Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.043439

ARTICLE

# Enhancing IoT Security: Quantum-Level Resilience against Threats

**Hosam Alhakami**[*]

College of Computing, Umm Al-Qura University, Makkah, Saudi Arabia

*Corresponding Author: Hosam Alhakami. Email: hhhakam@uqu.edu.sa

Received: 03 July 2023 Accepted: 09 November 2023 Published: 30 January 2024

**ABSTRACT**

The rapid growth of the Internet of Things (IoT) operations has necessitated the incorporation of quantum computing technologies to meet its expanding needs. This integration is motivated by the need to solve the specific issues provided by the expansion of IoT and the potential benefits that quantum computing can offer in this scenario. The combination of IoT and quantum computing creates new privacy and security problems. This study examines the critical need to prevent potential security concerns from quantum computing in IoT applications. We investigate the incorporation of quantum computing approaches within IoT security frameworks, with a focus on developing effective security mechanisms. Our research, which uses quantum algorithms and cryptographic protocols, provides a unique solution to protecting sensitive information and assuring the integrity of IoT systems. We rigorously analyze critical quantum computing security properties, building a hierarchical framework for systematic examination. We offer concrete solutions flexible to diverse as well as ambiguous opinions through using a unified computational model with analytical hierarchy process (AHP) multi-criteria decision-making (MCDM) as the technique for ordering preferences by similarity to ideal solutions (TOPSIS) in a fuzzy environment. This study adds practical benefit by supporting practitioners in recognizing, choosing, and prioritizing essential security factors from the standpoint of quantum computing. Our approach is a critical step towards improving quantum-level security in IoT systems, strengthening their resilience against future threats, and preserving the IoT ecosystem's long-term prosperity.

**KEYWORDS**

Quantum security; quantum computing; Internet of Things; fuzzy decision-making

## 1 Introduction

In the present context, quantum technology strengthens various application areas, such as 5G wireless connections, the Internet of Things (IoT), wearable technology, and artificial intelligence (AI). Quantum computing is a highly centralized computing infrastructure that treats and caches data from the site of generation and the cloud. Quantum extends cloud computing. Moreover, it also complements the perception of agile devices, which can work on the fringes of the network. Quantum computing delivers assorted services while synchronously handling diverse sensors, processes, users, actuators, and connectivity by putting processing competence closer to the users. Quantum setups are proficient at handling various volumes of data provincially, acting on the premise that they are fully compact and may be built into amalgamated hardware. Quantum computing could help with IoT applications and overcome the limitations of the cloud when it comes to removing time-sensitive apps.

Though quantum computing is characterized as an augmentation of cloud computing, its' weird attributes in wireless connectivity, regional subtlety, and geographical receptiveness establish new concerns about security and forensics. There are still threats that have not been well addressed in cloud security or forensics. Most of the quantum operations are galvanized by the service and the users' necessities, while the security facets are usually neglected or taken as an afterthought. The possible security hazards associated with quantum computing in IoT systems demand an in-depth analysis of significant security threats. There are various essential threats, such as data breaches, unauthorized access, data interception, and cryptographic protocol compromise. When confronted with quantum attacks, these risks exploit the flaws of classical computer techniques. The privacy and security threats and assets in quantum computing have not been methodically diagnosed. The exploration of the privacy and security threats of quantum computing for the IoT is still in its infancy. The security threats to quantum computing are a subject of fascinating debate in academia. Since quantum computing is assumed to be a non-trivial expansion of the cloud, many privacy and security threats in the ambiance of cloud computing can be expected to impact quantum computing inevitably. Quantum computing faces new privacy and security threats besides those rooted in cloud computing. Some of the security threats can be addressed by using appropriate mechanisms. Still, the apparent features of quantum computing bring up a lot of essential problems and hazards.

By utilizing its unique features, quantum computing significantly improves the IoT environment. One standout benefit is its exponential processing capacity, which makes it possible to handle the intricate data analytics and optimization activities essential to IoT operations. Faster insights and decision-making, which are necessary for real-time IoT applications, are made possible by quantum computing's parallel processing features. Quantum computing adds revolutionary components to security and privacy. Since eavesdropping attempts destroy the fragile quantum state, which immediately reveals infiltration, quantum encryption provides ultra-secure communication. Data secrecy is supported by quantum key distribution (QKD) as a quantum-based security mechanism, which offers unbreakable encryption keys. Due to the fundamental aspects of quantum mechanics, QKD uses quantum principles to generate encryption keys among parties, making them impervious to eavesdropping efforts. Unlike traditional critical exchange systems, QKD's dependence on the uncertainty concept assures that any effort to intercept a key's quantum state breaks its integrity, disclosing infiltration immediately. As it directly tackles the vulnerabilities of conventional encryption techniques to quantum attacks, it provides improved security against classical and quantum attackers.

Furthermore, quantum-resistant cryptographic techniques, such as lattice-based encryption, enable security in a post-quantum future by safeguarding sensitive data even with the advent of powerful quantum computers. Such quantum-enhanced procedures strengthen IoT security by utilizing the unique properties of quantum phenomena to combat both traditional and emergent threats. Quantum-resistant algorithms also protect sensitive data from upcoming quantum attacks by fending off the cryptographic dangers of quantum computers. Compared to conventional computing techniques, this quantum-based security dramatically improves IoT privacy and protection, making quantum-enhanced IoT a powerful platform for secure, effective, and privacy-preserving activities.

This research study contributes by discussing the essential problems with quantum-level security in the setting of the IoT. The researchers acknowledge the IoT market's rapid expansion as well as the growing significance of quantum computing as an essential supportive technology. The study highlights the necessity to protect private data and uphold system integrity while identifying potential security threats to implementing quantum computing in IoT systems. The main contribution is outlining a thorough strategy to improve quantum-level security for IoT devices. The authors particularly want to incorporate quantum computing methods into current IoT security frameworks. They want to build robust security systems that can withstand attacks from regular and advanced adversaries by utilizing quantum algorithms and cryptographic protocols. The research offers a hierarchical structure of quantum computing security qualities to facilitate a systematic evaluation of security methods to accomplish this goal. The study also makes use of a unified computational model of multi-criteria decision-making (MCDM) that integrates the analytical hierarchy process (AHP) and the technique for ordering preferences by similarity to ideal solutions (TOPSIS) in a fuzzy setting. With this method, it is possible to identify, pick, and prioritize essential security criteria while considering conflicting information. The present study aims at investigating more feasible and workable solutions for security concerns in quantum computing. To do this, the authors have written about the many security aspects of quantum computing, as well as their sub-aspects, to help with the management of quantum layer security systematically. In addition, the researchers have also created a ranking system to manage and prioritize the security aspects. The rank, thus obtained, will assist the academics and the industry experts in systematically dealing with the security issues in quantum computing.

In addition to the above, the rest of this research work has been organized as follows: Section 2 discusses the recent work in this domain, followed by a discussion of the recognized quantum-level security attributes and their sub-attributes. After that, Section 3 discusses the materials and methods used to find the impact of the critical security attributes selected by the investigators in preparing their hierarchical model. Section 4 compares the results obtained by this method with those obtained by the classical AHP-TOPSIS. Section 5 presents a discussion of the findings of the research study. The conclusion and future guidelines are enumerated in Section 6.

## 2 Literature Review

To exploit the scope of the studies cited by different researchers and practitioners, commonly used substitutes and synonyms of words were identified to do an exhaustive literature review for this research study. A thorough analysis of the previous research literature in this context shows that the present security research threats and challenges can be classified as privacy, trust, authentication, threats and attacks, security audit, and access control. This section also looks at and points out the security threats and elucidation of auxiliary areas, including edge computing and cloud computing, which comprise the quantum computing setting. To ensure a comprehensive survey and analysis for our study, we perused various search settings for some of the most pertinent research articles in this domain. A manual search using distinct search engines in the areas of quantum and cloud security has been conducted to cater to the needs of the section.

Since the users' prime concern is their data privacy [1], privacy conservation has become an essential issue in quantum. The information used in quantum computing arrives from diverse sources, including wireless networks, IoT devices, and cloud networks. Therefore, a convenient privacy affirmation should be considered a consequential security threat in the quantum environment. In 2020, Zhao introduced a new distributed algorithm for data analytics on quantum-enabled IoT devices [2]. By integrating the distributed algorithm with homomorphic encryption, the author devised a method for protecting the privacy of edge devices. Vehicular cloud computing has become one of the biggest threats to this technology.

Xue et al. [3] also presented a study in the same context. A sophisticated computation burden is securely outsourced to cloud and quantum servers with privacy conservation and confidentiality.

Wang et al. [4] discussed data privacy and confidentiality in 2018. The researchers worked on quantum-oriented public cloud computing and pioneered the concepts of anonymity and secure accumulation. Pseudonyms, as well as combinatorial cryptographic techniques, were among their contributions. In 2017, Lu et al. [5] investigated the device and data privacy using lighter-weight privacy-preserving data accumulation techniques for quantum and IoT processes. The homomorphic cryptography, the Chinese Remainder Theorem, and one hash chain method were used.

In 2018, Rauf et al. [6] proposed a risk-oriented trust prototype method for the IoT setting. They presented a dynamic domain-adaptive security solution. They used criteria based on response time, availability, and reliability. In their work, they used direct and indirect perception for reliance estimation. Soleymani et al. [7] worked on securing trust formulation among vehicles in 2017. The authors proposed a fuzzy trust structure based on validity and understanding. They exhibited a series of security investigations in their work. In 2017, Dang et al. [8] proposed a dynamic data prevention scheme for quantum computing for mobility management services. Their work talks about privacy-aware, role-centric access control techniques. They also introduced quantum-based region verification.

In 2019, Wazid et al. [9] established that the security of quantum devices may be assured with the help of key management and authentication schemes. The authors executed adequate and lightweight exercises. Dsouza et al. [10] introduced policy-oriented resource management in the Quantum network in 2014, which supports interoperability and secure association among assorted resources in the Quantum system. In 2018, Zhang et al. [11] proposed an encouraging CP-ABE-centric access controller for a quantum computing setting where encryption and decryption are outsourced. In 2018, Vohra et al. [12] also presented a quantum-based disseminated multi-authority credit-based data access protocol. Xiao et al. [13] proposed a mixture of explanations for fine-grained owner-enforced exploration and an access agreement covering user-quantum-cloud and encountering the supply restraints of end procedures.

