

Security Vulnerabilities in Quantum Cloud Systems: A Survey on Emerging Threats

Justin Coupel, Tasnuva Farheen
Division of Computer Science, Louisiana State University

Abstract—Quantum computing is becoming increasingly widespread due to the potential and capabilities to solve complex problems beyond the scope of classical computers. As Quantum Cloud services are adopted by businesses and research groups, they allow for greater progress and application in many fields. However, the inherent vulnerabilities of these environments pose significant security concerns. This survey delivers a comprehensive analysis of the security challenges that emerged in quantum cloud systems, with a distinct focus on multi-tenant vulnerabilities and the classical-quantum interface. Key threats such as crosstalk attacks, quantum-specific side-channel vulnerabilities, and insider threats are all examined, as well as their effects on the confidentiality, integrity, and availability of quantum circuits. The design and implementation of various quantum architectures from quantum cloud providers are also discussed. In addition, this paper delves into emerging quantum security solutions and best practices to mitigate these risks. This survey offers insights into current research gaps and proposes future directions for secure and resilient quantum cloud infrastructures.

Index Terms—Quantum computing, quantum cloud, quantum security, NISQ, multi-tenancy, privacy risks, crosstalk, quantum architecture, classical-quantum interface

I. INTRODUCTION

Quantum computing has emerged as a revolutionary technology capable of solving complex problems beyond the realm of classical computers with its exponentially increased efficiency. There are new advances in research for multiple aspects of the field, such as quantum algorithms, security measures, and vulnerabilities in quantum systems. At the same time, hardware is improving with an increasing number of qubits in modern quantum processors. Many industries are exploring the potential applications of quantum computing in fields such as cryptography, medical research, and artificial intelligence, making it a key player in the future of scientific and technological innovation.

In recent years, the ability to experiment with quantum hardware has become more accessible than ever. Cloud computing has become the backbone of modern digital services, offering scalable computing resources, storage, and specialized platforms to fit the needs of researchers and enterprises. There are many quantum platform providers such as IBM Quantum, Google, D-Wave, IonQ, Rigetti, and others that provide cloud-based access to quantum computers [1]. These platforms enable developers to experiment with quantum processors remotely, reducing the need for costly on-premises infrastructure. Quantum cloud services provide users with various tools, including quantum simulators, software develop-

ment kits (SDKs), development environments, and algorithm libraries, which facilitate experimentation and innovation [2].

There are many types of known threats posed by quantum cloud systems, ranging from vulnerabilities in quantum hardware, classical components of these systems, the quantum-classical interface, or, specifically, in multi-tenant environments. The confidentiality, integrity, and availability of quantum cloud systems can all be targeted as a result of these attacks. Threat actors could exploit vulnerabilities to gain unauthorized access, perform side-channel attacks, reduce availability through denial-of-service (DoS) attacks, or manipulate quantum computations. The consequences of attacking these systems could lead to data breaches and intellectual property theft. One threat to the classical-quantum interface is that of insiders who have access to room-temperature electronics. Through side-channel leakage, this attack could potentially decode internal signals [3]. Thus, it is important to be aware of all the vulnerabilities in quantum cloud systems, especially those that are emerging and receive less coverage, such as multi-tenancy.

Multi-tenancy is a core feature of cloud platforms, allowing several users to simultaneously share the same physical or virtual resources for testing on quantum computers. This design gives cloud providers lower costs for both hardware and software, as well as optimization of performance [4]. Although this widespread access to quantum resources promotes increased research and discoveries, it can have the disadvantage of introducing new problems that are not present in restricted single-user platforms. A bug in software or hardware activated by one user would negatively impact the experience of other users sharing quantum hardware [5]. Consequently, a threat actor can introduce many unique security risks to these shared environments, which could affect many unknowing users through various means.

Weak security in a multi-tenant quantum cloud environment can have severe implications. It includes many threats that single-tenant systems are exposed to, as well as its own problems. Many side-channel attacks can easily predict the circuits of users with increasingly limited knowledge and are challenging to defend under this system. Adversaries can detect crosstalk and timing patterns in these shared systems and utilize them for exploits. An example in which malicious actors can initiate attacks that utilize crosstalk in NISQ computers can result in circuit discovery [6]. Therefore, it is critical to ensure that robust security measures are in place to prevent such risks and protect sensitive quantum workloads, especially

for research in crucial sectors such as medicine and finance.

Previous research has covered the concept of multi-tenancy in quantum computing and how this system can be exploited [7]. There are many different proposed side-channel exploits that utilize various different methods. Research has also touched on threat vectors in the classical quantum interface and other attack types in quantum cloud systems [3]. Additionally, there are proposals for mitigation techniques that can reduce the risk of data breaches under multi-tenant and single-tenant frameworks. However, there is still a lot of room for more research into the specific challenges and vulnerabilities posed by multi-tenancy, the classical-quantum interface, and the specific solutions to these issues.

Key gaps that this survey paper addresses include the concise organization of many of the new vulnerabilities and solutions proposed by recent and ongoing research. There is also a lack of visual representations that can break down many complex systems like the architectures of quantum hardware, quantum cloud providers, the classical-quantum interface, and the multi-tenant model. Furthermore, research gaps and challenges are also presented to accomplish in the future, emphasizing vulnerability assessment of the exploits on other quantum hardware and creating secure solutions of the existing attack vectors. On the part of the cloud providers, monitoring and auditing mechanisms for quantum workloads are essential to ensure the integrity and confidentiality of computations. There is also room for more research on quantum-safe cryptographic algorithms that ensure data protection in multi-tenant quantum cloud systems to bolster its security [8].

