Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

Quantum Security in Cyber Risk Analysis Through Fuzzy Analytic Hierarchy Process

Mahfooz Ahmad[1], Eram Fatima[2], Ankit Shukla[3], Neeta Bhusal[3], Mazhar Khaliq[4], Alka Agrawal[*5]

[1]Department of Electronics and Communication, Integral University, Lucknow, India
[2]Department of Computer Science and Engineering, G. L. Bajaj Institute of Technology and Management, Greater Noida, India
[3]Department of Computer Science and Engineering, Shri Ramswaroop Memorial University, Lucknow, India
[4]Department of Computer Science and Information Technology, Khwaja Moinuddin Chisti Language University, Lucknow, India
[5]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, India

Received 29 Oct. 2024; Accepted 12 Dec. 2024; Available Online 31 Dec. 2024

Abstract

Quantum security is an evolving field that leverages principles of quantum physics to strengthen computing systems. Core concepts such as superposition and entanglement are foundation to this domain. However, current systems face significant challenges due to the extraordinary processing capabilities of quantum computers. As large-scale quantum computers with high qubit counts become operational, existing cybersecurity mechanisms are increasingly inadequate. This rapid advancement in quantum computing poses substantial risks to software, networks, web-based systems, and other security measures. To address these challenges, enhancing cybersecurity mechanisms is imperative. This paper explores various quantum security strategies categorized into six mechanisms (E1 to E6) and examines their effects on cybersecurity factors labeled H1 through H8. The analysis employs the Fuzzy Analytic Hierarchy Process (F-AHP) method, which assesses the relative importance of these factors based on an extensive literature review. By calculating the weight of different security aspects, the F-AHP method provides insights to prioritize critical components throughout the development cycle. The findings reveal that quantum-resistant cryptography is the most effective security measure. In contrast, digital signatures resistant to quantum errors were assigned the lowest priority, while the software system (H2) received the highest priority. These results underscore the importance of developing robust cybersecurity frameworks that align with the capabilities of quantum technology. As the field advances, it is crucial to design software, networks, and security systems that support the optimal functionality of quantum computers. Implementing quantum security mechanisms can significantly reduce vulnerabilities and mitigate the risk of cyberattacks. Over the next decade, new approaches to cybersecurity risk analysis leveraging quantum technology are expected to emerge, paving the way for enhanced cyber resilience in a quantum-powered future.

I. Introduction

Protecting Information Technology (IT) systems has become increasingly challenging as networks evolve and the world becomes more interconnected. Security experts continuously face the threat of sixth-generation cyberattacks, which are large-

Keywords: cybersecurity, quantum computing, quantum security, risk analysis

Production and hosting by NAUSS

* Corresponding Author: Alka Agrawal
Email: alkaagrawal1155@gmail.com
doi: 10.26735/FWSL8668

scale and rapidly spread across various attack vectors [1]. These attacks are more advanced than previous ones, evading traditional detection methods by targeting mobile devices, networks, and cloud services [2]. The European Association has announced a $13 million investment in new projects focused on secure communication. The Echelon intelligence-gathering system, utilized by the US, Australia, the UK, Canada, and New Zealand, will be at risk due to the protected correspondence architecture that employs quantum cryptography. Companies such as MagiQ Innovations and ID Quantique are also leveraging quantum cryptography to address challenges faced by governments, corporations, and other organizations, where preventing unauthorized data disclosure has become a critical priority [3]. This is the time to develop engineering solutions that safeguard IT infrastructures, advancing network protection as we enter this new era. Quantum security, also known as quantum cryptography, leverages the fundamental principles of quantum physics to transmit data securely and untraceably [4]. Quantum cybersecurity deals with security in the post-quantum era. The development of quantum technologies continues to accelerate exponentially. While it would take conventional supercomputers around 10,000 years to be built, Google's entirely quantum Sycamore Processor might crack security barriers in 200 seconds. Quantum computers, the existing network security architectural designs, online applications and software, banking and defence security are all inherently vulnerable [5]. Only individuals with the appropriate secret key can decrypt the data that has been encrypted and secured through cryptography. Quantum computing is one of the fastest-growing new technologies, with new discoveries and commercial applications emerging every few weeks. Advancements in quantum technology, with ideas that seemed impossible just a few months ago are quickly becoming a reality. Quantum-enabled computing strengthens Information Technology (IT) infrastructure security and reduces the risks of sophisticated cyberattacks, especially in the context of growing quantum computing capabilities. Quantum principles assist in protecting critical systems from evolving cybersecurity threats through advanced techniques. Risks associated with brute force attacks highlight research gap in system and software security, particularly in the context of advancements in quantum computing and IT infrastructure. The effectiveness of current encryption methods needs to be enhanced through the quantum techniques. The rise of computing power through the quantum principle used in computers has made brute force attacks easier for skilled attackers. On the other hand, quantum computing offers significant enhancements to encryption methods. The potential benefits of quantum technology for both industry and society are substantial. By the end of this era, practical quantum computing technology could revolutionize computing strategies across various sectors. In the next rounds of investment, quantum computing will fundamentally alter our understanding of computers and utilize encryption to safeguard overall digital economy. In critical applications, quantum-safe encryption features are essential for maintaining security.

II. Related Work

The industry, technology, and security must establish a clear plan and strategy for a future that is secure against quantum threats [6]. Even before quantum computing becomes a reality, the historical and ongoing complexities of migrating cryptographic systems may take years of reform, remediation, and strategic planning [7]. The threats to digital system security are growing more intricate and harder to detect. Quantum security offers highly scalable protection. Quantum security integrates cutting edge firewall systems to safeguard against the most advanced online threats, utilizing quantum-resistant encryption [8]. Hyper-scale organizations require integrated security mechanisms for unified management platforms, remote access VPNs, and IoT security. Quantum computers and software like quantum key distribution introduce potential security risks[9]. Certain encryption methods commonly used to protect sensitive data such as personal information, financial transactions, and military secrets could be compromised by quantum computers [5]. Classical computers cannot perform such calculations [10]. This indicates that if quantum computing becomes widely accessible, it could greatly impact traditional cybersecurity methods

[11]. The 256-bit encryption key would be nearly impossible for a standard computer to break, but a quantum computer could do it in mere seconds. As a result, any sensitive data currently protected by encryption could be vulnerable [5]. Quantum computers' ability to simulate materials and intricate processes could advance security research. If these technologies are misused, they could be employed to create more lethal weapons or execute cyberattacks on essential infrastructure, such as banks and other institutions [12]. Quantum computing presents unprecedented security risks that can't be mitigated by existing cryptography solutions, despite its immense promise to progress technology in many other sectors [13]. Researchers have made significant progress in developing quantum-resistant algorithms, including digital signatures, quantum-safe protocols, hardware, and standardization. Current research highlights the promise of scalable quantum security but overlooks the practical challenges of integrating these systems into existing IT infrastructures and decision-making processes. Security factors pose significant challenges for security experts.