Stojmenovic et al. [14] proposed an authentication scheme to mitigate MITM attacks. The authors concluded that encryption and decryption methods are only sometimes well-suited due to the system's constraints. Homayoun et al. [15] 2019 used entirely mechanized and quantum node ransomware detection methods for the quantum layer. The study also established that deep learning methods may be used. Awan et al. [16] performed a comprehensive analysis using the fuzzy analytic hierarchy process (F-AHP) to address essential difficulties in the software business. Their research sought to determine and prioritize significant concerns in the software technology business, showing substantial impediments such as a need for more resources for innovative design and organizational reluctance to adopt new methods. Malina et al. [17] concentrated on privacy issues in the context of IoT/II services and the consequences of quantum computing. They performed an in-depth study emphasizing the significance of Privacy-Enhancing Technologies (PETs) in protecting privacy in IoT/II services. Their research mapped PET systems based on post-quantum cryptographic primitives that can withstand quantum computing challenges and investigated their practical applications using case studies. They also reviewed the obstacles and prospects for post-quantum PET development. Schöffel et al. [18] investigated how prospective post-quantum fundamental encapsulation mechanisms (KEMs), as well as digital signature algorithms (DSAs), could be applied to IoT infrastructures. They evaluated the impact of these new cryptographic algorithms on energy consumption, latency, and memory requirements throughout TLS handshakes in a low-power IoT scenario. Their findings shed light on the bandwidth-related latency of post-quantum primitives, the advantages of mixing several DSAs, and the possibility of implementing different cryptographic algorithms on IoT edge devices, putting dedicated hardware accelerators to the test. Table 1 shows the meta-analysis findings of related works.

**Table 1:** Meta-analysis of related works

| Researcher | Contribution | Novelty |
|---|---|---|
| Zhao [2] | Introduced a distributed algorithm for quantum-enabled IoT data analytics and privacy protection through homomorphic encryption. | A novel approach to protect edge device privacy in quantum-enabled IoT. |
| Xue et al. [3] | Securely outsourced computation to cloud and quantum servers while emphasizing privacy conservation and anonymity. | Pioneered the use of quantum-oriented public cloud computing and anonymity concepts. |
| Wang et al. [4] | Discussed data privacy and confidentiality in quantum-oriented public cloud computing, introducing pseudonyms and cryptographic techniques. | Introduced pseudonyms and novel cryptographic techniques. |
| Lu et al. [5] | Investigated device and data privacy in quantum IoT using lightweight privacy-preserving techniques such as homomorphic cryptography. | Employed homomorphic cryptography and novel privacy-preserving methods. |
| Rauf et al. [6] | Proposed a risk-oriented trust prototype method for IoT with dynamic domain-adaptive security solutions based on response time, availability, and reliability criteria. | Introduced dynamic trust models in IoT based on novel criteria. |
| Soleymani et al. [7] | Developed a fuzzy trust structure for trust formulation among vehicles, focusing on validity and understanding, with extensive security investigations. | Innovatively applied fuzzy trust structures and conducted comprehensive security studies. |
| Dang et al. [8] | Proposed a dynamic data prevention scheme for quantum computing in mobility management services, emphasizing privacy-aware, role-centric access control techniques. | Introduced dynamic privacy-aware access control techniques for quantum computing. |
| Wazid et al. [9] | Established the security of quantum devices through key management and authentication schemes, employing lightweight exercises. | Employed lightweight exercises for quantum device security. |

(Continued)

**Table 1 (continued)**

| Researcher | Contribution | Novelty |
|---|---|---|
| Dsouza et al. [10] | Introduced policy-oriented resource management in the Quantum network, supporting interoperability and secure associations among various resources. | Developed policy-oriented resource management for Quantum network interoperability. |
| Zhang et al. [11] | Proposed a CP-ABE-centric access controller for quantum computing settings, where encryption and decryption are outsourced, contributing to efficient access control. | Innovatively applied CP-ABE in quantum computing access control. |
| Vohra et al. [12] | Presented a quantum-based disseminated multi-authority credit-based data access protocol, enhancing data access control in quantum environments. | Introduced a novel data access control protocol in quantum settings. |
| Xiao et al. [13] | Proposed a comprehensive approach for fine-grained owner-enforced exploration and access agreements in user-quantum-cloud scenarios, addressing supply constraints. | Addressed fine-grained exploration and access control in user-quantum-cloud settings. |
| Stojmenovic et al. [14] | Proposed an authentication scheme to mitigate MITM attacks and highlighted the limitations of encryption and decryption methods. | Investigated authentication in IoT and emphasized constraints of encryption methods. |
| Homayoun et al. [15] | Utilized automated quantum node ransomware detection methods and demonstrated the use of deep learning techniques for security in the quantum layer. | Applied deep learning for quantum node security, contributing to quantum ransomware detection. |
| Awan et al. [16] | Conducted a comprehensive study using F-AHP to identify and prioritize challenges in the software industry, emphasizing resource scarcity and organizational reluctance. | Employed F-AHP for software industry challenges, highlighting resource and adoption issues. |
| Malina et al. [17] | Conducted an in-depth survey on privacy in IoT/II services and the impact of quantum computing, focusing on Privacy-Enhancing Technologies (PETs). | Mapped PET systems based on post-quantum cryptographic primitives and explored practical applications. |

(Continued)

**Table 1 (continued)**

| Researcher | Contribution | Novelty |
|---|---|---|
| Schöffel et al. [18] | Investigated the application of post-quantum KEMs and DSAs in low-power IoT, revealing insights into latency, energy consumption, and hardware requirements. | Explored the impact of post-quantum cryptography on IoT infrastructure, challenging the need for dedicated hardware accelerators. |

Undoubtedly, quantum computing is contemplated as being more secure than cloud computing. The collected statistics in quantum computing are cultivated and evaluated on local quantum nodes adjacent to data sources. This reduces the addiction to network connections. Further, the local data repository, transactions, and investigation make it extra challenging for the intruders to advance access to the user's information. However, one cannot deny the number of security risks associated with data transactions between the user's gadget and the quantum computing node or data transactions among different quantum nodes. Therefore, manifold threats exist in the process, and safeguarding privacy and security in quantum computing is not easy. Security issues can exist in diverse areas of quantum computing. The most critical areas in this context are networks, service infrastructure, virtualization, and users' devices.

There is inconsistency in the aggregation of all Quantum security-related concerns. Furthermore, only a limited number of elucidations are available to detect and prevent malicious attacks on the quantum platform. Hence, optimum security stands at the crux of ensuring the efficacy of quantum computing systems and, therefore, becomes an important research query. The lack of a thorough and unified evaluation of quantum security in the setting of IoT is the identified research gap in this study. Although the literature analysis highlights numerous research concentrating on certain quantum security issues such as privacy, trust, authentication, risks, attacks, security auditing, and access control, there is inconsistency in the way that these issues are combined into a single framework. Additionally, the study emphasizes that there are only a few ways to identify and stop hostile assaults in the context of quantum computing. Due to the dearth of thorough explanations, it is difficult to comprehend and mitigate the security risks associated with quantum computing, particularly when it comes to IoT devices. The study highlights the urgent need for an integrated strategy that takes into account all aspects of quantum security and overcomes the difficulties brought on by the special properties of quantum computing. This research gap is urgent due to the vulnerability of quantum computing caused by the many user-driven administrations of devices and the lack of strict control. As quantum computing grows more popular, creating adequate safeguards to protect IoT systems from quantum incidents becomes a critical but understudied field of research. None of the scholarly works we referred to provide a corroborative assessment of all the facets of quantum security. Quantum computing is vulnerable to astounding threats due to its segregated features. In the quantum computing environment, different users primarily drive and manage the devices. The quantum computing exemplar uses futile resources engendered by the users' gadgets. These gadgets are generally not examined by any of the definitive bodies, which can amplify the threats to security in the quantum environment.

## 3 Materials and Methods

### *3.1 Hierarchical Structure for Evaluation*

As a centralized resource, the cloud exhibits an unexceptional opportunity to breach privacy. The current cloud-based security services continue to target perimeter-based safety [15–19]. Cloud-based security services may cause an extreme moratorium for several applications and systems that desire impractically long-term communication bandwidth. If a threat penetrates these barriers, a system under safety will typically have finite and archaic competence to fight against the compromises. So, the current security model will not be able to protect the wide variety of IoT systems, devices, and applications. Thus, the following unique IoT security challenges need to be addressed:

- To gauge, authentically, whether a very diverse number of devices are operating securely.
- To secure an ample range of resource-constrained devices.
- To dynamically counter security breaches based on the requirements of the system and the risk levels of the violation.

Quantum computing plays an extensive role in this new security exemplar. In the realm of IoT security, traditional cryptographic protocols face vulnerabilities due to the computational power of quantum computers. Quantum algorithms, on the other hand, have the potential to solve complex problems exponentially faster than classical algorithms, which pose a significant threat to existing security mechanisms. Therefore, it becomes imperative to integrate quantum computing into the security paradigm to ensure robust protection against quantum adversaries. It administers a remedy to augment the privacy demands of the end-users of services. A quantum system is best positioned to deliver security services across diverse IoT devices [20]. It is tangibly and reasonably adjacent to the endpoints. This will enable extensible and authentic oversight of various devices and execute time-demanding and resource-accelerated security assignments on behalf of the endpoints [21]. Hence, any platform or system's security basics and requirements must be appropriately investigated from the ground up.

The reciprocal interaction of quantum and heterogeneous smart devices makes security management a problematic problem under the quantum paradigm. As a result, studying all of the security elements involved has become an unavoidable concern. The hierarchical tree of quantum computing security attributes provides a structured framework for systematic and efficient security measure consideration. This method groups security risks into a logical hierarchy, providing a clear understanding of their interdependence and relationships. This hierarchy assists in prioritizing efforts and ensures that essential security aspects are thoroughly addressed. This technique offers a more strategic as well as holistic approach to strengthening quantum-level security in IoT systems by breaking down complicated security concerns into manageable components. Fig. 1 depicts the hierarchal tree of the critical quantum computing security vulnerabilities, as highlighted by previous studies in this field. In addition, this shows the tree structure of the different security concerns about quantum computing that have been sorted based on research and conversations with people who work with it. Quantum computers are unable to crack encryption systems. According to the experts, quantum computers will be able to break all the current cryptographic coding schemes, including the Rivest-Shamir-Adleman (RSA), Diffie-Hellman, and elliptic curve (ECC) approaches, in a matter of time. Quantum-safe algorithms are being developed, and when a quantum computer renders today's encryption technologies useless, such approaches will be required in government and commercial enterprises. "Q-Day" is the name given to the day [22].