Contributions: The main contributions of this paper are described below:

- 1) We present a comprehensive yet concise survey focusing on the security threats in quantum cloud systems and their effects on the confidentiality, integrity, and availability of a user's circuit.
- 2) We discuss many different attack vectors on these cloud systems, from the classical-quantum interface, single-tenant threats, multi-tenant threats, insider attacks, quantum hardware attacks, and classical component attacks in quantum devices.
- 3) We describe the architecture of a quantum computer and its hardware from a high level with aid from visuals.
- 4) We discuss many proposed mitigation strategies and secure solutions in terms of their effectiveness in reducing threats and their feasibility.
- 5) We highlight different areas that could require further research and proposals on improving the security in quantum cloud systems.

II. RELATED WORKS

This section highlights key references and prior research that have contributed to the understanding of quantum computers and the security threats in multi-tenant quantum cloud environments. The table I includes survey papers on quantum cloud security and multi-tenant systems. In addition, this section

explores ongoing research on new security threats, exploits, and mitigation strategies for these vulnerabilities.

A. Quantum Cloud Research

Here, we examine previous works on cloud-based infrastructures developed by major service providers. There have been works describing the structure of Quantum Computing as a Service (QCaaS), with the design and implementation that quantum platform providers use [9]. There has also been progress in surveying distributed quantum computing NISQ systems and how quantum computers operate in this environment [10]. Research on a comparison between the major platform providers including IBM Quantum, Google Quantum AI, Azure Quantum, and Amazon Bracket has also been discussed using the Traveling Salesman Problem [11].

B. Security Threats Papers

In this section, we cover many side-channel attacks that affect superconducting quantum computers. The following paper includes some single-tenant and multi-tenant threats ranging from power-based attacks, timing-based attacks, fault injections, and crosstalk exploits [7]. There is also research in power-based side-channel vulnerabilities in quantum computer controllers so this topic will not be focused on this paper [15]. Additionally, there is much coverage on specific quantum hardware issues and how machine learning (ML) can potentially be used to help mitigate these threats [16]. The impact of ML on quantum security is heavily researched on with discussions relating to quantum defenses like adversarial training, data privacy, and formal verification methods in this paper [17]. In addition, the classical-quantum interface is vulnerable to attacks especially by knowledgeable insiders who can analyze information on user circuits through passive monitoring on SFQ chips [3]. There are also proposed attack vectors of reverse engineering SFQ chips to recover circuits [18]. Overall, this topic has much less research, so it will be covered more extensively later.

C. Multi-Tenancy Research

Numerous works have been published on the usage of multi-tenancy in the classical realm, exploring its structure and vulnerabilities [12]. However, research on multi-tenancy in the quantum cloud is much more limited and typically focuses on analyzing the threats that it creates. There have been several proposed attacks against multi-tenant quantum platforms to discover information about the circuits of other users. The crosstalk created by NISQ multi-tenant computers has been shown to help extract unauthorized information on the victim's circuit by determining the number of CNOT gates in a quantum computer [6]. This prior paper also introduces a framework for a side-channel attack utilizing this crosstalk in NISQ systems with the aid of a graph-based model. However, crosstalk has been implemented for several side-channel attacks with the ultimate goal of rebuilding a quantum circuit that should have remained confidential. It has been a known exploit for some time, with multiple

TABLE I: Summary of Notable Research on Quantum Computing Security and Multi-Tenancy

Notable Research Work	Paper Coverage
Side-channel Attacks Targeting Classical-Quantum Interface in Quantum Computers [3]	Explains many different attack vectors that affect the classical-quantum interface on quantum hardware, mainly focusing on insider threat potential.
Crosstalk-induced Side Channel Threats in Multi-Tenant NISQ Computers [6]	Proposes crosstalk attack on multi-tenant systems to recover circuit information from victims in order to fully reproduce circuits using limited initial knowledge.
Securing the Cloud Infrastructure: Investigating Multi-tenancy Challenges, Modern Solutions and Future Research Opportunities [7]	A broad survey paper that discusses the development of various solutions to combat the many threats multi-tenancy poses. It suggests encryptions, anti-virus, and more.
A reference architecture for quantum computing as a service [8]	Describes Quantum Computing as a Service and the design decisions that platform providers make and implement.
Distributed quantum computing: a survey [9]	Explains how distributed quantum computing systems operate in NISQ environments.
Technological diversity of quantum computing providers: a comparative study and a proposal for API Gateway integration [10]	Extensive research on the common quantum platform providers and comparing them based on performance, hardware used, and pricing.
A survey of side-channel attacks in superconducting quantum computers [11]	Delivers information on many different side-channel exploits for single-tenant and multi-tenant quantum systems on the cloud with crosstalk, time-based attacks, fault injections, and power-based attacks.
Multi-Tenancy in Cloud Computing [12]	Provides information on multi-tenancy in the classical sphere and its impact overall in cloud computing. It can shed light to similar concepts applied to quantum platforms.
Quantum leak: Timing side-channel attacks on cloud-based quantum services [13]	Discusses several timing-based side-channel attacks on the quantum cloud to identify circuit information and unique quantum hardware.
Detecting fraudulent services on quantum cloud platforms via dynamic fingerprinting [13]	Proposes the idea that quantum platform providers switch the hardware users connect to without their permission and creates a method to detect these switches.
Enhancing security and privacy in advanced computing systems: A comprehensive analysis [14]	Examines several different security and privacy defense mechanisms to improve security and quantum systems such as data at rest encryption.

