King Saud University
College of Computer and Information Sciences

Securing Open Radio Access Networks (O-RAN) Against Quantum Computing Threats

حماية شبكة النفاذ الراديوية المفتوحة ضد تهديدات الحوسبة الكمية

Azam Adel Alajroosh
445107723
445107723@student.ksu.edu.sa

Advisor
Dr. Ridha Ouni
Co-advisor
Dr. Kashif Saleem

Research proposal for the degree of
MSc in Computer Engineering
College of Computer and Information Sciences
King Saud University

First Semester
27/04/1446 H
30/10/2024 G

ABSTRACT

The Open Radio Access Networks (O-RAN) is a new evolution of traditional Radio Access Networks (RAN) in cellular networks with the principles of openness and intelligence. Toward success of the O-RAN concept, the security aspect of the network must be considered. One of the security challenges resides in securing O-RAN against quantum computing threats. Quantum computing constitutes a significant threat to the current cryptographic algorithms due to its highly powerful computing performance. In this research, we are interested to propose analysis and mitigation techniques as potential solutions using post-quantum cryptographic algorithms that can ensure securing the O-RAN against Quantum computing threats.

KEYWORDS

Open Radio Access Networks (O-RAN), Security, Cryptography Algorithms, Post-quantum cryptography, Quantum Computing Threats.

الملخص

تعتبر شبكات النفاذ الراديوية المفتوحة**(ORAN)** تطورا جديدا لشبكات النفاذ التقليدية في الشبكات الخلوية مع مبدأ الانفتاح والذكاء. لتحقيق نجاح مفهوم **O-RAN**، يجب مراعاة الجانب الأمني للشبكة. يكمن أحد التحديات الأمنية في تأمين **O-RAN** ضد تهديدات الحوسبة الكمومية. تشكل الحوسبة الكمومية تهديدًا كبيرًا لخوارزميات التشفير الحالية بسبب أدائها الحوسبي القوي للغاية. نهتم في هذا البحث باقتراح تقنيات التحليل والتخفيف كحلول محتملة باستخدام خوارزميات التشفير ما بعد الكم والتي يمكن أن تضمن تأمين **O-RAN** ضد تهديدات الحوسبة الكمية.

الكلمات الرئيسية

شبكات النفاذ الراديوية المفتوحة (**O-RAN**)، الأمان، خوارزميات التشفير، التشفير ما بعد الكم، تهديدات الحوسبة الكمية.

Table of Contents

List of Tables

List of Figures

List of Acronyms and Abbreviations

O-RAN	Open Radio Access Network
RAN	Radio Access Network
BBUs	Base Band Units
O-DU	O-RAN Distributed Units
O-CU	O-RAN Centralized Units
O-RU	O-RAN Radio Units
Non-RT RIC	non-real time RAN Intelligent Controller
Near-RT RIC	near-real time RAN Intelligent Controller
SMO	O-RAN Service Management & Orchestrator
O-Cloud	O-RAN Cloud
RICs	O-RAN Intelligent Controllers
ZTA	Zero Trust Architecture
AI	Artificial Intelligence
ML	Machine Learning
SDN	Software-Defined Networking
PQC	Post-Quantum Cryptography
QKD	Quantum Key Distribution
3GPP	3rd Generation Partnership Project
MTU	maximum transmission unit

1. INTRODUCTION

The Open Radio Access Network (O-RAN) is the next-generation of wireless systems cellular network. It is defined through the O-RAN Alliance specifications with the virtualized RANs, which are divided into components, connected by open interfaces, and enhanced by intelligent controllers. The new design of O-RAN works with multi-vendor, interoperable components, a centralized abstraction layer that can be programmatically optimized, and data-driven closed-loop control [1].

By dividing traditional Base Band Units (BBUs) into O-RAN Distributed Units (O-DU) and O-RAN Centralized Units (O-CU), O-RAN gets more flexibility for upgrades and network automation [2].