The F-AHP is particularly effective in managing ambiguity and uncertainty in decision-making, an area where traditional Multi-Criteria Decision-Making (MCDM) techniques like Analytic Hierarchy Process (AHP), Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS), or VIseKriterijumska Optimizacija I Kompromisno Resenje (VIKOR) means Multicriteria Optimization and Compromise Solution, usually abate. F-AHP uses fuzzy set theory to account for human judgments that are subjective and flawed, decision-makers can employ language words instead of precise numerical values [13]–[16]. This flexibility makes pairwise comparisons more consistent and dependable.

Among MCDM approaches, F-AHP successfully balances qualitative and quantitative criteria, making it suitable for complex hierarchical settings [17]. Encouraging interval judgments reduce cognitive biases and overconfidence, improving the robustness of quantum alternatives. F-AHP is widely applicable across various domains and can be combined with other techniques for greater flexibility, making it a powerful tool for real-world decision-making challenges. Quantum computing has dual uses: it can improve sectors like healthcare and logistics while also endangering encrypted data and critical infrastructure, necessitating a balanced approach [18]. Despite progress in developing quantum-safe algorithms, little is known about how to effectively implement these technologies and ensure their adoption before quantum computing becomes widespread. The urgent need to address quantum software security emphasizes the need of doing interdisciplinary research that links theoretical advancements with practical implementation strategies for systems that are safe against quantum attacks.

Our analysis aims to bridge these gaps by exploring scalable quantum-safe encryption technologies and prioritizing feasible deployment strategies for industries vulnerable to quantum-era attacks. To address these threats, researchers are exploring how quantum computing can be applied in various sectors, including banking, healthcare, and logistics. The new encryption algorithms and security measures that can withstand quantum attacks are currently being developed.

III. Cyber Security Factors and Quantum Alternatives

The following describes the risk factors of cyber security and an overview of how risk analysis can be introduced in cybersecurity.

Lack of awareness [H1]: Employees may not be aware of the risks associated with cyber-security. Lack of knowledge about cyber-threats and how they work can lead to mistakes and negligence that are costly and harm one's image. Ignorance is a crucial element of effective phishing operations, which provide attackers access to personal information. An IBM study found that human errors, often caused by ignorance, accounts for 95% of cybersecurity breaches. Inadequate security protocols resulting from insufficient cybersecurity knowledge can lead to data breaches [9].

Errors in hardware and software configuration [H2]: It is possible that hardware and software are not configured properly. Errors in software and hardware can leave companies vulnerable to cyberattacks. Security vulnerabilities in outdated

software might be exploited by hackers. Malicious actors employ social engineering to trick individuals into giving up privileged accounts or disclosing personal information. When ransomware attacks occur, important data is encrypted and remains inaccessible until a ransom is paid. Weak or simple passwords increase the likelihood of unauthorized access to devices or accounts. Firewalls with improper configurations may elevate the risk of data breaches. Insider threats, originating within an organization, may involve workers, subcontractors, or business associates who have access to sensitive information. Ensure that all system defaults and configurations are up-to-date and set to secure settings. Adopt the principle of least privilege, granting users and systems only the permissions required to perform their duties [10].

Remote workforce [H3]: Employees may work remotely from various locations using unregulated equipment. The risk of data breaches increases when files are shared without encryption. Using personal devices for work purposes significantly raises the risk of cyberattacks [11].

Inadequate planning [H4]: 80% of cyberattacks originate from a compromised password. Employees often manage too many passwords, leading to non-compliance with password policies. Ineffective collaboration between security teams increases the risk of breaches or failed compliance audits. Conducting regular risk assessments is essential to identify and evaluate potential cybersecurity risks. Risk assessments should be performed frequently. Failure to evaluate risks and respond to compromises jeopardizes business operations. Verify that vendors critical to operations will not disrupt organizational goals or processes. A lack of adequate cybersecurity planning may exacerbate vulnerabilities [12].

Weak cybersecurity strategy [H5]: A cybersecurity strategy is a multi-layered plan to protect networks, systems, and digital assets from external and internal threats. A crucial part of a cybersecurity strategy as endpoints are often thought of as weak security sites. An established set of rules and procedures that employees must follow to protect data and resources is a plan outlining the steps a company should follow in the event of a cyberattack. Scammers continuously develop new tactics, making an adaptive cybersecurity strategy essential. Organizations may lack a strong cybersecurity plan, which increases their vulnerability [13], [14].

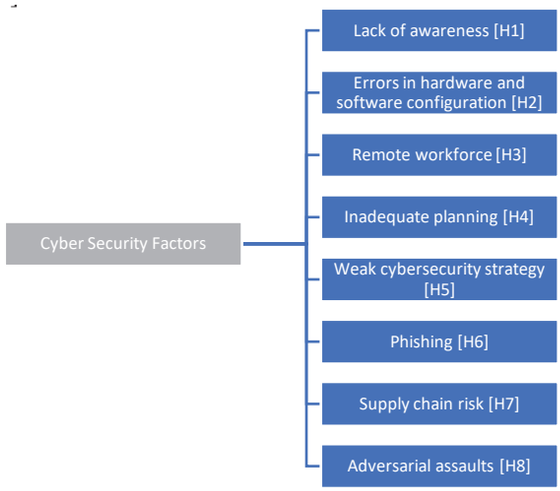


Fig. 1. Cyber security affecting factors /features

Phishing [H6]: Phishing is a type of cyberattack where victims are deceived into revealing personal information, installing malicious software, or exposing to cybercrime through fraudulent communications. Phishing is a form of social engineering. Phishers may send emails pretending to be friends, acquaintances, or trustworthy companies. These emails may contain links to phishing websites. Phishers may also use SMS or phone calls to impersonate trusted entities and coerce victims into sharing sensitive data. Fake websites created by phishers often mimic legitimate ones but aim to harvest personal information. Fake websites created by phishers often mimic legitimate ones but aim to harvest personal information. Phishing remains one of the most prevalent and significant cybersecurity challenges [15].