sources mentioning threats it may pose. There is another side-channel attack that can inflict potentially major disruptions on victim circuits using the SWAP path in active or passive attacks [19]. This attack, also taking advantage of the effects of crosstalk, focuses on the availability of quantum computers and emphasizes how devastating a disruption can be, reducing user output accuracy by intentionally positioning qubits. Side-channel attacks on quantum controllers on a NISQ quantum computing platform have also led to quantum circuit reconstruction [20]. Furthermore, timing-based side-channel attacks have been used on quantum cloud-based services to identify an individual quantum computer that executed a circuit with 10 measurements [13]. All of these attacks highlight the need for added protections and security measures that cloud providers must have to ensure the confidentiality, integrity, and availability of quantum circuits.

D. Privacy and Authenticity Concerns

Privacy can be a great concern for quantum systems with malicious actors having the ability to extract circuit information of users from various attack vectors. There have also been work highlighting some secretive measures quantum platform providers use which raise authenticity concerns. Fingerprinting methods have been tested on the trustworthiness of providers, which are accused of switching computers that

a user originally selects to save costs and increase efficiency on their platforms [21]. This study used a controlled test to detect fraudulent services using a comparison of user-side and device-side fingerprints to determine the authenticity of a given computer.

E. Classical-Quantum Interface Solutions

There have been a few proposed solutions to mitigate risks to the classical-quantum interface. One security measure uses camouflaging on rapid SQF circuits to prevent reverse engineering and has shown to greatly reduce exposure [18]. Another method uses logic locking to prevent outside attackers from being able to analyze the structural behavior of a circuit [22]. In addition, there is research on using entropy-based measures to detect any threats to the integrity of quantum systems [23].

F. Multi-Tenant Solutions

The final subsection discusses mitigation strategies aimed at securing multi-tenant quantum cloud environments. While there are some methods to increase security in the quantum cloud, many proposals are still theoretical, are not very practical to implement, or would conflict with the multi-tenancy framework companies have employed. An analysis explores the use of various security mechanisms, such as zero-trust

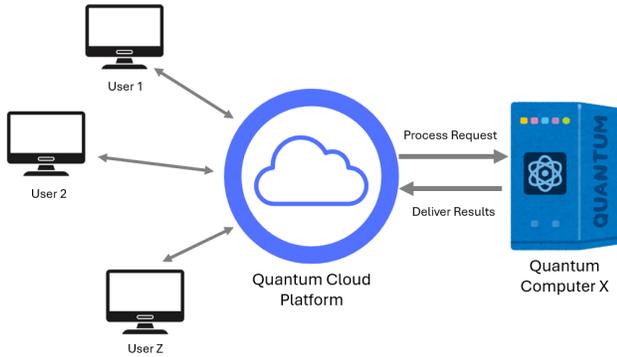


Fig. 1: Model of a Multi-Tenant Quantum Computing Platform on the Cloud

architectures, privacy-enhancing technologies, various encryptions, and access control, with the intention of suggesting secure solutions to eliminate some of the security threats in the quantum cloud. It suggests encryption for data at rest and in transit and stringent access control to help mitigate these problems [14]. One paper suggests the creation of an antivirus that can scan a user’s circuits for malicious patterns to help detect adversaries [24]. However, much more work remains in the development of encryption algorithms and other methods, including an antivirus, to reduce multi-tenant risks [8].

III. QUANTUM ARCHITECTURES

Quantum computers are constantly developing in this new age of progress, and various companies are competing to be the leader of this new movement. Microsoft, for instance, announced that it has developed a type of quantum chip that can help them reach one million qubits [25]. With new advances happening this often, it is important to understand the background and overall design of quantum computers and how they process data. This section will provide an overview of the architecture of quantum computers and the different quantum computing platforms provided by IBM, Google, and others. It will cover the underlying hardware technologies and a high-level description of how these systems operate. It will also provide the rationale for why companies deploy cloud platforms using a multi-tenant framework. In addition, quantum workloads will be described in terms of how they are managed, scheduled, and executed in a cloud environment. The figure 1 provides a general model for the quantum cloud platform and users interaction with it.

A. Background

Quantum computing platforms have been developed and refined by leading technology providers which include IBM, Google, Honeywell, IonQ, Rigetti, and others. Each of them utilize various hardware technologies to power their systems. Quantum computing leverages the principles of quantum mechanics, such as superposition and entanglement, to perform computations that are impossible for classical computers. IBM, Google, and Rigetti predominately rely on superconducting

qubits, which operate at extremely low temperatures close to absolute zero and are sensitive to environmental noise [2]. In contrast, companies such as IonQ and Honeywell use trapped ion technology, which manipulates charged atoms with electromagnetic fields to achieve potentially higher fidelity operations [2]. Understanding the design and functionality of these quantum cloud systems can help many to grasp the security risks of running quantum workloads. For example, the physical requirements of quantum hardware can introduce unique vulnerabilities, especially in the multi-tenant cloud, such as unauthorized interference or data leakage [6].