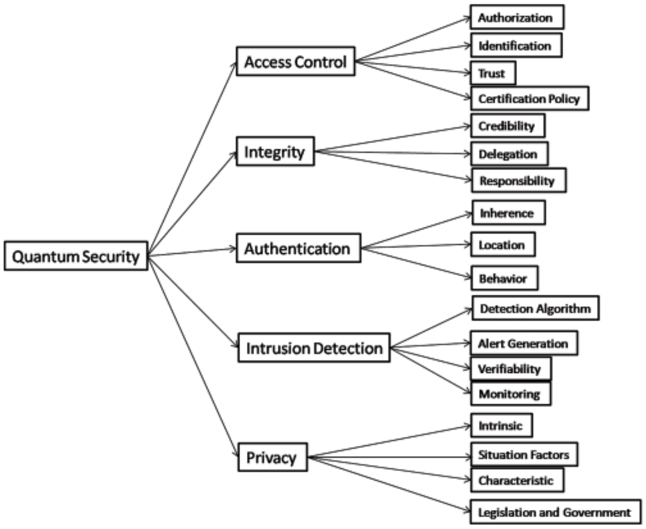

**Figure 1:** Tree structure of quantum security issues

### *3.1.1 Access Control [F1]*

Access management is a security strategy in a virtualized environment that governs who or what can gain access to or use resources. It is a fundamental security notion that mitigates the threat to an organization or business. There are two kinds of access control systems: physical and logical. Physical access controls the access to academic institutions, buildings, and spaces, as well as tangible IT resources. Logical access controls the restriction of access to computer network systems, system files, and data. Workforce access to confined business locations as well as proprietary territories, like data centers, is monitored through security access control models that depend on login details, access card users, auditing, and reports. A few of these systems have access control panels that restrict who can gain entry to rooms and housing developments. They also have alarms and lockdown mechanisms to keep individuals at bay and prevent them from entering or doing things they should not.

- *Authorization [F11]:* The process of permitting someone the right to use a resource is known as authorization [23]. This explanation may appear ambiguous, but many real-life circumstances can exemplify what authorization implies and how to apply those notions to computer systems. The household's ownership is a perfect example. The landlord has complete control over the assets (resources), and he or she can command the right of entry.
- *Identification [F12]:* Identification is a subject's claim to its own identity [24]. Authentication is the process of proving one's identity by supplying credentials to an access control system. The technique that determines the subject's access level(s) to the objects is called authorization.
- *Trust [F13]:* The belief in a machine's or sensor's ability to act consistently and securely, as well as consistently within a given environment, is known as trust [25]. Cryptography, digital signatures, and electronic certificates are often used in M2M networks to establish trust. This method develops and assesses a trust chain among devices; however, it does not provide sufficient information about the feature of data transmission between machines. Information security is only one aspect of trust; it also comprises subjective criteria and experience.
- *Certification Policy [F14]:* Policy for users is a process in which you validate that someone who is attempting to access services and applications is indeed the one who he or she claims to be [26]. This can be accomplished through a variety of certification methods.

### *3.1.2 Integrity [F2]*

The ability to ensure that a framework and its data have not even been tampered with is referred to as integrity. Not only is data protected by integrity preservation, but even operating systems, applications, and hardware are protected from unauthorized access [27].

- Credibility [F21]: A key concern for companies is that they need to be trustworthy and reliable. They have to be extra careful about their systems to avoid getting into trouble with the law if something bad happens. If they do not handle data and security well, it can be a real problem [28]. An example we have considered is that of an autonomous car. With no one in the driver's seat, human error is eliminated, leaving only the systems to blame when something goes wrong.
- Delegation [F22]: Delegation is the procedure of a computer consumer handing over its authentication credentials to another user [29]. In role-based access control models, delegation of authority involves delegating the roles that a user can assume or the set of permissions that the user can acquire to other users.
- Responsibility [F23]: This implies using advanced software security techniques following the technical reference architecture, implementing, testing, and running them [30]. To increase software security, undertake ongoing security testing and code review. Issues that develop are troubleshot and debugged.

### *3.1.3 Authentication [F3]*

Authentication is the procedure of validating the identity of the user or information [31]. User authentication is the process of verifying the user's identity at the time of login. Single-Factor Authentication (SFA): This was the first security solution devised.

- Inherence [F31]: The inherent risk is a vulnerability that exists within an organization before the implementation of security measures [32]. On the other side, residual risk is evaluated after all of these inherent hazards have been mitigated by cybersecurity measures. It considers every possible attack vector that could compromise a system or its data.
- Location [F32]: A secure location is an area in a defined site where entry is regulated by lock and key, backed up by an adequate security system, and only authorized company employees have access to that [33].
- Behavior [F33]: Behavior-based access control is a proactive strategy of protection in which all applicable actions are supervised to identify and address variances from regular patterns of behavior as soon as they occur [34,35].

### *3.1.4 Intrusion Detection [F4]*

An intrusion detection system, or IDS for short, keeps an eye on network and system traffic for any unusual activities [36]. Intrusion detection software will provide you with a notice after possible threats have been identified.

- Detection Algorithm [F41]: An intrusion detection system (IDS) is a network traffic analysis system that identifies strange activities and notifies the users when they are discovered [35]. It is software that scans a computer system or network for malicious activity. Any malicious activity or policy violations are notified to an operations manager or the central monitoring unit by using an SIEM scheme. A SIEM scheme can collect data from various sources and use alarm scanning methods to differentiate between harmful and false alarms.
- Alert Generation [F42]: IT alerting software sends out notifications when a computer system fails [9–12]. These tools will keep an eye on systems for issues including slow performance,

infrastructure problems, and other IT management difficulties. Email, SMS, or other forms of communication may be used to provide these notifications. These tools are used by businesses to identify problems with their networks, IT infrastructure, and other IT systems to save time and prevent irreversible damage. By capturing incidents, collecting historical records, and analyzing them, some tools can help speed up the resolution and recovery procedures.

- Verifiability [F43]: Software verification pledges that "you built it right" as well as that the artifact, when carried out, meets the developers' expectations [13]. Software authentication guarantees that "you produced the proper thing" as well as that the invention, as delivered, meets the stakeholders' intended use and goals.
- Monitoring [F44]: Security monitoring is the automated process of acquiring and analyzing signals of potential security threats, prioritizing them, and taking appropriate action to address them [14].

#### *3.1.5 Privacy [F5]*

The term "privacy software" refers to applications that are designed to keep their users confidential [15]. The program is generally used in combination with Internet usage to handle or restrict the amount of data made publicly available to third-party companies. The application is capable of a wide range of encryption and filtration.

- Intrinsic [F51]: The intrinsic security model replaces the reactive model with a framework that enables the company to be proactive [16]. Security is built into all of your environment's critical control points, including the network, the cloud, endpoints, workloads, and identity management.
- Situation Factors [F52]: Human variables are psychological, physiological, and environmental characteristics that are both inherent in humans and influence how they interact with the rest of the world [17,18]. Human variables such as fatigue, time of day, diversions, and even the way information is displayed on a screen are used to demonstrate the impact on how successfully individuals perform their tasks and how secure they are in industries such as aviation, trucking, healthcare, manufacturing, and nuclear power.
- Legislation and Government [F53]: Security legislation refers to all the laws that govern security protocols from time to time, along with the Aviation and Maritime Security Act of 1990, the International Code for the Security of Ships, as well as Port Facilities, and any manually configuring or substituting security legislative action [36].

### ***3.2 Methodology***

When paired with fuzzy sets, the multi-criteria decision-making (MCDM) model provides a systematic framework for choosing and prioritizing security factors in quantum computing for IoT. The model handles complicated, real-world scenarios by taking into account varied perspectives and uncertainty. This method allows practitioners to quantitatively assess security properties against a variety of criteria. It can, for example, assist in determining the most effective encryption method depending on a variety of characteristics such as processing efficiency, resistance to quantum assaults, and deployment expenses. The model could help choose access control strategies that balance user privacy, system efficiency, as well as security in scenarios involving vital infrastructure, such as smart grids. By integrating quantum computing into the security exemplar, we aim to harness the unique capabilities offered by this emerging technology to address the vulnerabilities and challenges faced by IoT systems. The extensive role of quantum computing in the exemplar underscores its potential to revolutionize IoT security and pave the way for resilient and quantum-resistant solutions. Managing security in software is the task of design management [37–40]. To make an effective and secure software design, it is always significant to work on the tactics of design management [41]. Hence, prioritizing this approach, the authors of the present study consulted several industry experts and researchers working in this area. After collating the recommendations given by these experts, the authors classified the various tactics and their sub-tactics. Thereafter, the next step was to design the computational model. For this, the authors adopted the most significant MCDM approach in the current era, i.e., fuzzy AHP-TOPSIS [42–44]. This approach provides an efficient and effective outcome in a situation where the user has more than one option to choose from. A descriptive discussion of the methodology is enunciated below.

Its fundamental precept is to find the highest-quality viable replacement among a set of alternative strategies and then rank all of them based on their evaluation metrics. Fuzzy-based AHP is used throughout the research to demonstrate the weights of the criterion (characteristics), as well as fuzzy-based TOPSIS, which is used to prioritize the alternatives. To figure out how to calculate the results for this method, the authors had to do the following.

Step 1: Triangular Fuzzy Number (TFN) is architecturally a triplet (f1, f2, f3) wherein f1 < f2 < f3 and f1 represents minor importance, f2 middle one and < f3 signifies upper importance. The membership function of the fuzzy number ∼T is confirmed with the assistance of Eqs. (1) and (2) as well as the quantity is documented as TFN. Fig. 2 demonstrates the structure of a TFN.

$$\mu_a(x) = F \to [0, 1] \tag{1}$$

$$\mu_a(x) = \begin{cases} \dfrac{x}{mi - lo} - \dfrac{b}{mi - lo} x \in [lo,\ mi] \\ \dfrac{x}{mi - up} - \dfrac{u}{mi - up} x \in [mi,\ up] \\ 0 \qquad\qquad\qquad\qquad \text{Otherwise} \end{cases} \tag{2}$$

As per the triangular membership function, Eq. (1), mi and u represent the lower, middle, and upper limit for triangular membership numbers.