Supply chain risk [H7]: In cybersecurity, supply chain risk refers to the potential compromise of an item or service within a supply chain due to cyberattacks. This includes risks associated with production, distribution, manufacturing, or maintenance of products or services. Through the supply chain, attackers can gain unauthorized access to systems and disrupt business operations [13], [16].

Adversarial assaults [H8]: Adversarial assaults involve cyberattacks that manipulate machine learn-

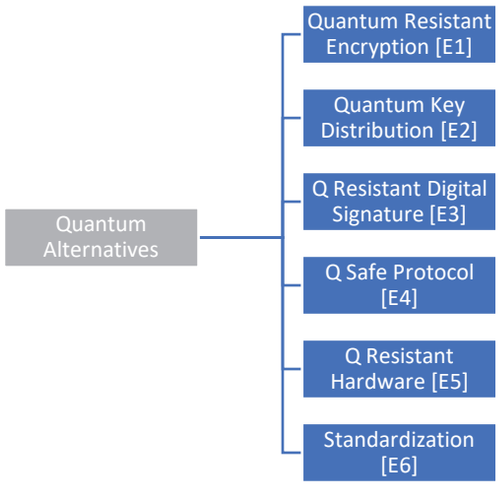


Fig. 2. Selected quantum computing enable attribute of security

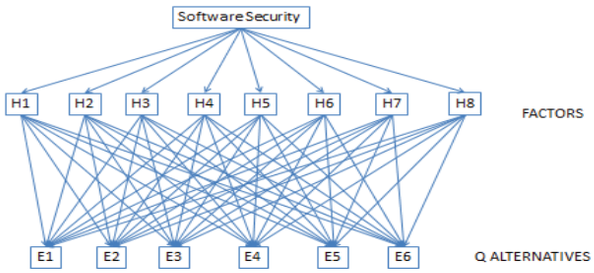


Fig. 3. Hierarchy diagram of cyber security factors and quantum alternatives

ing models to produce incorrect or unexpected outcomes. These attacks target AI systems by altering input data or the underlying models. Machine learning algorithms are particularly vulnerable to minor changes in input data, which adversaries exploit to deceive the system. Hackers and spammers may obfuscate malware and spam text to evade detection mechanisms. Adversarial assaults can lead to delayed detection of attacks, erroneous decisions, financial losses, and even fatalities. These attacks pose a significant threat to the security and reliability of Artificial Intelligence (AI) systems [17].

Quantum Alternatives

To ensure the safety of data and information against potential cyber-attacks, it is essential to address various cybersecurity challenges. Key factors to consider when designing and implementing secure projects include normalization, quantum-safe encryption, quantum key distribution, digital signatures, standards, and hardware. Quantum security concerns are vital for safeguarding data and information against the threats posed by quantum computers. Here are some key aspects to consider:

[E1] The capability to resist quantum cryptanalysis is crucial, as traditional encryption methods can be easily compromised by quantum computers [12]. Research and testing are underway for post-quantum cryptography and other encryption techniques that can withstand quantum attacks [19].

[E2] Quantum key distribution is a secure communication method that guarantees the integrity and confidentiality of the encryption key by leveraging principles of quantum physics [20]. Because quantum physics governs the distribution of these keys, they cannot be intercepted without detection [21].

[E3] Digital signatures, which are designed to resist quantum attacks, are used to verify and authenticate data [22]. One type of digital signature system that is currently being developed to prevent quantum assaults is hash-based digital signatures [23].

[E4] Quantum computers pose a risk to secure communication protocols, such as the Transport Layer Security (TLS) protocol [24]. To combat these threats, quantum-safe protocols, including the Quantum-Safe TLS protocol, are being developed [25].

[E5] Efforts are underway to develop quantum-resistant hardware, such as quantum random number generators and quantum-resistant smart cards [26], offering a secure foundation for cryptographic algorithms that resist quantum assaults [3].

[E6] It is essential to standardize quantum-resistant cryptographic algorithms and protocols to ensure interoperability and facilitate widespread adoption of these security measures [19] [27].

IV. Methodology (Fuzzy AHP)

The F-AHP is an enhancement of the analytic hierarchy process that incorporates uncertainty or imprecise data into decision-making. It was developed by Thomas L. Saaty in the 1970s [22]–[24].

AHP is a structured decision-making framework based on pairwise evaluations of criteria and alternatives [28]. F-AHP builds on this framework by introducing fuzzy sets, which allow for the representation of uncertainty in the decision-making process.

The first step in the F-AHP process involves establishing a set of options and criteria, followed by pairwise comparisons. These comparisons use a numerical scale from 1 (equal importance) to 9 (extremely important), similar to the standard AHP [25], [26]. However, instead of relying solely on precise numerical values to express the importance of each criterion, F-AHP employs fuzzy numbers or linguistic variables [29]. Fuzzy sets, each element indicates a degree of membership in the set, are utilized to manage these fuzzy values. The F-AHP approach determines the weights of the criteria and alternatives by applying a series of mathematical operations to the fuzzy sets after the pairwise comparisons [13]. F-AHP has been applied in several fields, such as design, finance, and environmental management, where decision-making often involves imprecise data [30]. However, it has a number of drawbacks, including the potential for subjectivity when interpreting fuzzy sets and the requirement for specialized knowledge to do pairwise comparisons [31], [32]. After converting linguistic values to numerical values from the TABLE I, assess each criterion in the hierarchy in light of the others by conducting pairwise comparisons. These fuzzy numbers can be represented by trapezoidal or triangular membership functions [33] as shown in Fig. 4.