B. Quantum Cloud Integration

Quantum workloads in a cloud environment follow a specific process for execution. Users submit jobs through cloud-based quantum computing platforms, where they get queued, scheduled, and executed on the quantum hardware they choose [21]. These platforms manage workloads by queuing jobs based on priority, resource availability, and the device the user selected. Security in this multi-tenant setting is critical because data must remain confidential during transmission and execution, protected by protocols such as encryption and authentication mechanisms [6]. However, adequate security in these multi-tenant systems is not yet present due to the many crosstalk timing-based exploits which can put user circuits at risk. Another element that platform providers face is the balance between performance and security. Efficient execution must be balanced with isolation and security of quantum hardware to prevent unauthorized access while still ensuring the performance and low costs to provide quantum computing services.

C. Security Considerations in Architectures

Security is a very important factor in usefulness in an architecture, whether it is classical or quantum. Without security measures, no one would be able to use computers for important tasks such as messaging, data storage, or researching unexplored areas. Classical computers have made great strides over the past few years in improving security, however, quantum computers will make many of these measures irrelevant once it is fully realized. Thus, it is vital to create new security measures for quantum computers. In multi-tenant quantum cloud environments, this feat comes with challenges due to the resource and hardware sharing users face when trying to perform research. The confidentiality of data is currently in question on these systems due to crosstalk exploitations and side-channel attacks. The integrity of data is also at risk from the ability to create noise or alter circuits by positioning qubits. [19] Additionally, the availability of devices is a concern when denial-of-service (DoS) attacks on a quantum computer will affect all users who currently share the device. Therefore, quantum service providers must factor all of these security considerations into their architecture designs to develop safe platforms for quantum development.

IV. PERFORMANCE VS. SECURITY

Quantum cloud platforms like IBM Quantum, Amazon Bracket, and Microsoft Azure Quantum utilize quantum cloud systems to boost accessibility, but this creates a tradeoff between performance and security, especially in a multi-tenant framework. Performance is often throttled by security measures such as advanced encryption schemes, isolation methods, or noise injection. One example, blind quantum computing, protects user data by hiding inputs and outputs from the server. Secure protocols like the one mentioned before introduce significant communication and resource overhead. This will impact performance, leading to slower execution times in modern NISQ systems, where counts of qubits and coherence times are limited [1].

The performance-security gap widens due to vulnerabilities like crosstalk between qubits or denial-of-service (DOS) attacks from miscalibrated qubits, which can disrupt shared resources. To counteract these, providers employ frequent calibrations and robust error correction, but these measures reduce computational efficiency [26]. Blind quantum computing in multi-tenant systems further conflicts with scalability, adding latency to ensure privacy across users [27]. Much research aims to develop protocols that minimize these tradeoffs, striving for a balance that maintains both security and performance in shared quantum cloud environments [1].

V. SECURITY THREAT LANDSCAPE

There are many types of known threats that affect quantum cloud systems, from new vulnerabilities exposed to existing threats that come naturally with these systems. There are also many works reporting on these threats in various survey papers, as well as others. This section is meant to provide references to key papers that already cover several topics of known security issues, as well as to identify what vulnerabilities do not have high-level survey coverage.

A. Previous Survey Coverage

One paper covers many side-channel attacks that affect superconducting quantum computers. This work includes some single-tenant and multi-tenant threats ranging from power-based attacks, timing-based attacks, fault injections, and crosstalk exploits [7]. There is also research on power-based side-channel vulnerabilities in quantum computer controllers, so this topic will not be focused on this paper [15]. Additionally, there is much coverage on specific quantum hardware issues and how machine learning (ML) can potentially be used to help mitigate these threats [16]. The impact of ML on quantum security is heavily researched on with discussions relating to quantum defenses like adversarial training, data privacy, and formal verification methods in this paper [17].

B. Survey and Research Gaps

One gap in the paper on side-channels in superconducting quantum computers [7], is that they did not focus in detail on multi-tenant threats specifically. These issues were not explained comprehensively and did not include some key

new research in exploits. Another paper covers side-channel attacks that target the classical-quantum interface in quantum computers [3]. These threats have limited research coverage, but this paper did well to address many of the vulnerabilities they pose. However, it can be difficult to grasp at a higher level to understand how these threats affect the overall landscape of security threats. These two topics will be the primary focus of this survey paper and how these exploits impact the security threat landscape.

VI. CLASSICAL-QUANTUM INTERFACE THREATS

One important subsystem of a quantum computer is the classical-quantum interface, which refers to the interface between isolated qubits and the classical control or readout technology that is used in operation [28]. Many side-channels that target the classical-quantum interface in quantum computers exploit vulnerabilities in single flux quantum (SFQ) circuits. These circuits are pivotal for refrigerator control and readout due to their high switching frequencies and low energy consumption per switch [3]. The SFQ to DC converter, essential for SFQ interface with CMOS technologies, has been shown to be particularly susceptible to exhibiting significant side-channel leakage [29].