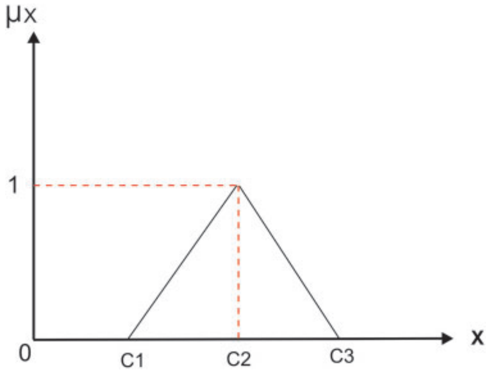

**Figure 2:** TFN

After that, a fuzzy transformation is completed on these numeric statistics. To transform the numeric data into TFNs, Eqs. (3)–(6) are employed as well as represented as (f1ij, f2ij, f3ij), where f1ij grants low importance, f2ij grants middle importance, and f3ij grants upper importance (Table 2). Additional TFN [ij] is distinct, such as:

$$n_{ij} = (l_{ij}, m_{ij,}u_{ij}) \tag{3}$$

where, $l_{ij} \leq m_{ij} \leq u_{ij}$

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

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

and $u_{ij} = (J_{ijd})$ (6)

**Table 2:** TFN scale

| Saaty scale definition | Scale | |
|---|---|---|
| 1 | Equally important | (1, 1, 1) |
| 3 | Weakly important | (2, 3, 4) |
| 5 | Fairly important | (4, 5, 6) |
| 7 | Strongly important | (6, 7, 8) |
| 9 | Absolutely important | (9, 9, 9) |

Jijk denotes the degree of importance of attributes among some of the two factors using professional opinion as well as the expressions presented above. I and j are the element pairs that are evaluated and symbolized. Furthermore, the processes on the two TFNs are carried out with the assistance of Eqs. (7)–(9). Supposing T1 and T2 are two TFNs, T1 = (f11, f21, f31) and T2 = (f12, f22, f32). At that moment, the functioning rules for them would be:

$$\left(l_1, m_{i1,}u_1\right) + \left(l_2, m_{i2,}u_2\right) = \left(l_1 + l_2, m_{i1} + m_{i2,}u_1 + u_2\right) \tag{7}$$

$$\left(l_1, m_{i1,}u_1\right) \times \left(l_2, m_{i2,}u_2\right) = \left(l_1 \times l_2, m_{i1} \times m_{i2,}u_1 \times u_2\right) \tag{8}$$

$$\left(l_1, m_{i1,}u_1\right) - 1 = \left(\frac{1}{u_1}, \frac{1}{m_{i1}}, \frac{1}{l_1}\right) \tag{9}$$

$$\tilde{A}^d = \begin{bmatrix} \tilde{k}_{11}^d & \tilde{k}_{12}^d & \tilde{k}_{1n}^d \\ \ldots\ldots & \ldots\ldots & \ldots\ldots \\ \tilde{k}_{n1}^d & \tilde{k}_{n2}^d & \tilde{k}_{nn}^d \end{bmatrix} \tag{10}$$

$$\tilde{k}_{ij} = \sum_{d=1}^{d} \tilde{k}_{ij}^d \tag{11}$$

By using Eq. (12), the authors integrate the experts' opinions into the mathematical function and try to elaborate on them in it.

$$\tilde{A} = \begin{bmatrix} \widetilde{k_{11}} & \cdots & \widetilde{k_{1n}} \\ \ldots & \ddots & \ldots \\ \widetilde{k_{n1}} & \cdots & \tilde{k}_{nn} \end{bmatrix} \tag{12}$$

The following Eqs. (13)–(16) are used by the authors to normalize the value and find the geometric mean of functions.

$$\tilde{P}_i = \left( \prod_{j=1}^{n} \tilde{k}_{ij} \right)^{1/n}, i = 1, 2, 3, 4, \ldots, \mathrm{n} \tag{13}$$

$$\widetilde{w_i} = \widetilde{p_i} \otimes \left( \widetilde{p_1} \oplus \widetilde{p_2} \oplus \widetilde{p_3} \ldots\ldots \oplus \widetilde{p_n} \right)^{-1} \tag{14}$$

$$\mathrm{M_i} = \frac{\tilde{\mathrm{w}}_1 \oplus \tilde{\mathrm{w}}_2 \ldots.. \oplus \tilde{\mathrm{w}}_\mathrm{n}}{\mathrm{n}} \tag{15}$$

$$\mathrm{Nr_i} = \frac{\mathrm{M_i}}{\mathrm{M_1} \oplus \mathrm{M_2} \oplus \ldots\ldots \oplus \mathrm{M_n}} \tag{16}$$

Now, after conducting all these steps and solving the equations, the BNP value is determined by using Eq. (17).

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

This completes the process for the fuzzy-AHP methodology. After this, the TOPSIS part begins. The TOPSIS methodology is adopted by the authors to test the ranking and effectiveness of the evaluated outcomes in a simulation scenario to validate the outcomes. The descriptive steps that were followed during this methodology are discussed below.

By using Table 3 and Eq. (18), we prepared the correlation between the previously evaluated data and the tested alternatives.

$$\tilde{K} = \begin{array}{c c} & \begin{array}{ccc} Cr_1 & \ldots. & Cr_n \end{array} \\ \begin{array}{c} A_1 \\ \ldots \\ A_m \end{array} & \begin{bmatrix} \tilde{\alpha}_{11} & \cdots & \tilde{\alpha}_{1n} \\ \ldots & \ddots & \ldots \\ \tilde{\alpha}_{m1} & \cdots & \tilde{\alpha}_{mn} \end{bmatrix} \end{array} \tag{18}$$

To make the standard of the function, Eq. (19) is used, and after that, to create the grid, Eq. (20) is utilized.

$$\tilde{P} = \left[ \tilde{P}_{ij} \right]_{m \times n} \tag{19}$$

$$\tilde{Q} = \left[ \tilde{q}_{ij} \right]_{m \times n} i = 1, 2, 3, \ldots\ldots.m; j = 1, 2, 3, 4, \ldots, n \tag{20}$$

**Table 3:** Ranking scale

| Linguistic variable | Corresponding TFN |
|---|---|
| Very poor | (0, 1, 3) |
| Poor (P) | (1, 3, 5) |
| Fair (F) | (3, 5, 7) |
| Good (G) | (5, 7, 9) |
| Very good (VG) | (7, 9,10) |

After identifying all these attributes and equations, the next step is to evaluate the gap degree by the following Eq. (21).

$$C\tilde{C} = \frac{\tilde{k}_i^-}{\tilde{k}_i^+ + \tilde{k}_i^-} = 1 - \frac{\tilde{k}_i^+}{\tilde{k}_i^+ + \tilde{k}_i^-}, i = 1, 2, \ldots, m \tag{21}$$

After evaluating all these equations and formulae, we found the whole simulated scenario of security tactics. This computational methodology is most effective in the current situation of its real-world application capability. The authors attempted a simulator approach to test the efficacy of the above technique.

## 4 Data Analysis and Results

### *4.1 Statistical Findings*

To apply the above-discussed technique in a real-world scenario, the authors prepared a security tactic based on the tree structure that has already been discussed in Fig. 1. The authors applied the adopted approach of fuzzy-AHP-TOPSIS to the stated readings in Fig. 1 and evaluated the results in a computational manner that would facilitate the industry's development. Moreover, the designed tree structure has seven security domains or tactics available that will enhance the design of software and help the developers manage software security effectively.

Using the method described in the previous section, the authors did the computational analysis to come up with Table 2 and Eqs. (1)–(17). Further, from Tables 4 to 9, we are showing the integrated fuzzy-based comparison matrices as per Fig. 1. In addition, Tables 10 to 15 show the defuzzified values for various groups, and Table 16 represents the final weights of the attributes.

**Table 4:** Integrated fuzzy-based comparison matrix at level 1

| Level 1 | F1 | F2 | F3 | F4 | F5 |
|---|---|---|---|---|---|
| F1 | 1.000000,<br>1.000000,<br>1.000000 | 1.872022,<br>2.527010,<br>3.203105 | 1.461400,<br>1.681042,<br>1.974301 | 1.441601,<br>2.431805,<br>3.386105 | 0.461707,<br>0.572104,<br>0.784501 |
| F2 | – | 1.000000,<br>1.000000,<br>1.000000 | 0.601083,<br>0.771504,<br>1.021065 | 0.771008,<br>0.950400,<br>1.213601 | 0.161300,<br>0.195013,<br>0.249017 |

(Continued)

**Table 4 (continued)**

| Level 1 | F1 | F2 | F3 | F4 | F5 |
|---|---|---|---|---|---|
| F3 | – | – | 1.000000, 1.000000, 1.000000 | 0.716904, 1.015002, 1.351503 | 0.201806, 0.241602, 0.311107 |
| F4 | – | – | – | 1.000000, 1.000000, 1.000000 | 0.195106, 0.228103, 0.219003 |
| F5 | – | – | – | – | 1.000000, 1.000000, 1.000000 |

**Table 5:** Integrated fuzzy-based comparison matrix for F1 at level 2

| | F11 | F12 | F13 | F14 |
|---|---|---|---|---|
| F11 | 1.00000, 1.00000, 1.00000 | 1.75540, 2.34580, 3.03630 | 1.48540, 1.95750, 2.52630 | 1.12980, 1.55510, 1.98950 |
| F12 | – | 1.00000, 1.00000, 1.00000 | 0.57000, 0.78600, 1.16000 | 0.56000, 0.72000, 0.96990 |
| F13 | – | – | 1.00000, 1.00000, 1.00000 | 0.62860, 0.81750, 1.07560 |
| F14 | – | – | – | 1.00000, 1.00000, 1.00000 |