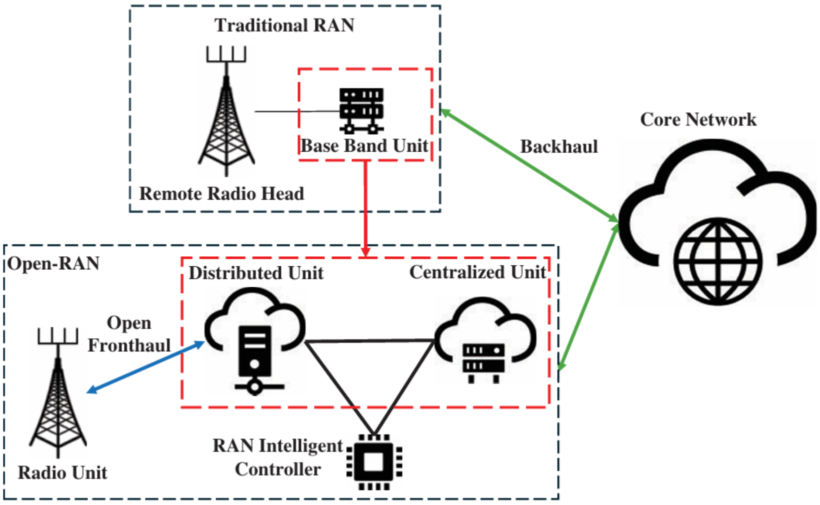

Figure 1: Comparison of traditional RAN with O-RAN architecture [2].

O-RAN has many advantages, However, openness brings in new security challenges. One of the challenges of security is securing O-RAN against quantum computing threats. Quantum computing is considered a significant threat to the current cryptographic algorithms due to its highly powerful computing performance. This research aims to provide mitigation techniques and analysis of potential solutions performance using post-quantum cryptographic algorithms that can ensure securing the O-RAN against Quantum computing threats.

This proposal is organized as follows. After the introduction, Section 2 will provide background information about the Quantum computing threats. Sections 3 and 4 present the problem statement and objectives of this research, respectively. Section 5 presents a literature review of the recent works related to O-RAN security including quantum computing threats. Section 6 presents the research methodology that will be used in this research. Sections 7 and 8 present the significance and relevance of the proposed research. Section 9 presents the research plan and timeline. Finally, a list of references, used as the background of this research, is presented at the end of the proposal.

2. BACKGROUND

2.1 Quantum Computing

There are two major types of computing: classical and quantum. Classical is the one which we all use in our daily lives. Another type is quantum computing, which uses concepts of computer science and quantum physics. There are differences between classical computing and quantum computing. Classical computing uses the traditional approach as the information is kept in bits. These bits are represented either in 0 or 1. On the other hand, Quantum computing uses the properties of quantum mechanics to provide a leap over classical computation in solving problems and calculations. Quantum computers use a probabilistic approach for calculations, as they solve problems with the most probable result, simultaneously using several other dimensions and offering many new ways of data representation. quantum computing uses quantum bits known as qubits. Quantum computing uses the concept of superposition due to which between these 0's and 1's, infinite other states can also be present there. In these states, there infinite number of qubits.in addition to other quantum mechanics-based phenomenon such as quantum entanglement. [3] The computing with an n-qubit quantum computer can be extremely powerful than any n-bit classical computer. The concept of the superposition speed-up as parallel operations on 2n states that can be simultaneously performed on a n-qubit register. However, the quantum computers can accelerate only some classes of computations and algorithms that work with superposition and parallel operations. For example, a quantum computer can solve efficiently is searching in an unsorted N entries database using Grovers quantum search algorithm to solve the problem in approximately √N steps compared to classical computer which needs N steps in the worst case.[4]

2.2 The Impact of Quantum Computing

quantum computing has several impacts on cryptographic algorithms which are made for classical computers. As quantum computers are expected to provide a huge number of calculations, it makes it easy for quantum computers to break the security provided to us by the classical methods of cryptography. Current cryptographic algorithms are considered insecure to quantum computers. This introduces new research and studies on new cryptographic algorithms and standards of quantum-resistant cryptographic algorithms. the new type of cryptography post-quantum cryptography or quantum-resistant or quantum-proof which can protect from attacks that use quantum computers. [3] Quantum computer can attack symmetric encryption using Grovers quantum search algorithm. This attack is working with the same concept of searching in an unsorted database. by searching for the known ciphertext using a large database of unsorted values. For example, AES with a 128-bit and assuming we have a plaintext and ciphertext pair. The key can be broken with a classical computer in approximately 2^{128} steps. On the other hand, with the quantum computer using Grovers algorithm, the same attack is more efficient: It would take only $\sqrt{2^{128}}$