A. Threat Models for Attacks

The threat model for classical-quantum interface attacks typically involves an insider, who has special access to electronics preferably at room temperature and a greater understanding of the system architecture. With this knowledge, the malicious actor can analyze variations in the bias current of SFQ chips to potentially decode internal signals through monitoring [3]. Multiple attacks exploit SFQ-to-DC converter leakage. One exploit decodes control signals for two-qubit (CZ) gates by analyzing the bias current of current generators with 25 converters switching simultaneously [29]. Another attack targets qubit state readout using a Josephson photomultiplier, where an SFQ pulse signals a logical '1', which allows attackers to infer the Hamming weight of the qubit's bit string through bias current measurements [30]. With multi-tenant systems commonly used, the effect of a compromise or information leak increases with more users exposed per quantum system. It is also possible for reverse engineering attempts to occur on circuits by both outside and inside attackers, as discussed in some papers below.

B. Proposed Solutions

All the mentioned vulnerabilities emphasize the importance of improved security to protect scalable quantum systems. One security measure through camouflaging method has been proposed on rapid SFQ circuits to prevent reverse engineering attempts and has shown to greatly reduce the risks of exposure. However, this comes with a performance cost required in delay overhead and power overhead [18]. A method called logic locking has also been proposed to prevent outside attackers from being able to analyze the structural behavior of a design even when a circuit is obtained [22]. The implementation

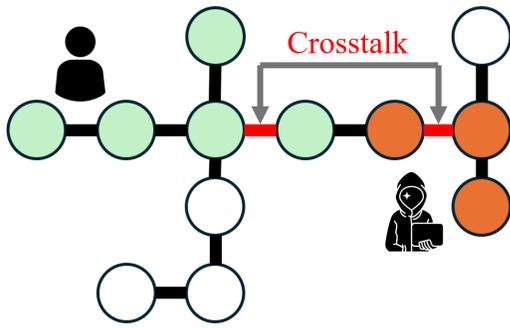


Fig. 2: Crosstalk-Channel Attack on a Quantum System

of this method also requires a reduction in performance to ensure security with the logic locked OR gate used to perform this method requiring 20 percent overhead leading to a 3.6 percent overhead in total. There is also recent research as of this paper’s writing on using entropy-based measures to detect any threats to the integrity of quantum systems [23]. Ongoing research should continue and prioritize developing robust countermeasures, such as improved circuit designs, noise injection techniques, and pursue new methods to secure the classical-quantum interface. There should also be access control measures in place to restrict as many insiders as possible from having the ability to obtain confidential information.

VII. MULTI-TENANCY VULNERABILITIES

Modern quantum computing platforms operate using multi-tenancy, allowing resource sharing among users to optimize usage and save costs. This framework introduces many new vulnerabilities that exploit shared access among several users who want to keep their information confidential. It is very important to acknowledge the security landscape associated with multi-tenancy for researchers and developers who want to create circuits in research fields such as medicine, space applications, secure communications, and many others [31]. This section will explore the various security threats that appear in multi-tenant quantum cloud environments. It will cover crosstalk interference, timing-based side-channels, qubit flipping attacks, and the risks of data leakage. Each threat will be analyzed for its impact on the confidentiality, integrity, and availability of quantum resources.

A. Crosstalk Exploits

Crosstalk is the unwanted effect of interaction between sets of qubits in a quantum computing system. This has the effect of altering or leaking quantum information, thus affecting both integrity and confidentiality [32]. Figure 2 showcases a basic crosstalk attack on a multi-tenant cloud system. One paper describes crosstalk in detail, as well as proposes a side-channel attack that uses it to extract unauthorized information on the victim’s circuit by determining the number of CNOT gates in a quantum computer [6]. The attack framework introduced in this paper impacts the confidentiality and integrity of circuits

of users sharing quantum hardware under a multi-tenant system. However, to perform the attack, the qubit numbers, total CNOT gates per qubit, time distribution of gates, and pairwise CNOT gate counts must be extracted to train their graph-based (GCN) model to accurately identify circuits.

Another paper mentions that information can still be obtained from the effects of crosstalk in a multi-tenant NISQ system that goes under a reset [33]. This side-channel attack occurs because a reset does not fully clear data like a complete system wipe, leaving the potential to acquire leftover information. The author’s threat model requires the attacker to have control over the execution of a victim’s program, use repeat measurements, and be co-located with the target victim. Through eavesdropping via crosstalk, information can be leaked across the reset gates on the same qubit. The paper advocates for the development of more secure resets that do not present this risk to confidentiality. It also acknowledges that full system wipes would solve the issue of data leakage, but it happens at a much slower speed.

B. Timing-based Side-Channels

Timing-based side-channel security exploits take advantage of the timing of computational processes to retrieve sensitive information such as part of a victim’s circuit, keys, or passwords. Malicious actors can accomplish this through timing behavior analysis [7]. These attacks can be dangerous due to their ability to be performed effectively on multi-tenant systems remotely, often in a secretive manner. Timing-based side-channel vulnerabilities have been explored on cloud-based quantum services working on both single-tenant and multi-tenant systems [13]. This research also demonstrates that it is possible to uniquely identify the quantum processor in use with just 10 measurements. The attack primarily targets the confidentiality of information, so it is important for quantum platforms to create mechanisms to keep data secretive.