**Table 6:** Integrated fuzzy-based comparison matrix for F2 at level 2

| | F21 | F22 | F23 |
|---|---|---|---|
| F21 | 1.00000, 1.00000, 1.00000 | 0.23750, 0.28790, 0.36750 | 0.3421, 0.4477, 0.8247 |
| F22 | – | 1.00000, 1.00000, 1.00000 | 0.66140, 1.17250, 1.69360 |
| F23 | – | – | 1.00000, 1.00000, 1.00000 |

**Table 7:** Integrated fuzzy-based comparison matrix for F3 at level 2

| | F31 | F32 | F33 |
|---|---|---|---|
| F31 | 1.00000, 1.00000, 1.00000 | 0.66503, 1.17230, 1.69740 | 1.15760, 1.44720, 1.70430 |
| F32 | – | 1.00000, 1.00000, 1.00000 | 1.00770, 1.52470, 1.93430 |
| F33 | – | – | 1.00000, 1.00000, 1.00000 |

**Table 8:** Integrated fuzzy-based comparison matrix for F4 at level 2

| | F41 | F42 | F43 | F44 |
|---|---|---|---|---|
| F41 | 1.00000, 1.00000, 1.00000 | 0.69410, 0.89530, 1.11240 | 0.23450, 0.28780, 0.36410 | 0.71120, 0.95410, 1.35120 |
| F42 | – | 1.00000, 1.00000, 1.00000 | 0.49310, 0.64230, 1.24140 | 0.27130, 0.35150, 0.52160 |
| F43 | – | – | 1.00000, 1.00000, 1.00000 | 1.08540, 1.32970, 1.55820 |
| F44 | – | – | – | 1.00000, 1.00000, 1.00000 |

**Table 9:** Integrated fuzzy-based comparison matrix for F5 at level 2

| | F51 | F52 | F53 |
|---|---|---|---|
| F51 | 1.00000, 1.00000, 1.00000 | 1.19780, 1.58803, 2.15640 | 0.49110, 0.64202, 1.00990 |
| F52 | – | 1.00000, 1.00000, 1.00000 | 0.22410, 0.29560, 0.42790 |
| F53 | – | – | 1.00000, 1.00000, 1.00000 |

**Table 10:** Integrated comparison matrix and local weights at level 1

| Level 1 | F1 | F2 | F3 | F4 | F5 | Weights |
|---|---|---|---|---|---|---|
| F1 | 1.000000 | 2.551440 | 1.710170 | 2.421740 | 0.591930 | 0.2400000 |
| F2 | 0.391150 | 1.000000 | 0.791640 | 0.971690 | 0.201730 | 0.0952000 |
| F3 | 0.581760 | 1.255160 | 1.000000 | 1.051630 | 0.251320 | 0.1200000 |
| F4 | 0.411200 | 1.021360 | 0.941670 | 1.000000 | 0.231570 | 0.1032000 |
| F5 | 1.661860 | 4.821390 | 3.941950 | 4.214270 | 1.000000 | 0.4416000 |
| CR = 0.0025025 | | | | | | |

**Table 11:** Integrated comparison matrix and local weights for F1 at level 2

| | F11 | F12 | F13 | F14 | Weights |
|---|---|---|---|---|---|
| F11 | 1.000000 | 2.372300 | 1.981900 | 1.556400 | 0.3900000 |
| F12 | 0.421500 | 1.000000 | 0.824300 | 0.744700 | 0.1700000 |
| F13 | 0.504600 | 1.213200 | 1.000000 | 0.830900 | 0.2000000 |
| F14 | 0.642500 | 1.342800 | 1.203500 | 1.000000 | 0.2400000 |
| CR = 0.0015400 | | | | | |

**Table 12:** Integrated comparison matrix and local weights for F2 at level 2

| | F21 | F22 | F23 | Weights |
|---|---|---|---|---|
| F21 | 1.000000 | 1.173000 | 0.494000 | 0.2749000 |
| F22 | 0.852500 | 1.000000 | 1.172000 | 0.3296000 |
| F23 | 2.024300 | 0.853200 | 1.000000 | 0.3955000 |
| CR = 0.0024500 | | | | |

**Table 13:** Integrated comparison matrix and local weights for F3 at level 2

| | F31 | F32 | F33 | Weights |
|---|---|---|---|---|
| F31 | 1.000000 | 1.172000 | 1.363000 | 0.3843000 |
| F32 | 0.853300 | 1.000000 | 1.491000 | 0.3562000 |
| F33 | 0.733700 | 0.670700 | 1.000000 | 0.2595000 |
| CR = 0.0025000 | | | | |

**Table 14:** Integrated comparison matrix and local weights for F4 at level 2

| | F41 | F42 | F43 | F44 | Weights |
|---|---|---|---|---|---|
| F41 | 1.000000 | 0.892000 | 1.173000 | 0.994000 | 0.2463000 |
| F42 | 1.121100 | 1.000000 | 0.691000 | 0.372000 | 0.1820000 |
| F43 | 0.852500 | 1.447200 | 1.000000 | 1.298000 | 0.2724000 |
| F44 | 1.006100 | 2.688200 | 0.770400 | 1.000000 | 0.2993000 |
| CR = 0.0025400 | | | | | |

**Table 15:** Integrated comparison matrix and local weights for F5 at level 2

| | F51 | F52 | F53 | Weights |
|---|---|---|---|---|
| F51 | 1.000000 | 1.633000 | 0.691000 | 0.3159000 |
| F52 | 0.612400 | 1.000000 | 0.303000 | 0.1731000 |
| F53 | 1.447200 | 3.300300 | 1.000000 | 0.5110000 |
| CR = 0.005200 | | | | |

**Table 16:** Final weights

| Attributes of level 1 | Independent weights | Attributes of level 2 | Independent weights | Dependent weights |
|---|---|---|---|---|
| F1 | 0.2400000 | F11 | 0.3900000 | 0.0093600 |
| | | F12 | 0.1700000 | 0.0040800 |
| | | F13 | 0.2000000 | 0.0048000 |
| | | F14 | 0.2400000 | 0.0057600 |
| F2 | 0.0952000 | F21 | 0.2749000 | 0.0261705 |
| | | F22 | 0.3296000 | 0.0313779 |
| | | F23 | 0.3955000 | 0.0376516 |
| F3 | 0.1200000 | F31 | 0.3843000 | 0.0461160 |
| | | F32 | 0.3562000 | 0.0427440 |
| | | F33 | 0.2595000 | 0.0311400 |
| F4 | 0.1032000 | F41 | 0.2463000 | 0.0254182 |
| | | F42 | 0.1820000 | 0.0187824 |
| | | F43 | 0.2724000 | 0.0281117 |
| | | F44 | 0.2993000 | 0.0308878 |
| F5 | 0.4416000 | F51 | 0.3159000 | 0.1395014 |
| | | F52 | 0.1731000 | 0.0764410 |
| | | F53 | 0.5110000 | 0.2269824 |

After analyzing the fuzzy AHP technique and its priority list, the authors evaluated the overall impact by adopting the TOPSIS approach. To perform this approach, we took fifteen real-time projects from Babasaheb Bhimrao Ambedkar University, Lucknow, Uttar Pradesh, India. These projects' data comprised a repository of the results of quiz competitions and entrance tests held at the university over a two- to five-year period. The selected projects were taken as the alternatives in this study. The sensitivity of these selected alternatives was very high. Tables 17 and 18 demonstrate the use of the fuzzy TOPSIS method (Table 3 and Eqs. (18)–(21)) to evaluate the results.

**Table 17:** Subjective cognition results

| Alternatives/ attributes | A1 | A2 | A3 | A4 | A5 | A6 | A7 |
|---|---|---|---|---|---|---|---|
| F11 | 6.3800,<br>8.3800,<br>9.6900 | 4.3800,<br>6.3800,<br>8.3800 | 7.0000,<br>9.0000,<br>10.0000 | 6.3800,<br>8.3800,<br>9.6900 | 4.3800,<br>6.3800,<br>8.3800 | 7.0000,<br>9.0000,<br>10.0000 | 3.0000,<br>5.0000,<br>7.0000 |

(Continued)