This involves several mathematical techniques, including normalization, defuzzification, and aggregation from equations 1 to 17. Pairwise comparison and weight calculation for the alternatives using the established criterion weights as the basis for comparison [34]. Assign a score to each option to obtain weighted scores that will aid in ranking the alternatives by applying the criterion weights and comparing the alternative loads. To assess the reliability of the results, input values are altered, and their impact on the outcomes is observed. Sensitivity analysis is conducted to validate the results of the analysis. The F-AHP technique offers a sys-

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

$$\mu_a(x) = \{\frac{x}{cf-l} - \frac{l}{cf-l} x \in [l, cf] \frac{x}{cf-mb} - \frac{mb}{cf-mb} x \in [cf, mb] \quad (2)$$

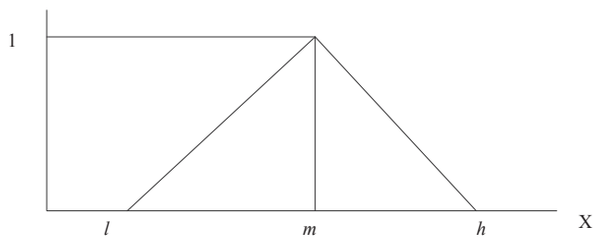


Fig. 4. Triangular Fuzzy Numbers

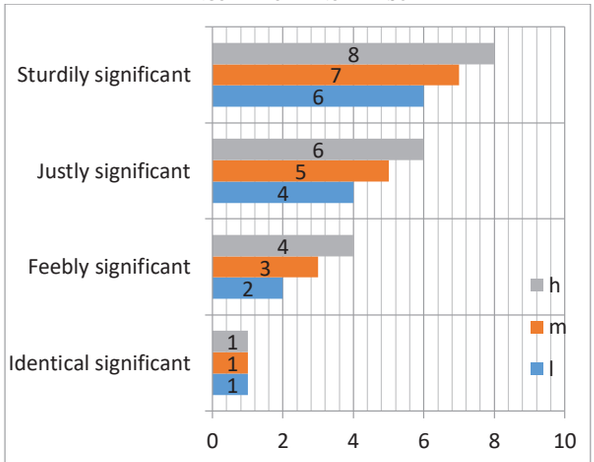
tematic approach to incorporating uncertainty and fuzzy logic into decision-making while maintaining a strong mathematical foundation [35].

The F-AHP approach is designed to address decision-making challenges effectively. The problem is first organized into a tree structure, as illustrated in Fig. 4. This structure is developed based on expert insights. A Triangular Fuzzy Number (TFN) [36], [37] is then established within a hierarchical framework. Given that multiple criteria can be influenced by a single norm, analyzing the range of any set of prioritized objectives becomes essential. The study utilized the TFN, which ranges from 0 to 1. This choice was made due to the computational simplicity of TFN and its ability to manage ambiguous data. It is often referred to as TFN if equation (1-2) can be applied to assess the participation capabilities of a fuzzy number P on Q.

The maximum breaking point, center farthest point, and lower limit are denoted by the letters l, m, and h, respectively, in the TFN shown in Fig. 3. TABLE I lists the values for the Saaty Scale [19], which divides the analysis's initial value into three groups: lower, middle, and upper [15], [17], [38]–[40]. The numerical values of the TFN are converted into l, m, and h using equations 3, 4, 5, and 6. In the two-dimensional matrix, the rows and columns are represented by the letters "i" and "j." Additionally, it is assumed that TFN is:

Equations 7, 8, and 9 are used to derive the back-consolidated TFN values. Let *M1 = (l1, m1, h1)* and *M2 = (l2, m2, h2)* be two TFNs. The prerequisites for these operations have been defined. After determining the TFN values for each pair of

TABLE I
TRIANGULAR FUZZY NUMBER SCALE



	Identical significant	Feebly significant	Justly significant	Sturdily significant
h	1	4	6	8
m	1	3	5	7
l	1	2	4	6

$$\Phi_{ij} = (l_{ij}, \mathrm{m}_{ij}, h_{ij}) \quad (3)$$

where $l_{ij} \leq m_{ij} \leq h_{ij}$

$$l_{ij} = cfn(J_{ijd}) \quad (4)$$

$$m_{ij} = (J_{ij1}, J_{ij2}, J_{ij3})^{\frac{1}{x}} \quad (5)$$

And $h_{ij} = max(J_{ijd})$ (6)

$$(l_1, m_1, h_1) + (l_2, m_2, h_2) = (l_1 + l_2, \mathrm{m} + m_2, \mathrm{h} + h_2) \quad (7)$$

$$(l_1, m, h_1) \times (l_2, m_2, h_2) = (l_1 \times l_2, m_1 \times m_2, h_1 \times h_2) \quad (8)$$

$$(l_1, m_1, h_1)^{-1} = \left(\frac{1}{h_1}, \frac{1}{m_1}, \frac{1}{l_1}\right) \quad (9)$$

$$\widetilde{A^d} = \left[\tilde{k}^d_{11}\tilde{k}^d_{12} \ldots . \tilde{k}^d_{1n}\tilde{k}^d_{21}\tilde{k}^d_{22} \ldots . \tilde{k}^d_{2n} \cdots \cdots \cdots \tilde{k}^d_{n1}\tilde{k}^d_{n2} \ldots \tilde{k}^d_{nn}\right] \quad (10)$$

$$\tilde{k}_{ij} = \sum_{d=1}^{d} \tilde{k}^{\mathrm{d}}_{\mathrm{ij}} \quad (11)$$

$$\tilde{A} = [\widetilde{k_{11}} \ \ldots \ \widetilde{k_{1n}} \cdots \ddots \cdots \widetilde{k_{n1}} \cdots \tilde{k}_{nn}\ ] \quad (12)$$

$$\tilde{p}_i = \left(\prod_{j=1}^{n} \tilde{k}_{\mathrm{ij}}\right)^{\frac{1}{n}}, i = 1,2,3 \ldots \mathrm{n} \quad (13)$$

$$\widetilde{w}_i = \tilde{p}_i \otimes (\tilde{p}_1 \oplus \tilde{p}_2 \oplus \tilde{p}_3 \ldots . \oplus \tilde{p}_n)^{-1} \quad (14)$$

$$M_i = \frac{\widetilde{w}_1 \oplus \widetilde{w}_2 \ldots . \oplus \widetilde{w}_n}{n} \quad (15)$$