Another side-channel attack involves timing through measurements before and after an execution of a circuit on IBM’s cloud-based superconducting quantum computers. This exploit was able to achieve 60 percent accuracy to identify circuits on IBM’s publicly available superconducting quantum computers [34]. The attack also exposes a risk to the confidentiality of user circuits on IBM’s platforms and multi-tenant QCaaS platforms as a whole.

C. Qubit Flipping Attacks

There is new research as of writing this paper on qubit flipping attacks that can bypass existing security measures and leak important information. This paper proposes QubitHammer attacks which take advantage of qubit pulses to impact quantum circuits [35]. The paper presented four different attack situations as well as single and repeated attack pulse methods to perform these exploits. Their results conclude that current defense methods are not adequate enough to greatly reduce the risk of crosstalk. With this threat, these types of exploits can negatively affect the integrity of circuits by

TABLE II: Types of threats and their damage possibility stemming from the primary goals of the exploits on multi-tenant quantum cloud systems, focusing on their effects on the CIA Triad (confidentiality, integrity, and availability).

Research Papers	Confidentiality	Integrity	Availability	Threat Level
Crosstalk Side Channels [6]	Yes	Yes		High
Active SWAP Attack [19]		Yes	Yes	Moderate
Passive SWAP Attack [19]	Yes			High
Reset Operation Threats [33]	Yes			Moderate
Reconstructing Circuits [34]	Yes			Moderate
Qubit Flipping Attacks [35]		Yes		High

creating errors or disturbances. The research group claims attack success against existing security measures like dynamical decoupling, disabling qubit 0, crosstalk-aware qubit allocation, and active padding [35]. The primary goal of their work is to demonstrate the need for more effective and secure methods to prevent crosstalk and to stop these vulnerabilities inherent in multi-tenant quantum systems.

D. Proposed Solutions

There are several security solutions proposed to help mitigate risks in multi-tenant quantum cloud systems. One analysis delves into the use of zero-trust architectures, privacy-enhancing technologies, various encryptions, and access control, with the goal of recommending secure solutions to eliminate some of the security threats in the quantum cloud. It also suggests encryption for data at rest and in transit as well as strict access control to help mitigate these threats [14]. Another proposal is for the creation of an antivirus that can scan a user's circuits for malicious patterns to help detect adversaries. This group did not actually create the antivirus, but instead made a theoretical one that could help reduce many threats in the quantum cloud [24]. Other defensive measures (dynamical decoupling, disabling qubit 0, crosstalk-aware qubit allocation, and active padding) were also mentioned in the very recent qubit flipping attack, but were shown to be ineffective [35]. When using multi-tenant cloud systems, the risk of leakage from crosstalk has been clear and still have not had any viable solutions to stop this threat. Many works point to the need for more resources and time to be invested in new solutions to reduce multi-tenant risks [8], [7], [35].

VIII. SECURITY THREAT EVALUATIONS

This portion of the paper reviews the general threats from the domains covered on the classical-quantum interface and multi-tenant systems and evaluates how concerning they should be for quantum platform providers and users. It will judge the overall damage these attacks can inflict, the feasibility of the attacks, and the areas these attacks primarily target. The ability of these attacks to perform against current defensive mechanisms will also be studied and incorporated into the overall risk the exploits pose. The evaluations will also transition into research gaps and challenges that need to be further studied and improved to limit these risks.

A. Classical-Quantum Interface Risks

The attacks present on the classical-quantum interface mainly focus on insider threats who have access to hardware and can make measurements that the majority of users could not. This threat presents less of a risk due to the lack of users who can perform this attack due to the knowledge and location required [3]. The exploits on this interface should not be discounted, however, since they can cause significant information leakage revealing internal signals used to recreate circuits without detection. The best countermeasure for this threat would be access control and least-privilege mechanisms to limit the amount of users who have the capabilities to perform this attack. Another method of promoting information confidentiality would be through camouflaging [18] or logic locking [22], but both of these methods require overhead costs which are not attractive to cloud platform providers. This can lead to a fine line, where providers may not want to create too many secure measures that would reduce performance yet need to help ensure user circuits remain secret to keep their consumers. Overall, the attacks on the classical-quantum interface can deal moderate to significant damage depending on the goals of the adversary, but require a knowledgeable insider with great access to perform them thus making the attack less concerning than others such as multi-tenant threats.

B. Multi-Tenant Threats

Multi-Tenant quantum cloud systems are vulnerable to numerous different exploits which many works have proposed especially in the past few years. This fact is very concerning considering that many quantum platform providers have adopted this system to increase performance and savings. While there have been many different defensive measures proposed by researchers, the crosstalk that is inherently a part of multi-tenant systems can still be used to gain partial information on user circuits [6]. This information is often significant enough to accurately reconstruct the circuits causing a breach in confidentiality of important new work in quantum computing, medicine, or finance [20]. There are also timing-based attacks, power-based attacks, SWAP attacks, and qubit flipping attacks, and others which all go down different avenues to either cause integrity damage to user circuits, by flipping qubits and creating errors, or confidentiality through revealing circuit information. Many of the main multi-tenant attacks are shown in table II with their threat levels and impact on the CIA Triad.

The most ideal solution would be for platform providers to use a different system than the current multi-tenant model that is exposed to these issues, but the costs make that unrealistic for them. Exploits in this area are very important to monitor and a major concern for both providers and users.