**Table 17 (continued)**

| Alternatives/ attributes | A1 | A2 | A3 | A4 | A5 | A6 | A7 |
|---|---|---|---|---|---|---|---|
| F12 | 7.0000, 9.0000, 10.000 | 6.3800, 8.3800, 9.6900 | 4.3800, 6.3800, 8.3800 | 7.0000, 9.0000, 10.000 | 7.0000, 9.0000, 10.000 | 6.2400, 8.2400, 9.6200 | 5.0000, 7.0000, 9.0000 |
| F13 | 3.0000, 5.0000, 7.0000 | 7.0000, 9.0000, 10.000 | 7.0000, 9.0000, 10.000 | 3.0000, 5.0000, 7.0000 | 7.0000, 9.0000, 10.000 | 5.6200, 7.6200, 9.3100 | 7.0000, 9.0000, 10.000 |
| F14 | 7.0000, 9.0000, 10.000 | 3.0000, 5.0000, 7.0000 | 7.0000, 9.0000, 10.000 | 7.0000, 9.0000, 10.000 | 7.0000, 9.0000, 10.000 | 5.7600, 7.7600, 9.3800 | 3.0000, 5.0000, 7.0000 |
| F21 | 6.3800, 8.3800, 9.6900 | 4.3800, 6.3800, 8.3800 | 6.3800, 8.3800, 9.6900 | 4.3800, 6.3800, 8.3800 | 7.0000, 9.0000, 10.0000 | 3.0000, 5.0000, 7.0000 | 3.0000, 5.0000, 7.0000 |
| F22 | 7.0000, 9.0000, 10.000 | 7.0000, 9.0000, 10.000 | 6.3800, 8.3800, 9.6900 | 4.3800, 6.3800, 8.3800 | 7.0000, 9.0000, 10.0000 | 3.0000, 5.0000, 7.0000 | 3.0000, 5.0000, 7.0000 |
| F23 | 3.0000, 5.0000, 7.0000 | 7.0000, 9.0000, 10.000 | 7.0000, 9.0000, 10.000 | 6.3800, 8.3800, 9.6900 | 4.3800, 6.3800, 8.3800 | 7.0000, 9.0000, 10.0000 | 3.0000, 5.0000, 7.0000 |
| F31 | 7.0000, 9.0000, 10.000 | 7.0000, 9.0000, 10.000 | 3.0000, 5.0000, 7.0000 | 7.0000, 9.0000, 10.000 | 7.0000, 9.0000, 10.000 | 6.2400, 8.2400, 9.6200 | 5.0000, 7.0000, 9.0000 |
| F32 | 5.6200, 7.6200, 9.3100 | 3.7600, 5.7600, 7.7600 | 7.0000, 9.0000, 10.000 | 3.0000, 5.0000, 7.0000 | 7.0000, 9.0000, 10.000 | 5.6200, 7.6200, 9.3100 | 7.0000, 9.0000, 10.000 |
| F33 | 5.6200, 7.6200, 9.3100 | 8.3800, 9.6900, 10.0000 | 5.6200, 7.6200, 9.3100 | 7.0000, 9.0000, 10.000 | 7.0000, 9.0000, 10.000 | 5.7600, 7.7600, 9.3800 | 3.0000, 5.0000, 7.0000 |
| F41 | 6.3800, 8.3800, 9.6900 | 4.3800, 6.3800, 8.3800 | 7.0000, 9.0000, 10.0000 | 3.0000, 5.0000, 7.0000 | 3.0000, 5.0000, 7.0000 | 4.3800, 6.3800, 8.3800 | 3.0000, 5.0000, 7.0000 |
| F42 | 7.0000, 9.0000, 10.000 | 7.0000, 9.0000, 10.000 | 6.3800, 8.3800, 9.6900 | 4.3800, 6.3800, 8.3800 | 7.0000, 9.0000, 10.0000 | 3.0000, 5.0000, 7.0000 | 3.0000, 5.0000, 7.0000 |
| F43 | 3.0000, 5.0000, 7.0000 | 7.0000, 9.0000, 10.000 | 7.0000, 9.0000, 10.000 | 7.0000, 9.0000, 10.000 | 6.2400, 8.2400, 9.6200 | 5.0000, 7.0000, 9.0000 | 3.7600, 5.7600, 7.7600 |
| F44 | 7.0000, 9.0000, 10.000 | 7.0000, 9.0000, 10.000 | 3.0000, 5.0000, 7.0000 | 6.3800, 8.3800, 9.6900 | 4.3800, 6.3800, 8.3800 | 7.0000, 9.0000, 10.0000 | 3.0000, 5.0000, 7.0000 |

(Continued)

**Table 17 (continued)**

| Alternatives/ attributes | A1 | A2 | A3 | A4 | A5 | A6 | A7 |
|---|---|---|---|---|---|---|---|
| F51 | 5.6200, 7.6200, 9.3100 | 3.7600, 5.7600, 7.7600 | 7.0000, 9.0000, 10.000 | 7.0000, 9.0000, 10.000 | 7.0000, 9.0000, 10.000 | 6.2400, 8.2400, 9.6200 | 5.0000, 7.0000, 9.0000 |
| F52 | 5.6200, 7.6200, 9.3100 | 8.3800, 9.6900, 10.0000 | 5.6200, 7.6200, 9.3100 | 3.0000, 5.0000, 7.0000 | 7.0000, 9.0000, 10.000 | 5.6200, 7.6200, 9.3100 | 7.0000, 9.0000, 10.000 |
| F53 | 5.6200, 7.6200, 9.3100 | 9.0000, 10.0000, 10.000 | 5.6200, 7.6200, 9.3100 | 7.0000, 9.0000, 10.000 | 7.0000, 9.0000, 10.000 | 5.7600, 7.7600, 9.3800 | 3.0000, 5.0000, 7.0000 |

**Table 18:** Weighted normalized fuzzy-decision matrix

| Alternative/ attributes | A1 | A2 | A3 | A4 | A5 | A6 | A7 |
|---|---|---|---|---|---|---|---|
| F11 | 0.00400, 0.00600, 0.00800 | 0.00300, 0.00400, 0.00600 | 0.00900, 0.01400, 0.02000 | 0.02500, 0.03400, 0.04100 | 0.02800, 0.04100, 0.05400 | 0.02000, 0.03300, 0.04600 | 0.00900, 0.01400, 0.02000 |
| F12 | 0.00000, 0.00100, 0.00300 | 0.00000, 0.00200, 0.00300 | 0.00400, 0.00600, 0.00800 | 0.00300, 0.00400, 0.00600 | 0.00900, 0.01400, 0.02000 | 0.02500, 0.03400, 0.04100 | 0.02800, 0.04100, 0.05400 |
| F13 | 0.00100, 0.00300, 0.00500 | 0.00000, 0.00000, 0.00100 | 0.00000, 0.00100, 0.00300 | 0.00000, 0.00200, 0.00300 | 0.00900, 0.01400, 0.02000 | 0.00300, 0.01000, 0.01900 | 0.00400, 0.01500, 0.02800 |
| F14 | 0.00400, 0.00600, 0.00800 | 0.00300, 0.00400, 0.00600 | 0.00900, 0.01400, 0.02000 | 0.02500, 0.03400, 0.04100 | 0.02800, 0.04100, 0.05400 | 0.03100, 0.04000, 0.04400 | 0.05900, 0.06600, 0.06600 |
| F21 | 0.00000, 0.00100, 0.00300 | 0.00000, 0.00200, 0.00300 | 0.00900, 0.01400, 0.02000 | 0.00300, 0.01000, 0.01900 | 0.00400, 0.01500, 0.02800 | 0.01300, 0.02200, 0.03100 | 0.03700, 0.05000, 0.06100 |
| F22 | 0.00100, 0.00300, 0.00500 | 0.00000, 0.00000, 0.00100 | 0.00400, 0.00600, 0.00800 | 0.00300, 0.00400, 0.00600 | 0.00900, 0.01400, 0.02000 | 0.02500, 0.03400, 0.04100 | 0.02800, 0.04100, 0.05400 |
| F23 | 0.00400, 0.00600, 0.00800 | 0.00300, 0.00400, 0.00600 | 0.00900, 0.01400, 0.02000 | 0.02500, 0.03400, 0.04100 | 0.02800, 0.04100, 0.05400 | 0.00300, 0.01000, 0.01900 | 0.00400, 0.01500, 0.02800 |
| F31 | 0.00000, 0.00100, 0.00300 | 0.00000, 0.00200, 0.00300 | 0.00900, 0.01400, 0.02000 | 0.00300, 0.01000, 0.01900 | 0.00400, 0.01500, 0.02800 | 0.03100, 0.04000, 0.04400 | 0.05900, 0.06600, 0.06600 |

(Continued)

**Table 18 (continued)**

| Alternative/ attributes | A1 | A2 | A3 | A4 | A5 | A6 | A7 |
|---|---|---|---|---|---|---|---|
| F32 | 0.00100, 0.00300, 0.00500 | 0.00000, 0.00000, 0.00100 | 0.00400, 0.00600, 0.00800 | 0.00300, 0.00400, 0.00600 | 0.00900, 0.01400, 0.02000 | 0.02500, 0.03400, 0.04100 | 0.02800, 0.04100, 0.05400 |
| F33 | 0.00400, 0.00600, 0.00800 | 0.00300, 0.00400, 0.00600 | 0.00400, 0.00600, 0.00800 | 0.00300, 0.00400, 0.00600 | 0.00900, 0.01400, 0.02000 | 0.02500, 0.03400, 0.04100 | 0.02800, 0.04100, 0.05400 |
| F41 | 0.00000, 0.00100, 0.00300 | 0.00000, 0.00200, 0.00300 | 0.00000, 0.00100, 0.00300 | 0.00000, 0.00200, 0.00300 | 0.00900, 0.01400, 0.02000 | 0.00300, 0.01000, 0.01900 | 0.00400, 0.01500, 0.02800 |
| F42 | 0.00400, 0.00600, 0.00800 | 0.00300, 0.00400, 0.00600 | 0.00900, 0.01400, 0.02000 | 0.02500, 0.03400, 0.04100 | 0.02800, 0.04100, 0.05400 | 0.03100, 0.04000, 0.04400 | 0.05900, 0.06600, 0.06600 |
| F43 | 0.00000, 0.00100, 0.00300 | 0.00000, 0.00200, 0.00300 | 0.00400, 0.00600, 0.00800 | 0.00300, 0.00400, 0.00600 | 0.00900, 0.01400, 0.02000 | 0.02500, 0.03400, 0.04100 | 0.02800, 0.04100, 0.05400 |
| F44 | 0.00100, 0.00300, 0.00500 | 0.00000, 0.00000, 0.00100 | 0.00000, 0.00100, 0.00300 | 0.00000, 0.00200, 0.00300 | 0.00900, 0.01400, 0.02000 | 0.00300, 0.01000, 0.01900 | 0.00400, 0.01500, 0.02800 |
| F51 | 0.00400, 0.00600, 0.00800 | 0.00300, 0.00400, 0.00600 | 0.00900, 0.01400, 0.02000 | 0.02500, 0.03400, 0.04100 | 0.02800, 0.04100, 0.05400 | 0.03100, 0.04000, 0.04400 | 0.05900, 0.06600, 0.06600 |
| F52 | 0.00000, 0.00100, 0.00300 | 0.00000, 0.00200, 0.00300 | 0.00400, 0.00600, 0.00800 | 0.00300, 0.00400, 0.00600 | 0.00900, 0.01400, 0.02000 | 0.02500, 0.03400, 0.04100 | 0.02800, 0.04100, 0.05400 |
| F53 | 0.00100, 0.00300, 0.00500 | 0.00000, 0.00000, 0.00100 | 0.00000, 0.00100, 0.00300 | 0.00000, 0.00200, 0.00300 | 0.00900, 0.01400, 0.02000 | 0.00300, 0.01000, 0.01900 | 0.00400, 0.01500, 0.02800 |

For calculating the normalized values and various other computational outcomes, the authors performed the gap degree analysis of evaluated numerical values to test which alternative's performance was the highest and which one's was the lowest. The assessed outcomes are discussed in the following Table 19 and Fig. 3. The evaluated results from the fuzzy TOPSIS approach corroborate that the results are totally verified and fairly accurate.