= 2^{64} steps. However, the symmetric encryption problem can be solved by increasing the key length of symmetric algorithms. Unfortunately, the impact of quantum computers attacks with asymmetric encryption is a much more serious threat to all asymmetric algorithms that are currently in use, because discrete logarithms that can be broken in polynomial time using Shor's algorithm on a quantum computer. It's very important to develop and deploy new asymmetric algorithms that can resist quantum computers. The brightest PQC algorithms considered in the NIST competition open standardization call for quantum-secure asymmetric and belong to the families of lattice-based, code-based and hash-based cryptography.[4]

3. PROBLEM STATEMENT

Quantum computing is considered as a significant threat to the current cryptographic algorithms due to its highly powerful computing performance that can easily break encrypted data. The impact of Quantum computing on the O-RAN needs to be addressed since the O-RAN uses cryptographic algorithms in different parts of the architecture. This research proposes analysis and mitigation techniques using post-quantum cryptographic algorithms. However, the complexity of these algorithms as well as their network overhead represent their major challenging design.

4. RESEARCH GOAL AND OBJECTIVES

The goal of this research consists of selecting the most optimal post-quantum cryptographic algorithm from the recent literature ([19,20,21]). Then, it conducts analysis and provide mitigation techniques that can ensure O-RAN security against Quantum computing threats.

The main objectives of this research are the following:

- Perform a deep investigation on the vulnerabilities of the O-RAN to Quantum Computing Threats.
- Study and review several mitigation techniques for Quantum Computing Threats.
- Analysis of potential solutions performance using post-quantum cryptographic algorithms.
- Apply the most optimal post-quantum cryptographic algorithm selected from the recent literature.
- Improve the O-RAN network performance to mitigate the risk of Quantum computing threats.
- Ensuring security of the O-RAN network against Quantum computing threats and conducting performance evaluation while considering network layer metrices especially traffic including quantum attacks.
- Study security solutions scalability as the network grows.

5. LITERATURE REVIEW

The O-RAN or Open Radio Access Network is the next generation and the future for the previous generations of RAN (Radio Access Network) making them more open and intelligent. The increase in users of wireless and mobile networks needs to be followed by an increase in networks and equipment. By using the O-RAN network for Virtualization, Software-driven to become smarter, flexible, and energy efficient. O-RAN uses embedded machine learning systems for Real-time analytics and artificial intelligence to make network modules more intelligent. O-RAN key aspects of making the network elements virtualized with open interfaces as standardized Technologies. The reference designs will be open source and open white box network elements with important software and hardware components. This will make the vendors and operators strive to lead and drive this transformation.[5] however, O-RAN theology needs with high security level to avoid any cybersecurity attacks or threats against the users. In this literature review, we will overview O-RAN security concepts and show some of the issues with security in different parts of the architecture and how to secure the O-RAN network. In addition to the Quantum Computing Threats in the O-RAN network.

The authors in [6] presented the concept of Zero Trust Architecture or ZTA for Secure O-RAN. Since the O-RAN adopted the concept of the cloud and open architectures it can be exposed to cybersecurity attacks. O-RAN infrastructure is built with a ZTA to protect against internal and external threats. ZTA ensures confidentiality by using the micro-perimeters to secure the assets. ZTA ensures integrity through security controls to safeguard internal interfaces and protection in data-in-transit, at-rest, and in-use. ZTA ensures the authentication and authorization for any access to the resources external or internal, and always monitors and logs any suspicious activity. The paper addressed the important principle of ZTA throughout the network lifecycle. The O-RAN ALLIANCE is continuously pursuing with the other Partners to enhance the security of each asset of the O-RAN, including architectural elements, Infrastructure, interfaces, data, and Services. In addition to the New O-RAN elements, such as O-Cloud, AI/ML, Decoupled SMO,rApps/xApps, and Shared O-RU.