IX. RESEARCH GAPS AND CHALLENGES

This section will identify the limitations of current security solutions and outline the unresolved challenges in securing multi-tenant quantum cloud environments. It will also emphasize the need for innovative security models. The roles of regulatory frameworks and the importance of cross-disciplinary collaboration in addressing these challenges will be mentioned.

There are several research gaps for new exploits and secure solutions in the quantum cloud. In terms of the classical-quantum interface, there needs to be more secure measures that have less overhead costs than the existing proposed methods of defense. Quantum platform providers are likely to not focus on security on this front if the cost is too high since it requires an insider with great access to perform. It can also be very difficult to defend an attack against someone with this level of knowledge and capabilities, so measures with significantly positive results will be necessary for these providers to embrace them. There is also limited research on exploits on the interface, so there requires much more research on how much damage can be caused through this attack vector as well as if it is possible for an attack to be done without needing an insider like the one mentioned [3].

There is also a definite need for more research on secure measures to prevent crosstalk exploitation in multi-tenant systems. The new attacks being proposed that utilize crosstalk are able to bypass many existing methods, so new research is needed for circuits on these systems to remain confidential. The qubit flipping attack, QubitHammer, needs to be addressed in particular as it was able to introduce errors and disruptions into quantum systems in multiple different ways against many of the known defenses [35]. Finally, there is also a lack of survey papers that cover the threat landscape that exists in quantum cloud systems that this work aims to contribute to.

X. CONCLUSION

In this paper, we provide a comprehensive survey on the types of threats posing quantum computing cloud platforms. We cover the background of how these platforms operate and the reasoning behind their resource sharing. We discuss previous works breaking down multi-tenancy and the modern QCaaS architecture. We also delve into the security threat landscape behind these modern platforms as well as current proposed solutions to these risks. We focus heavily on describing the threats and solutions for the classical-quantum interface and multi-tenant quantum systems, two topics with limited coverage. A ranking of these exploits affecting the confidentiality, integrity, and availability of users and their ability to access the quantum computers was also used. Finally, new research in proposing solutions to the vulnerabilities and side-channel is encouraged. This paper aims to spread

awareness of the ongoing threats that quantum platforms can face to researchers and developers who want to create innovative applications in a secure environment. Finally, we strive to highlight the need for future research and development of secure access control, encryption algorithms, and least privilege mechanics to address the limitations of these threats. With progress in this area, these gaps can be further addressed to create a secure future for quantum computing.

REFERENCES

- [1] H. T. Nguyen, P. Krishnan, D. Krishnaswamy, M. Usman, and R. Buyya, "Quantum cloud computing: a review, open problems, and future directions," *arXiv preprint arXiv:2404.11420*, 2024.
- [2] P. Singh, R. Dasgupta, A. Singh, H. Pandey, V. Chamola, and B. Sikdar, "A survey on available tools and technologies enabling quantum computing," *IEEE Access*, 2024.
- [3] Y. Mustafa and S. Köse, "Side-channel attacks targeting classical-quantum interface in quantum computers," in *2024 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2024, pp. 1–5.
- [4] W. Su, Q. Liu, C. Lin, and S. Shen, "Modeling and analysis of availability in multi-tenant saas," in *2015 24th International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 2015, pp. 1–8.
- [5] G. Karataş, F. Can, G. Doğan, C. Konca, and A. Akbulut, "Multi-tenant architectures in the cloud: A systematic mapping study," in *2017 International Artificial Intelligence and Data Processing Symposium (IDAP)*. IEEE, 2017, pp. 1–4.
- [6] N. Choudhury, C. N. Mude, S. Das, P. C. Tikkireddi, S. Tannu, and K. Basu, "Crosstalk-induced side channel threats in multi-tenant nisq computers," *arXiv preprint arXiv:2412.10507*, 2024.
- [7] N. Choudhury and K. Basu, "A survey of side-channel attacks in superconducting quantum computers," in *2024 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. IEEE, 2024, pp. 373–378.
- [8] M. A. Hayat, S. Islam, and M. F. Hossain, "Securing the cloud infrastructure: Investigating multi-tenancy challenges, modern solutions and future research opportunities," *ResearchGate*, Aug, 2024.
- [9] A. Ahmad, A. B. Altamimi, and J. Aqib, "A reference architecture for quantum computing as a service," *Journal of King Saud University-Computer and Information Sciences*, vol. 36, no. 6, p. 102094, 2024.
- [10] M. Caleffi, M. Amoretti, D. Ferrari, J. Illiano, A. Manzalini, and A. S. Cacciapuoti, "Distributed quantum computing: a survey," *Computer Networks*, vol. 254, p. 110672, 2024.
- [11] J. Alvarado-Valiente, J. Romero-Álvarez, E. Moguel, J. García-Alonso, and J. M. Murillo, "Technological diversity of quantum computing providers: a comparative study and a proposal for api gateway integration," *Software Quality Journal*, vol. 32, no. 1, pp. 53–73, 2024.
- [12] H. AlJahdali, A. Albatli, P. Garraghan, P. Townend, L. Lau, and J. Xu, "Multi-tenancy in cloud computing," in *2014 IEEE 8th international symposium on service oriented system engineering*. IEEE, 2014, pp. 344–351.
- [13] C. Lu, E. Telang, A. Aysu, and K. Basu, "Quantum leak: Timing side-channel attacks on cloud-based quantum services," *arXiv preprint arXiv:2401.01521*, 2024.
- [14] C. Mendoza, J. Herrera *et al.*, "Enhancing security and privacy in advanced computing systems: A comprehensive analysis," *Journal of Advanced Computing Systems*, vol. 3, no. 12, pp. 1–9, 2023.
- [15] C. Xu, F. Erata, and J. Szefer, "Exploration of power side-channel vulnerabilities in quantum computer controllers," in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, 2023, pp. 579–593.
- [16] N. Karimi, K. Basu, C.-H. Chang, and J. M. Fung, "Hardware security in emerging technologies: Vulnerabilities, attacks, and solutions," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 11, no. 2, pp. 223–227, 2021.
- [17] N. Franco, A. Sakhnenko, L. Stolpmann, D. Thuerck, F. Petsch, A. Rüll, and J. M. Lorenz, "Predominant aspects on security for quantum machine learning: Literature review," in *2024 IEEE International Conference on Quantum Computing and Engineering (QCE)*, vol. 1. IEEE, 2024, pp. 1467–1477.