$$Nr_i = \frac{M_i}{M_1 \oplus M_2 \oplus \ldots \ldots \oplus M_n} \quad (16)$$

$$BNPwD1 = \frac{[(uw1 - lw1) + (miw1 - lw1)]}{3} + lw1 \quad (17)$$

comparisons, a fuzzy span correlation framework is generated as n X n lattice using Equation 10. All span connection structures along the hierarchy chain are based on the middle value of preferences, which is determined by Equations 11 and 12. Equation 13 calculates the fuzzy geometric mean and fuzzy weights for each factor using the geometric mean technique. The normal and standardized weight conditions are applied using Equations 14, 15, and 16. The most accurate evaluation of the non-fuzzy performance of the fuzzy weights is provided by the center-of-area technique in Equation 17. The equations and fuzzy set theory have been used to address uncertainty and imprecision in criteria weighting and pairwise comparisons. The facilitation and computation of fuzzy consistency ratios involve the aggregation of fuzzy preferences and the derivation of priority weights, providing a more reliable and accurate representation of complex decision problems. F-AHP leverages these equations to support hierarchical problem structures, enhance the robustness of decision outcomes, and offer a systematic approach to addressing ambiguity. F-AHP is a valuable tool for real-world multi-criteria decision-making scenarios.

V. Numerical Data Analysis

The F-AHP is a valuable approach for tackling complex decision-making problems. This method decomposes the problem into a tree structure for enhanced clarity. Fig. 3 illustrates the hierarchical structure or geometry of the available criteria. This form of connection is based on expert opinions. In the next step, a hierarchical framework is established to develop the Triangular Fuzzy Numbers (TFN). Since a single standard can influence multiple criteria, evaluating the range of any set of prioritized objectives is essential. Currently, linguistic characteristics are being transformed into TFNs and converted into numerical values. This decision was made due to the computational simplicity of TFNs. A fuzzy number is classified as TFN if its participation capabilities meet the specified criteria. TABLE II presents the aggregated pairwise comparison matrix, TABLE III lists the weights of the factors, and TABLE IV shows the closeness coefficient of the evaluated results through F-AHP. The degree of closeness is represented by the graph in Fig. 5.

VI. Comparison

The techniques AHP and F-AHP are the consistent quality and expertise of the procedure, as the same information can be presented in different

TABLE II
AGGREGATED PAIRWISE MATRIX

	H1	H2	H3	H4	H5	H6	H7	H8
H1	1.00, 1.00, 1.00,	0.90, 1.10, 1.40	1.20, 1.50, 1.70	0.90, 1.00, 1.10	2.10, 2.90, 3.80	1.10, 1.30, 1.60	2.10, 2.90, 3.80	0.90, 1.10, 1.40
H2	0.70, 0.90, 1.10	1.00, 1.00, 1.00,	1.10, 1.60, 1.90	1.80, 1.90, 2.10	2.70, 3.40, 4.00	2.10, 2.70, 3.20	2.70, 3.40, 4.00	1.00, 1.00, 1.00,
H3	0.60, 0.70, 0.80	0.50, 0.60, 0.90	1.00, 1.00, 1.00,	1.40, 1.60, 1.90	1.70, 2.20, 2.90	1.70, 2.10, 2.60	1.70, 2.20, 2.90	0.50, 0.60, 0.90
H4	0.90, 1.00, 1.20	0.50, 0.55, 0.60	0.50, 0.60, 0.70	1.00, 1.00, 1.00,	1.90, 2.50, 2.70	1.60, 2.50, 2.60	1.90, 2.50, 2.70	0.50, 0.55, 0.60
H5	0.30, 0.30, 0.50	0.30, 0.35, 0.40	0.30, 0.50, 0.70	0.30, 0.40, 0.50	1.00, 1.00, 1.00,	1.00, 1.10, 1.30	1.00, 1.00, 1.00,	0.30, 0.35, 0.40
H6	0.70, 0.80, 1.00	0.30, 0.40, 0.50	0.40, 0.50, 0.60	0.40, 0.50, 0.60	0.80, 0.90, 1.10	1.00, 1.00, 1.00,	0.80, 0.90, 1.10	0.30, 0.40, 0.50
H7	2.10, 2.90, 3.80	2.70, 3.40, 4.00	1.70, 2.20, 2.90	1.90, 2.50, 2.70	1.00, 1.00, 1.00,	0.80, 0.90, 1.10	1.00, 1.00, 1.00,	2.70, 3.40, 4.00
H8	0.90, 1.10, 1.40	1.00, 1.00, 1.00,	0.50, 0.60, 0.90	0.50, 0.55, 0.60	0.50, 0.55, 0.60	0.30, 0.35, 0.40	0.30, 0.40, 0.50	1.00, 1.00, 1.00,

TABLE III
WEIGHTS OF THE FACTORS

Factors	Weights	BNP	Rank
H1	0.15,0.18,0.21	1/6	2
H2	0.19,0.20,0.22	1/5	1
H3	0.13,0.16,0.19	1/7	4
H4	0.12,0.15,0.18	1/6	3
H5	0.06,0.08,0.10	0	8
H6	0.07,0.09,0.13	0	6
H7	0.13 ,0.10 ,0.08	0	5
H8	0.12 ,0.08 ,0.05	0	7

TABLE IV
CLOSENESS COEFFICIENT

Alternatives	+d	-d	Satisfaction degree of CCi
E1	2/9	1/2	1/3
E2	4/5	1	2/9
E3	1/4	1/2	1/3
E4	1/3	1/2	2/5
E5	4/9	3/5	2/5
E6	2/7	1/3	1/2

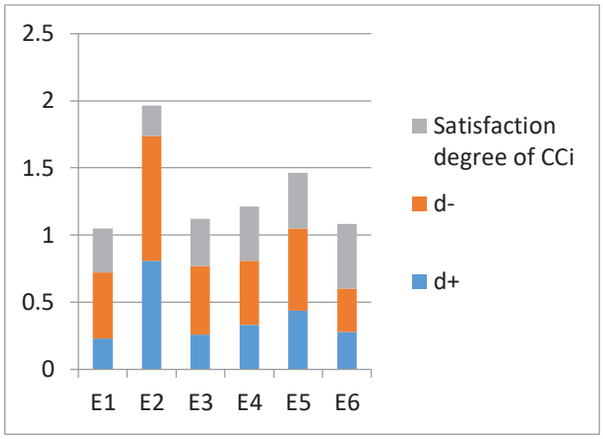


Fig. 5. Graphical representation of the degree of closeness

ways [20]. The F-AHP approach aims to assess the effectiveness and accuracy of the generated results. The data collection and estimation methods for AHP are similar to those of F-AHP, with the key difference being the absence of Fuzzification in Classical-AHP, which uses real number values.