The authors in [1] presented a detailed tutorial on O-RAN to understand O-RAN, its architecture, interfaces, and workflows. The authors discussed the main O-RAN challenges and reviewed early research results. The authors provide a deep study of the O-RAN specifications, describing its architecture, showing the main design principles, and the O-RAN interfaces. The paper presented how the O-RAN Intelligent Controllers (RICs) can be used to effectively control and manage 3GPP-defined RANs. The authors discussed new methods and challenges of O-RAN networks, including the Artificial Intelligence (AI) and Machine Learning (ML) processes that the architecture and interfaces enable, security, and standardization issues. The authors reviewed experimental research platforms that can be used to design and test O-RAN networks, along with recent research results, and outlined future directions for O-RAN development.

The authors in [7] presented in the design of O-RAN that the cost and the benefit are important factors that need to be considered for securing the data and controlling interfaces, for example, the short timescales of wireless operation. The paper studies the impact of encryption on a critical O-RAN E2 interface that connects the base station to a near-real time radio intelligence controller near-RT RIC. The paper included quantitative measurements of the latency and CPU utilization for the encryption on the E2 interface that could impact data and machine learning models. The authors found encryption adds CPU utilization limits throughput to approximately 500 Mbps and around 50µs of delay. The cost of securing O-RAN is low based on the experimental and theoretical analysis shown, However, O-RAN designers must take into consideration the computing resources that can handle encryption overhead and the system budget does not exceed the actual traffic load. The authors suggest Future work Significant work to understand the secure O-RAN and any additional costs or hidden costs for securing other interfaces such as the Open Fronthaul that must have lower latency and higher throughput. Moreover, ensures security in a multi-vendor xApp environment, and building the O-RAN system uses a zero-trust approach.

The authors in [8]presented that since the O-RAN architecture is a newly imported technique and has an open nature, the security in O-RAN architecture from the early development stage is evaluated as crucial. The paper studies the O-RAN architecture from several attack surfaces, including architectural openness, cloud and virtualization, network slicing, and machine learning. The authors provided guidance and recommendations for the O-RAN designers and implementers in building the security concept for O-RAN networks. The paper shows a further study of the conceivable solutions to security threats. The security level of O-RAN still needs enhancement through the community's contribution including practical research of attacks, which will lead to defense methods that should be applied in the future. O-RAN would evolve in the long term into a secure system through Continuous updates and re-evaluation specifications of O-RAN.

The authors in [9] presented the impact of encryption on two critical Open RAN interfaces: the E2 interface, between the base station and a near-real-time RAN Intelligent Controller, and the Open Fronthaul, between the Radio Unit and the Distributed Unit. The authors presented different security protocols such as IPsec for E2 and MACsec for Open Fronthaul using encryption techniques and compared the impact on critical network performance. The paper quantitative study of the latency and throughput using Several encryption protocols. The authors find that the cost of securing the E2 interface is low, however, MACsec is more probably to impact the Open Fronthaul interface. The paper presented basic concepts for implementing security within Open RAN systems design and provides a roadmap for Open RAN security. The authors presented that system designers must ensure O-RAN nodes have enough computing resources to handle the encryption algorithm and security protocol. in addition, the designers must understand the end-to-end network MTU to avoid I/O bottlenecks and manage local MTU settings. The authors conclude that securing the O-RAN system needs further studying the associated costs of O-RAN security and the open problem with possible hidden expenses security of multi-vendor xApp environment, also adopting a zero-trust approach.

The authors in [10] presented the Security aspects of O-RAN systems in specifications, architectures, and intelligence. The paper is a holistic perspective on securing O-RAN systems including the open interfaces in O-RAN components, cloud-based platforms, intelligence, and data-driven. The paper identifies potential threats and discusses the solutions to these issues for each focus area. The authors observed the effect of delay for encrypting packets for IPsec protocol for the E2 interface as the encryption adds a delay of less than 50µs. However, we can overcome the computation cost by using a higher CPU to increase the throughput. the paper shows Security measures for intelligence Threats and deploying ML models including preventing, detecting, and reacting to attacks. The authors demonstrate a mitigated data poisoning attack in the case of an xApp that runs a Deep Reinforcement Learning (DRL) model that uses an autoencoder before the input to the DRL. The experiments show that autoencoders can decrease the unexpected ML outputs for slicing and scheduling by 30% and 70%. The authors presented security measures for cloud-based platforms. They focus on shared cloud and the principles for O-RAN cloud deployment, as well as the importance of separation between customers, visibility and auditing, and security by design. Also, they state that securing the service and data is the responsibility of the service providers and users.