### *4.2 Comparison with the Classical Approach*

Establishing the validity of the results is always a key point in any type of computational approach [32–36]. For affirming the accuracy and reliability of any methodology, comparison analysis is the most apt methodology. In this study, the comparison was performed with four other similar techniques that are described below in Table 20 and Fig. 4. All these approaches are similar to the selected one and were performed on the same alternatives for better understanding. The coefficient gap value in all these techniques is 0.7681. After a thorough analysis of the evaluated comparison analysis result, it is clear that the adopted methodology has a more effective outcome than the other selected approaches. The performance of the alternatives in the selected approach is better than the other techniques.

**Table 19:** Closeness coefficients of the selected alternative

| Alternatives | Di− | Di+ | Satisfaction degree of CCi |
|---|---|---|---|
| A1 | 0.74124551 | 29.12855649 | 0.0201212234 |
| A2 | 0.73451245 | 29.48545797 | 0.0210341247 |
| A3 | 0.65454679 | 29.14445233 | 0.0244456458 |
| A4 | 0.70464575 | 29.04576541 | 0.0265596879 |
| A5 | 0.71585467 | 29.05794652 | 0.0254452158 |
| A6 | 0.66522543 | 29.54546794 | 0.0235546575 |
| A7 | 0.65854477 | 29.24457645 | 0.0254475799 |

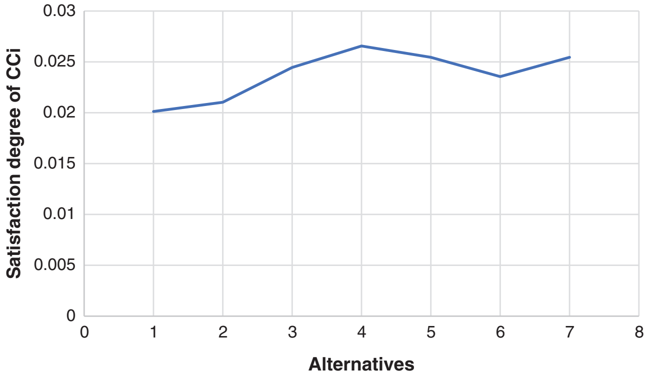

**Figure 3:** Graphical representation of the satisfaction degrees

**Table 20:** Comparison analysis

| Alternatives | Fuzzy AHP-TOPSIS method | Classical AHP-TOPSIS method | Fuzzy ANP-TOPSIS method | Classical ANP-TOPSIS method | Fuzzy weighted method |
|---|---|---|---|---|---|
| A1 | 0.0201212234 | 0.0201215542 | 0.0201211474 | 0.0201203214 | 0.0201255654 |
| A2 | 0.0210341247 | 0.0210745441 | 0.0210344412 | 0.0211121477 | 0.0210345245 |
| A3 | 0.0244456458 | 0.0244411425 | 0.0244451234 | 0.0244465587 | 0.0244445474 |
| A4 | 0.0265596879 | 0.0265574411 | 0.0265595625 | 0.0265574583 | 0.0265602577 |
| A5 | 0.0254452158 | 0.0254411421 | 0.0254444547 | 0.0254474574 | 0.0254451247 |
| A6 | 0.0235546575 | 0.0235512345 | 0.0235547459 | 0.0235544598 | 0.0235501147 |
| A7 | 0.0254475799 | 0.02544445778 | 0.0254474574 | 0.0254454244 | 0.0254445464 |

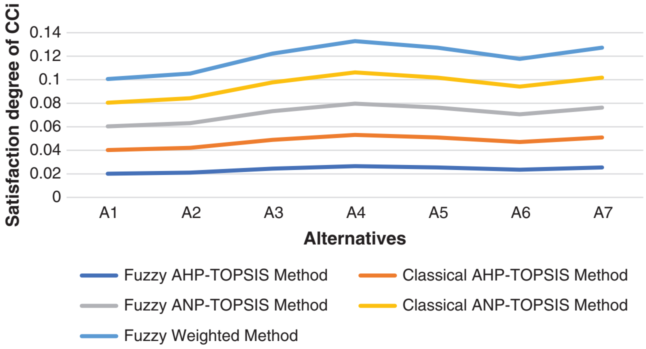

**Figure 4:** Graphical representation of the comparative results

## 5 Discussion

The concept of structural security management was first developed in 2017 [11]. However, even after many years of this concept, the challenges and issues of creating design-based security are still the same and even more complex due to the software's large-scale production and application [37–42]. The application of AHP and TOPSIS in the proposed scheme has significant implications beyond this research. Many authors have applied these methodologies in the context of Software Defined Networks (SDN) [43–45] and various related areas. Securing the data in the software and ensuring that the application is always sustainable continue to be formidable challenges for developers. In such a scenario, the best recourse is the suggested mechanism in this study for producing effective solutions. Several obstacles in achieving quantum-level security for IoT were identified in our research. Because quantum hardware is continually changing, one major problem is integrating quantum innovations with existing IoT infrastructures. To solve this, we concentrated on developing adaptive security frameworks that can handle evolving quantum technology. Another issue is the possible overhead of quantum encryption and computation. We overcame this by investigating hybrid techniques that efficiently exploit classical and quantum resources. Furthermore, quantum-resistant algorithms are still being developed, and the switch to these algorithms can be difficult. To ensure a gradual transition, our research suggests a staged method that incorporates both current and quantum-resistant technology. These solutions allow us to address the issues posed by quantum computing while also capitalizing on its tremendous potential for improving IoT security. The proposed study adopted a computational mechanism for assessing possible significant tactics that can make any software secure. These tactics and their evaluation through the adopted computational methodology will help the developers understand and use the evaluated results as an example. Moreover, the proposed mechanism would prove to be one of the essential practices for achieving the desired level of security in a quantum computing system. The significant contributions of this study can be thusly summarized as follows:

- It is always more effective to perform a numerical analysis of any situation instead of understanding it through a theoretical background.
- The proposed study undertook a unique and effective quantitative analysis of security tactics through a computational approach that was developed by the quantum computing technique.
- The domains or tactics selected in this study are effective and would be useful for secure web application development.

- The systematic pathway proposed in the study can be employed by the developers to produce effective security in web applications.
- The results of this study show that confidentiality is one of the most effective security tactics among all the ones selected.

The pros and cons of this study may be listed as:

### 5.1 *Pros*

Using security tactics for security management by associating a computational approach is a highly feasible, economically viable, and workable methodology for security designers working at any stage of security design. The prioritized scheme of security tactics in this study is an effective example to be alluded to during development.

### 5.2 *Cons*

There is a need to focus on more security tactics. Further, the source of information used in this study is limited; there is scope for accessing different resources related to information about security tactics.

Proactive strategies are required to ensure the long-term security and robustness of IoT ecosystems against quantum-level threats. To begin, ongoing collaboration among quantum researchers, IoT practitioners, as well as regulators is required to develop and update security standards that include quantum-resistant solutions. Furthermore, investment in post-quantum cryptographic algorithm advancement and research should be prioritized to effectively defeat emerging quantum threats. Furthermore, hybrid security systems that include classical and quantum algorithms can achieve a balance between IoT device security and resource constraints. Putting in place real-time monitoring as well as anomaly detection techniques can help discover quantum-based threats quickly. Also, training IoT stakeholders about quantum hazards and responses can help to create a more secure environment. Finally, incorporating quantum-safe hardware components can improve IoT devices' inherent resistance to quantum attacks. By implementing these recommendations, the IoT ecosystem will be able to navigate the quantum terrain while maintaining security and resilience when confronted with growing problems.

## 6 Conclusions

Security management is a challenging context that demands structural security. To address this query, the authors categorized various tactics related to security and then assessed their efficiency at the quantum level by review analysis and tree structure creation. The study also performed a computational and quantitative analysis of security tactic mechanisms. The MCDM approach named fuzzy-AHP-TOPSIS was adopted for this intent. The evaluated results were tested and established as effective. Moreover, the study undertook a comparative analysis and proved that the selected approach in this study was the most effective one. For future investigations in the same league, the authors propose elaborating on the security tactics more deeply and selecting the second-level security tactics for more affirmative outcomes. We recognize that future advances in quantum technology will have a substantial influence on the security environment of IoT systems. Quantum computers have the capability of breaking traditional encryption systems, rendering present security measures obsolete. Our proposed security methods, on the other hand, may adapt dynamically. We advocate for the development of quantum-resistant algorithms capable of withstanding attacks from powerful quantum computers. Our hierarchical model and MCDM-fuzzy technique are also adaptable to developing quantum technologies. We can ensure that our security procedures stay successful in the face of shifting threats by continuously upgrading the model with the most recent quantum capabilities and weaknesses. Thus, our research presents a flexible framework that may expand in tandem with quantum advancements, ensuring the security and privacy of IoT devices. The finding provides the foundation for several intriguing potential fields of research in the field of quantum-level security for IoT. The incorporation of quantum security measures into current IoT systems could be the subject of research to promote seamless compatibility. Exploring machine learning as well as AI-driven techniques to anticipate and stop quantum-based attacks has possibilities. Strong quantum security regulations and standards can be developed through cooperative efforts involving academia, industry, as well as policymakers. The future scope intends to secure the robustness and dependability of IoT systems against the changing landscape of quantum risks by pursuing research in these domains.

**Acknowledgement:** None.

**Funding Statement:** The author received no specific funding for this study.

**Author Contributions:** Study conception and design: H. Alhakami; data collection: H. Alhakami; analysis and interpretation of results: H. Alhakami; draft manuscript preparation: H. Alhakami. Author reviewed the results and approved the final version of the manuscript.

**Availability of Data and Materials:** The author confirms that the data supporting the findings of this study are available within the article.

**Conflicts of Interest:** The author declares that he has no conflicts of interest to report regarding the present study.

## References

[1] A. Lohachab, A. Lohachab and A. Jangra, "A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum IoT networks," *Internet of Things*, vol. 9, no. 1, pp. 100174, 2020.

[2] L. Zhao, "Privacy-preserving distributed analytics in fog-enabled IOT systems," *Sensors*, vol. 20, no. 6, pp. 1–21, 2020.

[3] K. Xue, J. Hong, Y. Ma, D. S. L. Wei, P. Hong *et al.,* "Fog-aided verifiable privacy preserving access control for latency-sensitive data sharing in vehicular cloud computing," *IEEE Network*, vol. 32, no. 3, pp. 7–13, 2018.