TABLE V
COMPARISON OF ALTERNATIVE WITH CLASSICAL-AHP

Methods/Alternatives	E1	E2	E3	E4	E5	E6
Fuzzy-AHP	207/625	139/625	141/400	118/291	158/381	289/596
Classical-AHP	14/43	89/400	73/205	28/69	357/859	325/669

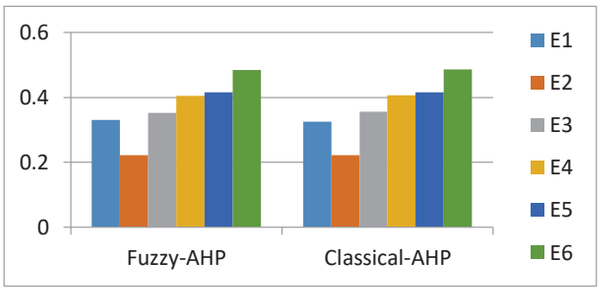


Fig. 6. Comparative bar graph of alternative between Fuzzy and Classical AHP

The results from both regular AHP and F-AHP are displayed separately in the table. There is a notably high Pearson correlation value (0.99171600) between the outcomes of the F-AHP methodology and the Classical-AHP strategy as shown in TABLE V and Fig. 6. F-AHP proves to be more efficient than the classical AHP method, offering enhanced productivity and reliability.

VII. SENSITIVITY ANALYSIS

Sensitivity analysis is conducted to validate the results for each variable. This study focuses on the weights assigned to the variables. Multiple trials are performed for each factor in our estimation using quantum alternatives to ensure the validity of the sensitivity analysis. The results of these tests are presented in TABLE VI. The closeness coefficient (CC-I) is calculated based on the security factor weights, which range from H1 to H8. The CC-I is determined using the F-AHP method to compute the component weights. The initial weights are displayed in the first row of TABLE VI and illustrated in Fig. 7. Among the quantum alternatives, E6 had the highest weight in the initial results, despite the fact that there are at least eight quantum alternatives ranging from E1 to E6. To evaluate the satisfaction level of CC-I, eight trials were conducted. H7 demonstrated the highest satisfaction level with quantum alternative E6. Across all tests, E2 required the least amount of effort. According to conflicting studies, the evaluations of alternatives are significantly influenced by these weights.

VIII. RESULTS

The F-AHP approach to cybersecurity assessment is a critical procedure for verifying quantum alternatives in cybersecurity. We discussed the

TABLE VI
SENSITIVITY ANALYSIS

Experiments	Weights/Alternatives	E1	E2	E3	E4	E5	E6
Exp-0	Original Weights	207/625	139/625	141/400	118/291	158/381	289/596
Exp-1	H1	291/826	19/80	29/79	91/216	98/233	67/135
Exp-2	H2	33/100	91/400	108/305	184/449	400/973	59/119
Exp-3	H3	1/3	111/500	13/36	170/421	37/91	477/965
Exp-4	H4	37/108	36/809	337/967	297/754	200/481	33/68
Exp-5	H5	24/79	94/495	169/536	92/243	351/938	446/977
Exp-6	H6	148/577	72/511	254/939	284/847	79/241	258/625
Exp-7	H7	256/735	59/259	49/136	164/383	52/125	167/333
Exp-8	H8	256/769	211/881	294/821	12/29	277/655	304/625

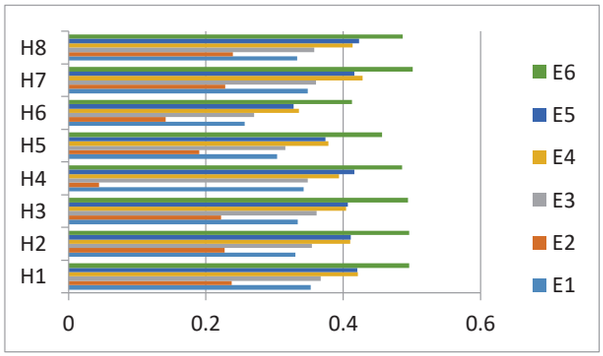


Fig. 7. Graphical representation of sensitivity analysis of quantum alternatives

challenges associated with cybersecurity, emphasizing the need for a solid foundation to establish a secure framework. Developers, engineers, and network and software systems that are both secure and viable are now essential requirements for this period. This analysis focuses on a multi-level structure to highlight the key components and contributing factors of cybersecurity. Their varied nature and functionality are progressively evolving as their applications become increasingly sought after. As security assessments grow exponentially, developers also need to ensure cybersecurity supportability. The most effective method for achieving realistic security is to estimate and evaluate cybersecurity. This exploratory analytical approach produces security in the same way as practical software approaches and examines reasonable security in connection to the factors and alternatives. The conclusions of this analysis will help security experts better balance adequate security with the development of cybersecurity mechanisms. We examined eight cybersecurity options based on expert opinion data, focusing on specific security features, moderation, and the organizations involved.

- Cybersecurity assessment will help developers address significant security issues by planning mitigation strategies and other related actions, ultimately enhancing cybersecurity.
- Experts will use F-AHP quantitative outcomes to classify cybersecurity components that rank higher in the hierarchy.
- The security variables related to risk, as shown in TABLE III and derived using the F-AHP technique, indicate that H2 received the highest weight in our quantitative evaluation, while H5 received the lowest.
- Comparing F-AHP with standard AHP reveals more effective approaches.
- Sensitivity analysis assesses user satisfaction with cybersecurity.

