simulation through BB84 Protocol Using Python3," *Sensors 2022, Vol. 22, Page 6284*, vol. 22, no. 16, p. 6284, Aug. 2022, doi: 10.3390/S22166284.

[19] K. Mishima, K. Tokumo, and K. Yamashita, "Quantum computing using molecular electronic and vibrational states," *Chem. Phys.*, vol. 343, no. 1, pp. 61–75, 2008, doi: https://doi.org/10.1016/j.chemphys.2007.10.027.

[20] K. Rycerz, J. Patrzyk, B. Patrzyk, and M. Bubak, "Teaching Quantum Computing with the QuIDE Simulator," *Procedia Comput. Sci.*, vol. 51, pp. 1724–1733, 2015, doi: https://doi.org/10.1016/j.procs.2015.05.374.

[21] J. Hooyberghs, "Deutsch-Jozsa Algorithm," *Introd. Microsoft Quantum Comput. Dev.*, pp. 233–270, 2022, doi: 10.1007/978-1-4842-7246-6_9.

[22] D. Qiu and S. Zheng, "Revisiting Deutsch-Jozsa algorithm," *Inf. Comput.*, vol. 275, p. 104605, Dec. 2020, doi: 10.1016/J.IC.2020.104605.

[23] D. Petrosyan and P. Zhang, "Quantum Attacks on Sum of Even–Mansour Construction with Linear Key Schedules," *Entropy 2022, Vol. 24, Page 153*, vol. 24, no. 2, p. 153, Jan. 2022, doi: 10.3390/E24020153.

[24] M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt, "Applying Grover's Algorithm to AES: Quantum Resource Estimates," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9606, pp. 29–43, 2016, doi: 10.1007/978-3-319-29360-8_3.

[25] K. Nagata, T. Nakamura, and A. Farouk, "Quantum Cryptography Based on the Deutsch-Jozsa Algorithm," *Int. J. Theor. Phys. 2017 569*, vol. 56, no. 9, pp. 2887–2897, Jun. 2017, doi: 10.1007/S10773-017-3456-X.

[26] S. Abidin, A. Swami, E. Ramirez-Asís, J. Alvarado-Tolentino, R. K. Maurya, and N. Hussain, "Quantum cryptography technique: A way to improve security challenges in mobile cloud computing (MCC)," *Mater. Today Proc.*, vol. 51, pp. 508–514, 2022, doi: https://doi.org/10.1016/j.matpr.2021.05.593.

[27] M. Nazim, C. Wali Mohammad, and M. Sadiq, "A comparison between fuzzy AHP and fuzzy TOPSIS methods to software requirements selection," *Alexandria Eng. J.*, vol. 61, no. 12, pp. 10851–10870, Dec. 2022, doi: 10.1016/J.AEJ.2022.04.005.

[28] G. Dwivedi, R. K. Srivastava, and S. K. Srivastava, "A generalised fuzzy TOPSIS with improved closeness coefficient," *Expert Syst. Appl.*, vol. 96, pp. 185–195, Apr. 2018, doi: 10.1016/J.ESWA.2017.11.051.