The authors in[11] presented a centralized controller's architectural vulnerability in O-RAN compared with the Software-Defined Networking (SDN) controller. the paper presented a security analysis of two open-source Near-RT RICs (µONOS and OSC), focused on the A1 interface of the Near-RT RIC. The first part shows the supply-chain risks analysis of µONOS and OSC using off-the-shelf open-source dependency analysis and configuration file analysis. The result of the first part shows that open-source Near-RT RICs have multiple dependency risks and insecure configurations. the analysis identified 211 and 285 known dependency vulnerabilities in µONOS and OSC. The A1 interface takes most of the dependency risks in both Near-RT RICs. in addition to the issues related to access control, lack of encryption, and poor secret management due to security misconfiguration. the second part shows testing of the run-time security of the A1 API executed in µONOS and OSC using a custom O-RAN A1Interface Testing Tool (OAITT). The result of the second part shows that Near-RT RICs lack TLS for the A1 interface. The malicious Non-Real Time RAN Intelligent Controller (Non-RT RIC) or rApps that are built into the Non-RT RIC could interfere with some policies installed in the Near-RT RIC which can impact the O-RAN availability. Non-RT RICs could exploit the A1 protocol for hidden communication via the Near-RT RIC. The A1 of µONOS was vulnerable to degradation of service attacks and a denial-of-service attack with 10–60s response time for GET requests.

The authors in [12] presented the existing attack threats from the view of O-RAN components and interfaces. The authors during the experimental O-RAN environment H-Release discovered significant threats due to the absence of specified access control permissions for xApps. Malicious attackers can illegally have access to the APIs and view other services or launch attacks on legitimate xApps and E2 nodes through the E2 interface, it can result in E2 interface interruptions between O-DU, O-CU, and Near-RT RIC which can cause a complete RAN disruption. The paper identified the vulnerabilities in designing three attacks, providing a comprehensive analysis and detailed explanations of their impact on the system.

The authors in [2] presented an overview of the general O-RAN architecture and use cases such as B5G and 6G applications. Also due to the limitations of traditional RANs, the O-RAN introduces openness and intelligence, however this opens new security challenges. The paper investigates the specifications of O-RAN requirements security and threats issues focusing on mitigating security vulnerabilities Efficiently. The authors provided a comprehensive study of the architecture, use cases, and security of O-RAN, in addition to providing recommendations for future research in O-RAN and its security such as Quantum Computing Threats to O-RAN networks. Quantum Computing affects the O-RAN security due to high computing power more than supercomputers. Quantum Computing challenges the cryptographic algorithms complexity in the O-RAN. The paper suggested future research for cryptography-based security that can Quantum Resistance to ensure the security of the O-RAN and mitigate Quantum Computing Threats. On the other hand, the O-RAN can enhance security level requirements using the Quantum Cryptography algorithms.

The authors in [13] analyze the components of the Open RAN architecture and how it has a high risk for attack possibilities. The paper shows the measures required to ensure secure operation in the current state of security in the O-RAN. The paper presented some of the mitigations of security problems such as the Post-Quantum Security. As quantum computers using post-quantum schemes are expected to have the ability to break the current public-key schemes, however quantum-resistant cryptographic schemes should be included within O-RAN. The authors presented that to operate the Open-RAN securely needs to define the individual critical points and the overall security methodologies and to apply them in the O-RAN network.

The authors in [14] analyzed the security and privacy risks and challenges in Open RAN architecture. The paper discussed security solutions to secure Open RAN architecture and presented Open RAN security standardization efforts. The authors presented how Open RAN can provide more advanced security and privacy solutions in 5G and RAN networks. The authors presented the Impact of quantum computing and how it's a technology that challenges O-RAN security and the complexity of modern cryptographic algorithms. Quantum Resistance cryptography was introduced as a solution to Quantum computing's threat to the security of O-RAN networks. The authors presented that a defense technique should be taken for signaling and critical channels to improve both the security and efficiency of the O-RAN.