This evaluation will provide engineers with a clearer understanding of the security framework. Engineers may receive guidance during this assessment to help them refine the security framework while working with the specific structured elements involved. Some of the weaknesses identified in this estimate could be addressed in future research. The limitations of the results are as follows:

- The data gathered for cybersecurity is valuable despite its limitations.
- There could be additional security configuration parameters beyond those discussed in this study; an abundance of information could lead to varying outcomes.

The results of the F-AHP approach to cybersecurity assessment demonstrate its significance for evaluating and prioritizing security choices. This research develops a systematic methodology to identify critical components and factors influencing secure systems and quantum alternatives for security. The approach provides valuable information for risk reduction and framework enhancement by allowing developers and engineers to objectively assess security aspects.

It identifies H2 as the most critical security element and demonstrates that F-AHP is superior to traditional AHP. Additionally, sensitivity analysis facilitates the validation of results. Despite the limited scope of the data, the findings offer valuable guidance for enhancing cybersecurity defenses and informing future research.

IX. Conclusions

The cybersecurity assignments leverage insights from various experts who were consulted about the specific product's security features, strategies, and underlying support. F-AHP is employed to incorporate the expertise gained through the master's program. The intricate research frame-

work of quantum security references cybersecurity assessment and development.

This analysis explores cybersecurity factors and their relationships with alternatives by analyzing a diverse group of cyber developers worldwide who utilize different security metrics. Our research supports engineers and developers in enhancing systems by effectively integrating quantum technology to address cyber threats. While many evaluation models and strategies are available for independently assessing security, models and procedures that integrate security within the F-AHP framework are far less accessible.

This study examined various cybersecurity challenges across multiple domains in the context of quantum computing. The industrial collaboration will also help in to the development of quantum cyber security frameworks. It also explored numerous security measures designed to counter potential quantum attacks. Countermeasures serve as essential defences against these security threats. Additionally, this research introduces a novel AHP approach that forms the basis of a new strategy specifically tailored for cybersecurity. This system employs the F-AHP method to identify distinct security threats. In the realm of quantum computing, the comprehensive security measure is referred to as the quantum security alternative. The findings of this study will aid software developers in addressing the identified risks during the cybersecurity process.

Conflict of Interest

Authors declare that they have no conflict of interest.

Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

[1] R. Montasari and R. Hill, "Next-Generation Digital Forensics: Challenges and Future Paradigms," *Proc. 12th Int. Conf. Glob. Secur. Saf. Sustain. ICGS3 2019*, Apr. 2019, doi: 10.1109/ICGS3.2019.8688020.

[2] C. R.-I. J. of S. Home and undefined 2015, "IoT-based intelligent for fire emergency response systems," *iot.gen.tr*, vol. 9, no. 3, pp. 161–168, 2015, doi: 10.14257/ijsh.2015.9.3.15.

[3] P. Kurariya, A. Bhargava, S. Sailada, N. Subramanian, J. Bodhankar, and A. Kumar, "Experimentation on Usage of PQC Algorithms for eSign," *2022 IEEE Int. Conf. Public Key Infrastruct. its Appl. PKIA 2022*, 2022, doi: 10.1109/PKIA56009.2022.9952354.

[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. Arute et al., "Quantum supremacy using a programmable superconducting processor," *Nat. 2019 5747779,* vol. 574, no. 7779, pp. 505–510, Oct. 2019, doi: 10.1038/s41586-019-1666-5.

[6] A. M. Perumal and E. R. S. Nadar, "Architectural framework and simulation of quantum key optimization techniques in healthcare networks for data security," *J. Ambient Intell. Humaniz. Comput.,* vol. 12, no. 7, pp. 7173–7180, Jul. 2021, doi: 10.1007/S12652-020-02393-1.

[7] S. H. Almotiri, M. Nadeem, M. A. Al Ghamdi, and R. A. Khan, "Analytic Review of Healthcare Software by Using Quantum Computing Security Techniques," *Int. J. Fuzzy Log. Intell. Syst.,* vol. 23, no. 3, pp. 336–352, Sep. 2023, doi: 10.5391/IJFIS.2023.23.3.336.

[8] J. Howe, A. Khalid, C. Rafferty, F. Regazzoni, and M. O'Neill, "On Practical Discrete Gaussian Samplers for Lattice-Based Cryptography," *IEEE Trans. Comput.*, vol. 67, no. 3, pp. 322–334, Mar. 2018, doi: 10.1109/TC.2016.2642962.

[9] H. K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.,* vol. 108, no. 13, Mar. 2012, doi: 10.1103/PHYSREVLETT.108.130503.

[10] L. Zhao, "Privacy-Preserving Distributed Analytics in Fog-Enabled IoT Systems," *Sensors*, vol. 20, no. 21, 2020, doi: 10.3390/s20216153.

[11] D. Rosch-Grace and J. Straub, "Analysis of the likelihood of quantum computing proliferation," *Technol. Soc.,* vol. 68, p. 101880, Feb. 2022, doi: 10.1016/J.TECHSOC.2022.101880.

[12] F. Kirmani, B. J. Lane, and J. R. Rose, "Exploring Machine Learning Techniques to Improve Peptide Identification," in *2019 IEEE 19th International Conference on Bioinformatics and Bioengineering (BIBE)*, 2019, pp.

66–71, doi: 10.1109/BIBE.2019.00021.

[13] M. Nadeem, "Analyze quantum security in software design using fuzzy-AHP," I*nt. J. Inf. Technol.,* 2024, doi: 10.1007/s41870-024-02002-w.

[14] M. Alenezi, R. Kumar, A. Agrawal, and R. A. Khan, "ICIC Express Letters ICIC International ©2019 ISSN," vol. 13, no. 6, pp. 453–460, 2019, doi: 10.24507/icicel.13.06.453.

[15] A. Alharbi et al., "Managing Software Security Risks through an Integrated Computational Method," *Intell. Autom. Soft Comput.,* vol. 28, no. 1, p. 179, Mar. 2021, doi: 10.32604/IASC.2021.016646.

[16] K. Sahu, F. A. Alzahrani, R. K. Srivastava, and R. Kumar, "Evaluating the Impact of Prediction Techniques: Software Reliability Perspective," *Comput. Mater. Contin.*, vol. 67, no. 2, p. 1471, Feb. 2021, doi: 10.32604/CMC.2021.014868.