- [18] H. Kumar, T. Jabbari, G. Krylov, K. Basu, E. G. Friedman, and R. Karri, "Toward increasing the difficulty of reverse engineering of rsfq circuits," *IEEE Transactions on Applied Superconductivity*, vol. 30, no. 3, pp. 1–13, 2019.
- [19] W. J. B. Lee, S. Wang, S. Dutta, W. E. Maouaki, and A. Chattopadhyay, "Swap attack: Stealthy side-channel attack on multi-tenant quantum cloud system," *arXiv preprint arXiv:2502.10115*, 2025.
- [20] F. Erata, C. Xu, R. Piskac, and J. Szefer, "Quantum circuit reconstruction from power side-channel attacks on quantum computer controllers," *arXiv preprint arXiv:2401.15869*, 2024.
- [21] J. Wu, T. Hu, and Q. Li, "Detecting fraudulent services on quantum cloud platforms via dynamic fingerprinting," *arXiv preprint arXiv:2408.11203*, 2024.
- [22] T. Jabbari, Y. Mustafa, E. G. Friedman, and S. Köse, "Hardware security of sfq circuits," in *Design Automation of Quantum Computers*. Springer, 2022, pp. 135–165.
- [23] S. Chehade, J. A. Dawson, S. Prowell, and A. Passian, "Entropy of the quantum-classical interface: A potential metric for security," 2025.
- [24] S. Deshpande, C. Xu, T. Trochatos, Y. Ding, and J. Szefer, "Towards an antivirus for quantum computers," in *2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2022, pp. 37–40.
- [25] Bolgar, "Microsoft's majorana 1 chip carves new path for quantum computing," <https://news.microsoft.com/source/features/innovation/microsofts-majorana-1-chip-carves-new-path-for-quantum-computing/>, 2025, online; accessed 30 March 2025.
- [26] M. Golec, E. S. Hatay, M. Golec, M. Uyar, M. Golec, and S. S. Gill, "Quantum cloud computing: Trends and challenges," *Journal of Economy and Technology*, 2024.
- [27] J. F. Fitzsimons, "Private quantum computation: an introduction to blind quantum computing and related protocols," *npj Quantum Information*, vol. 3, no. 1, p. 23, 2017.
- [28] D. J. Reilly, "Engineering the quantum-classical interface of solid-state qubits," *npj Quantum Information*, vol. 1, no. 1, pp. 1–10, 2015.
- [29] Y. Mustafa and S. Köse, "Side-channel leakage in sfq circuits and related attacks on qubit control and readout systems," *IEEE Transactions on Applied Superconductivity*, vol. 33, no. 6, pp. 1–7, 2023.
- [30] C. Howington, A. Opremcak, R. McDermott, A. Kirichenko, O. A. Mukhanov, and B. L. Plourde, "Interfacing superconducting qubits with cryogenic logic: Readout," *IEEE Transactions on Applied Superconductivity*, vol. 29, no. 5, pp. 1–5, 2019.
- [31] M. Möller and C. Vuik, "On the impact of quantum computing technology on future developments in high-performance scientific computing," *Ethics and information technology*, vol. 19, pp. 253–269, 2017.
- [32] A. Ash-Saki, M. Alam, and S. Ghosh, "Analysis of crosstalk in nisq devices and security implications in multi-programming regime," in *Proceedings of the ACM/IEEE International Symposium on Low Power Electronics and Design*, 2020, pp. 25–30.
- [33] A. Mi, S. Deng, and J. Szefer, "Securing reset operations in nisq quantum computers," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022, pp. 2279–2293.
- [34] B. Bell and A. Trügler, "Reconstructing quantum circuits through side-channel information on cloud-based superconducting quantum computers," in *2022 IEEE International Conference on Quantum Computing and Engineering (QCE)*. IEEE, 2022, pp. 259–264.
- [35] Y. Tan, N. Choudhury, K. Basu, and J. Szefer, "Qubithammer attacks: Qubit flipping attacks in multi-tenant superconducting quantum computers," *arXiv preprint arXiv:2504.07875*, 2025.