The authors in [15] presented quantum computing is one of the threats to the security of mobile systems. The use of public-key and symmetric-key cryptographic algorithms makes mobile systems such as O-RAN vulnerable to quantum attacks. The authors presented Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD), new fields of research that target the development of cryptographic algorithms that are secure against quantum attacks. The paper provided a perspective on the PQC and provided a categorizing of the various threats based on risk, impact, and potential mitigation techniques using PQC. The authors presented some challenges such as performance, and interoperability that need to be addressed to maintain those new algorithms for secure communication in future mobile systems.

In conclusion, the security in O-RAN plays an important role in the overall O-RAN system. In this review, we presented an overview of the O-RAN, the Evaluating, testing, and Implementing Security in O-RAN, The Security concept of Zero Trust Architecture ZTA, the cost of securing O-RAN, in addition to Securing Open Interfaces, Intelligence, and Platforms. We have also presented the quantum computing security threats to the O-RAN.

Table 1 : Presents the summary table for a literature review of the O-RAN security.

Table 1: Summary of literature review of the O-RAN security.

Ref	Topic	Year	Description
[1]	O-RAN Architecture, Interfaces, Algorithms, Security, & Challenges	2023	• O-RAN specifications: architecture, design principles, and interfaces. • O-RAN Intelligent Controllers (RICs) effectively control and manage 3GPP-defined RANs. • Artificial Intelligence (AI) and Machine Learning (ML) workflows. • Experimental platforms used to design and test O-RAN networks. • Challenges of O-RAN and future directions for O-RAN development.
[2]	ORAN Specifications: Use Cases, Security Threats, Requirements.	2024	• O-RAN architecture and use cases relevant to B5G and 6G applications. • Specifications of O-RAN security threats and requirements to mitigate security vulnerabilities effectively. • O-RAN architecture: use cases, and security considerations.
[5]	O-RAN: Towards an Open and Smart RAN	2018	• Challenges with traditional RAN. • Future vision & objectives for the O-RAN Alliance, motivation, and plans. • O-RAN Architecture & O-RAN Alliance
[6]	Zero Trust Architecture (ZTA) for Secure O-RAN	2024	• ZTA: multi-layered security controls (confidentiality, integrity, availability, authentication, and authorization protection of O-RAN from internal and external threats).
[7]	The Cost of Securing O-RAN	2023	• Impact of encryption E2 interface with quantitative measurements of latency and CPU. • Theoretical model to extend this study to other O-RAN implementations beyond the emulation environments.
[8]	Survey: Open Radio Access Network Security	2023	• Investigation of the current ORAN architecture from several attack surfaces. • Mitigation methods of the existing attack surfaces and corresponding. • Recommendation for the O-RAN implementers and framework designers.
[9]	Securing O-RAN Open Interfaces	2024	• The impact of encryption on two pivotal Open RAN interfaces: the E2 interface, and the Open Fronthaul.

			• Quantitative insights into the latency and throughput from various encryption protocols. • Fundamental principles for constructing security by design within Open RAN systems.
[10]	Security in O-RAN: Interfaces, Intelligence, and Platforms (implementation & evaluation)	2024	• Security of O-RAN focusing on the specifications, architectures, and intelligence. • A holistic perspective for securing O-RAN, including open interfaces platform, and intelligence. • Identify threats, discuss relevant solutions, and demonstrate experimentally the solutions.
[11]	Security Threats to xApps Access Control and E2 Interface in O-RAN.	2024	• Highlight the architectural weakness of a centralized controller in O-RAN. • Present a two-part security evaluation of two open-source Near-RT RICs (µONOS and OSC): supply-chain risks and run-time security testing.
[12]	Security Testing The O-RAN Near-Real Time RIC & A1 Interface.	2024	• An experimental O-RAN environment and discover threats from the absence of specified access control permissions for xApps. • Identified vulnerabilities to design three attacks, providing detailed explanations and a comprehensive analysis of their impact.
[13]	Conventional radio access networks more secure and trustworthy than Open-RAN?	2022	• Open RAN components are involved in deployment, assess the current state of security, and measures to ensure secure the Open RAN operation.
[14]	Open RAN security: Challenges and opportunities.	2023	• Analyze the security and privacy risks and challenges with Open RAN architecture. • Discusses security and privacy solutions to secure Open RAN architecture and standardization efforts for Open RAN security. • Open RAN deploy more advanced security and privacy solutions in 5G and traditional RAN.
[15]	Research Report on Quantum Security	2023	• Provide a perspective on the Post-Quantum Cryptographic algorithms. • Classification of the various threats based on risk and impact profiles and potential mitigation techniques using PQC. • Cryptographic algorithms challenges such as performance, and interoperability to develop new cryptographic algorithms against quantum attacks.