[17] M. Alenezi, M. Nadeem, A. Agrawal, R. Kumar, and R. A. Khan, "Fuzzy multi criteria decision analysis method for assessing security design tactics for web applications," *Int. J. Intell. Eng. Syst.*, vol. 13, no. 5, 2020, doi: 10.22266/ijies2020.1031.17.

[18] Y. Keim and A. K. Mohapatra, "Cyber threat intelligence framework using advanced malware forensics," *Int. J. Inf. Technol.,* vol. 14, no. 1, pp. 521–530, 2022, doi: 10.1007/s41870-019-00280-3.

[19] J. Bos et al., "CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM," *Proc. - 3rd IEEE Eur. Symp. Secur. Privacy, EURO S P 2018*, pp. 353–367, Jul. 2018, doi: 10.1109/EUROSP.2018.00032.

[20] S. Kirmani, H. Sun, and P. Raghavan, "A Scalability and Sensitivity Study of Parallel Geometric Algorithms for Graph Partitioning," in *2018 30th International Symposium on Computer Architecture and High Performance Computing (SBAC-PAD)*, 2018, pp. 420–427, doi: 10.1109/CAHPC.2018.8645916.

[21] M. I. Garcia Cid, J. Álvaro González, L. Ortíz Martín, and D. Del Río Gómez, "Disruptive Quantum Safe Technologies," *ACM Int. Conf. Proceeding Ser.,* Aug. 2022, doi: 10.1145/3538969.3544484.

[22] S. Kirmani and P. Raghavan, "Scalable parallel graph partitioning," in *SC '13: Proceedings of the International Conference on High Performance Computing, Networking, Storage and Analysis,* 2013, pp. 1–10, doi: 10.1145/2503210.2503280.

[23] F. Cavaliere, J. Mattsson, and B. Smeets, "The security implications of quantum cryptography and quantum computing," *Netw. Secur.,* vol. 2020, no. 9, pp. 9–15, 2020, doi: https://doi.org/10.1016/S1353-4858(20)30105-7.

[24] S. Kirmani and M. Shankar, "Generating keywords by associative context with input words." Google Patents, 2022.

[25] C. Sanavio, E. Tignone, and E. Ercolessi, "Entanglement Classification via Witness Operators generated by Support Vector Machine," Jan. 2023, doi: 10.48550/arxiv.2301.06759.

[26] S. Kirmani, J. Park, and P. Raghavan, "An embedded sectioning scheme for multiprocessor topology-aware mapping of irregular applications," *Int. J. High Perform. Comput. Appl.,* vol. 31, no. 1, pp. 91–103, 2017, doi: 10.1177/1094342015597082.

[27] S. Kirmani and K. Madduri, "Spectral Graph Drawing: Building Blocks and Performance Analysis," in *2018 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)*, 2018, pp. 269–277, doi: 10.1109/IPDPSW.2018.00053.

[28] R. V. Rao and B. K. Patel, "Decision making in the manufacturing environment using an improved PROMETHEE method," *https://doi.org/10.1080/00207540903049415*, vol. 48, no. 16, pp. 4665–4682, Jan. 2009, doi: 10.1080/00207540903049415.

[29] 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.

[30] G. Candan, "Efficiency and performance analysis of economics research using hesitant fuzzy AHP and OCRA methods," *Scientometrics,* vol. 124, no. 3, pp. 2645–2659, 2020, doi: 10.1007/s11192-020-03584-5.

[31] A. F. S. S. K. A. H. S. M. N. A. A. Masood Ahmad Jehad F. Al-Amri, "Healthcare Device Security Assessment through Computational Methodology," *Comput. Syst. Sci. Eng.,* vol. 41, no. 2, pp. 811–828, 2022, doi: 10.32604/csse.2022.020097.

[32] A. Alharbi *et al.,* "Selection of data analytic techniques by using fuzzy AHP TOPSIS from a healthcare perspective," BMC Med. *Inform. Decis. Mak.,* vol. 24, no. 1, p. 240, 2024, doi: 10.1186/s12911-024-02651-8.

[33] A. Alharbi *et al.,* "A Link Analysis Algorithm for Identification of Key Hidden Services," *Comput. Mater. Contin.,* vol. 68, no. 1, 2021, doi: 10.32604/cmc.2021.016887.

[34] H. Alyami et al., "The evaluation of software security through quantum computing techniques: A durability perspective," *Appl. Sci.,* vol. 11, no. 24, 2021, doi: 10.3390/app112411784.

[35] A. Attaallah, S. Khatri, M. Nadeem, S. A. Ansar, A. K. Pandey, and A. Agrawal, "Prediction of COVID-19

pandemic spread in Kingdom of Saudi Arabia," *Comput. Syst. Sci. Eng.,* vol. 37, no. 3, 2021, doi: 10.32604/CSSE.2021.014933.

[36] S. A. Khan, M. Nadeem, A. Agrawal, R. A. Khan, and R. Kumar, "Quantitative analysis of software security through fuzzy promethee-ii methodology: A design perspective," *Int. J. Mod. Educ. Comput. Sci.,* vol. 13, no. 6, 2021, doi: 10.5815/ijmecs.2021.06.04.

[37] M. Ahmad et al., "Healthcare device security assessment through computational methodology," *Comput. Syst. Sci. Eng.,* vol. 41, no. 2, 2022, doi: 10.32604/csse.2022.020097.

[38] M. Nadeem, M. Ahmad, M. Ahmad, P. C. Pathak, S. Gupta, and H. Pandey, "Evaluating the Factors of CGTMSE Scheme in Bank by Using Fuzzy AHP," in *2023 6th International Conference on Contemporary Computing and Informatics (IC3I),* 2023, vol. 6, pp. 56–61, doi: 10.1109/IC3I59117.2023.10397669.

[39] W. Alosaimi et al., "Analyzing the impact of quantum computing on IoT security using computational based data analytics techniques," *AIMS Math.,* vol. 9, no. 3, pp. 7017–7039, 2024, doi: 10.3934/math.2024342.

[40] P. C. Pathak, M. Nadeem, and S. A. Ansar, "Security assessment of operating system by using decision making algorithms," *Int. J. Inf. Technol.,* 2024, doi: 10.1007/s41870-023-01706-9.