[4] H. Wang, Z. Wang and J. D. Ferrer, "Anonymous and secure aggregation scheme in fog-based public cloud computing," *Future Generation Computer Systems*, vol. 78, no. 5, pp. 712–719, 2018.

[5] R. Lu, K. Heung, A. H. Lashkari and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing enhanced IoT," *IEEE Access*, vol. 5, no. 8, pp. 3302–3312, 2017.

[6] A. Rauf, R. A. Shaikh and A. Shah, "Security and privacy for IoT and fog computing paradigm," *Learning and Technology Journal*, vol. 1, no. 6, pp. 96–101, 2018.

[7] S. A. Soleymani, A. H. Abdullah, M. Zareei, M. H. Anisi, C. V. Rosales *et al.,* "A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing," *IEEE Access*, vol. 5, no. 6, pp. 15619–15629, 2017.

[8] T. D. Dang and D. Hoang, "A data protection model for fog computing," in *Proc. of the 2017 Second Int. Conf. on Fog and Mobile Edge Computing*, Valencia, Spain, pp. 32–38, 2017.

[9] M. Wazid, A. K. Das, N. Kumar and A. V. Vasilakos, “Design of secure key management and user authentication scheme for fog computing services,” *Future Generation Computer Systems*, vol. 91, no. 8, pp. 475–492, 2019.

[10] C. Dsouza, G. J. Ahn and M. Taguinod, “Policy-driven security management for fog computing: Preliminary framework and a case study,” in *Proc. of the 2014 IEEE 15th Int. Conf. on Information Reuse and Integration*, Redwood City, CA, USA, pp. 16–23, 2014.

[11] P. Zhang, Z. Chen, J. K. Liu, K. Liang and H. Liu, “An efficient access control scheme with outsourcing capability and attribute update for fog computing,” *Future Generation Computer Systems*, vol. 78, pp. 753–762, 2018.

[12] K. Vohra and M. Dave, “Multi-authority attribute-based data access control in fog computing,” *Procedia Computer Science*, vol. 132, no. 8, pp. 1449–1457, 2018.

[13] M. Xiao, J. Zhou, X. Liu and M. Jiang, “A hybrid scheme for fine-grained search and access authorization in fog computing environment,” *Sensors*, vol. 17, no. 6, pp. 1423–1433, 2017.

[14] I. Stojmenovic, S. Wen, X. Huang and H. Luan, “An overview of fog computing and its security issues,” *Concurrency and Computation: Practice and Experience*, vol. 28, no. 10, pp. 2991–3005, 2016.

[15] S. Homayoun, A. Dehghantanha, M. Ahmadzadeh, S. Hashemi, R. Khayami *et al.,* “DRTHIS Deep ransomware threat hunting and intelligence system at the fog layer,” *Future Generation Computer Systems*, vol. 90, no. 1, pp. 94–104, 2019.

[16] U. Awan, L. Hannola, A. Tandon, R. K. Goyal and A. Dhir, “Quantum computing challenges in the software industry. A fuzzy AHP-based approach,” *Information and Software Technology*, vol. 147, no. 1, pp. 106896, 2022.

[17] L. Malina, P. Dzurenda, S. Ricci, J. Hajny, G. Srivastava *et al.,* “Post-quantum era privacy protection for intelligent infrastructures,” *IEEE Access*, vol. 9, no. 1, pp. 36038–36077, 2021.

[18] M. Schöffel, F. Lauer, C. C. Rheinländer and N. When, “Secure IoT in the era of quantum computers—Where are the bottlenecks?,” *Sensors*, vol. 22, no. 7, pp. 2484, 2022.

[19] B. A. Mozzaquatro, C. Agostinho, D. Goncalves, J. Martins and R. J. Goncalves, “An ontology-based cybersecurity framework for the Internet of Things,” *Sensors*, vol. 18, no. 9, pp. 1–21, 2018.

[20] O. D. Okey, S. S. Maidin, R. Lopes Rosa, W. T. Toor, D. Carrillo Melgarejo *et al.,* “Quantum key distribution protocol selector based on machine learning for next-generation networks,” *Sustainability*, vol. 14, no. 23, pp. 15901, 2022.

[21] V. Chamola, A. Jolfaei, V. Chanana, P. Parashari and V. Hassija, “Information security in the post quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography,” *Computer Communications*, vol. 176, no. 1, pp. 99–118, 2021.

[22] F. Raheman, T. Bhagat, B. Vermeulen and P. van Daele, “Will zero vulnerability computing (ZVC) ever be possible? Testing the hypothesis,” *Future Internet*, vol. 14, no. 8, pp. 238, 2022.

[23] A. Attaallah, M. Ahmad, M. T. J. Ansari, A. K. Pandey, R. Kumar *et al.,* “Device security assessment of Internet of Healthcare Things,” *Intelligent Automation & Soft Computing*, vol. 27, no. 2, pp. 593–603, 2021.

[24] I. Indu, P. R. Anand and V. Bhaskar, “Identity and access management in cloud environment: Mechanisms and challenges,” *Engineering Science and Technology, an International Journal*, vol. 21, no. 4, pp. 574–588, 2018.

[25] M. T. J. Ansari, D. Pandey and M. Alenezi, “STORE: Security threat oriented requirements engineering methodology,” *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 2, pp. 191–203, 2022.

[26] C. Braghin, M. Lilli and E. Riccobene, “A model-based approach for vulnerability analysis of IoT security protocols: The Z-Wave case study,” *Computers & Security*, vol. 127, no. 1, pp. 103037, 2023.

[27] R. Kumar, M. T. J. Ansari, A. Baz, H. Alhakami, A. Agrawal *et al.,* “A multi-perspective benchmarking framework for estimating usable-security of hospital management system software based on fuzzy logic, ANP and TOPSIS methods,” *KSII Transactions on Internet and Information Systems*, vol. 15, no. 1, pp. 240–263, 2021.

[28] R. Mai and M. Wu, "Using information technology to quantitatively evaluate and prevent cybersecurity threats in a hierarchical manner," *International Journal for Applied Information Management*, vol. 3, no. 1, pp. 01–10, 2023.

[29] J. García-Rodríguez and A. Skarmeta, "A privacy-preserving attribute-based framework for IoT identity lifecycle management," *Computer Networks*, vol. 236, no. 1, pp. 110039, 2023.

[30] C. Steglich, S. Marczak, R. P. dos Santos, L. Guerra, L. Mosmann *et al.,* "Factors that affect developers' decision to participate in a mobile software ecosystem," *Journal of Systems and Software*, vol. 205, no. 1, pp. 111808, 2023.

[31] P. A. Thomas and K. Preetha Mathew, "A broad review on non-intrusive active user authentication in biometrics," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 1, pp. 339–360, 2023.

[32] F. Al-Mudaires, A. Al-Samawi, A. Aljughaiman and L. Nissirat, "Information security risk management framework for a governmental educational institute," *Journal of Information and Knowledge Management (JIKM)*, vol. 13, no. 1, pp. 36–54, 2023.

[33] H. M. Alshahrani, S. S. Alotaibi, M. T. J. Ansari, M. M. Asiri, A. Agrawal *et al.,* "Analysis and ranking of IT risk factors using fuzzy TOPSIS-based approach," *Applied Sciences*, vol. 12, no. 12, pp. 5911, 2022.

[34] V. Vasani, A. K. Bairwa, S. Joshi, A. Pljonkin, M. Kaur *et al.,* "Comprehensive analysis of advanced techniques and vital tools for detecting malware intrusion," *Electronics*, vol. 12, no. 20, pp. 4299, 2023.

[35] Q. Fang, D. Castro-Lacouture and C. Li, "Smart safety: Big data-enabled system for analysis and management of unsafe behavior by construction workers," *Journal of Management in Engineering*, vol. 40, no. 1, pp. 04023053, 2024.

[36] A. M. Basahel, M. Yamin, S. M. Basahel and E. L. Lydia, "Enhanced coyote optimization with deep learning based cloud-intrusion detection system," *Computers, Materials & Continua*, vol. 74, no. 2, pp. 4319–4336, 2023.

[37] A. El-Sayed and F. Ibrahim, "Comparative study of blockchain-based approaches for securing Internet of Things (IoT) devices," *Journal of Intelligent Connectivity and Emerging Technologies*, vol. 8, no. 3, pp. 72–93, 2023.

[38] A. G. Bonorino, M. Ndiaye and C. DeCusatis, "Near term hybrid quantum computing solution to the matrix riccati equations," *Journal of Quantum Computing*, vol. 4, no. 3, pp. 135–146, 2022.

[39] A. Alharbi, M. T. J. Ansari, W. Alosaimi, H. Alyami, M. Alshammari *et al.,* "An empirical investigation to understand the issues of distributed software testing amid COVID-19 pandemic," *Processes*, vol. 10, no. 5, pp. 838, 2022.

[40] I. Cvitić, D. Peraković, M. Periša and B. Gupta, "Ensemble machine learning approach for classification of IoT devices in smart home," *International Journal of Machine Learning and Cybernetics*, vol. 12, no. 11, pp. 3179–3202, 2021.

[41] A. Al-Qerem, M. Alauthman, A. Almomani and B. B. Gupta, "IoT transaction processing through cooperative concurrency control on fog-cloud computing environment," *Soft Computing*, vol. 24, pp. 5695–5711, 2020.

[42] C. Wang, T. Nguyen and T. Dang, "Two-stage fuzzy mcdm for green supplier selection in steel industry," *Intelligent Automation & Soft Computing*, vol. 33, no. 2, pp. 1245–1260, 2022.

[43] F. Alassery, A. Alzahrani, A. Irshad Khan, A. Khan, M. Nadeem *et al.,* "Quantitative evaluation of mental-health in type-2 diabetes patients through computational model," *Intelligent Automation & Soft Computing*, vol. 32, no. 3, pp. 1701–1715, 2022.

[44] S. Hwang, J. Kim, H. Kim, H. Kim and Y. Kim, "Suggestion of maintenance criteria for electric railroad facilities based on fuzzy topsis," *Computers, Materials & Continua*, vol. 70, no. 3, pp. 5453–5466, 2022.

[45] A. Tariq, I. Ud din, R. Asif Rehman and B. Kim, "An intelligent forwarding strategy in SDN-enabled named-data IoV," *Computers, Materials & Continua*, vol. 69, no. 3, pp. 2949–2966, 2021.