6. RESEARCH METHODOLOGY

To achieve the research objectives, the research methodology combines theoretical and simulation methodology as it uses a suitable environment for analysis, simulation, testing, and validation of securing O-RAN against quantum computing threats. It involves the following steps:

- First, we need to expand our study and perform a deep investigation of the vulnerabilities of the O-RAN network to quantum computing threats. This study may cover their impact as well on performance.

- Second, analyze the post-quantum cryptographic algorithm and select the most appropriate algorithms to find potential solutions and mitigation techniques for Quantum Computing Threats.
- Third, simulate and test the potential solutions and mitigation techniques in the O-RAN network. The simulation will cover the O-RAN network and test the potential solutions and mitigation techniques such as applying different post-quantum cryptographic algorithms.

  For the O-RAN simulations will use the OpenRAN Gym tools, a publicly available Open Toolbox platform for O-RAN experimentation by providing the tools for Building on frameworks for data collection and testing of end-to-end design.[16]

  The mine OpenRAN Gym tools that that will help with the simulations the O-RAN:

  - ns-O-RAN: an open-Source Open RAN Simulation Platform with a functional 4G/5G protocol stack in ns-3. ns-O-RAN simulator can enhance data collection testing capabilities. also with different simulated scenarios applications, and with different such as multimedia streaming, web browsing, etc., ns-O-RAN supports implements E2 service models, Performance Metrics monitoring and Control, that enable a closed-loop control for example, of traffic steering and mobility.[17]
  - Colosseum: a wireless network emulator of next-generation radio network technologies in repeatable and highly configurable Radio frequency and traffic environments. Colosseum is Accessible as a cloud-based platform, Colosseum provides built-in powerful computational resources and provides unique experimentation and data-collection capabilities. emulates multiple operational environments for example real-time with effects such as multipath and fading effects. Carry out large-scale testing and data-collection with Instantiate softwarized protocol stacks on a general-purpose infrastructure.[18]
- Fourth, Measure and compare the performance of the potential solutions and mitigation techniques in the O-RAN network.

  Performance Validation will validate the results by setting the specific performance metrics that will define as performance metrics for example throughput, Response time, and CPU Utilization and compare simulation results with normal O-RAN and with the post-quantum cryptographic algorithms.

7. CONTRIBUTION TO THE FIELD/ SIGNIFICANCE AND /OR IMPACT OF PROPOSED RESEARCH

This research will contribute to outlining the challenges of securing O-RAN against quantum computing threats. The proposed research will show the potential solutions and mitigation techniques for quantum computing threats in the O-RAN network. The outcome of this research would be beneficial to academics and professionals in related fields.

8. RELEVANCE TO THE DEPARTMENT

The proposed research is based on multiple fields in Computer Engineering such as computer networks, wireless networks, cellular networks, network security, cryptography, and quantum computing. This thesis constitutes an initial research work on securing O-RAN networks against Quantum computing threats. The future works in the department may use this thesis to improve and ensure the security of computer networks in general against Quantum Computing threats.

9. RESEARCH PLAN AND TIMELINE

Table 2 : Presents the timeline of the thesis achievement mapped with our proposed methodology.

Table 2: Timeline to perform the proposed research

Task	**TimeLine (Months)**											
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
Expanding Literature Review	🟩	🟩										
Studying O-RAN architecture, O-RAN security, and Quantum Computing Threats.		🟩	🟩	🟩								
Detection & mitigation of Quantum Computing Threats in O-RAN networks.				🟩	🟩	🟩	🟩					
Simulation and performance evaluation						🟩	🟩	🟩	🟩	🟩		
Results and analysis									🟩	🟩	🟩	
Thesis writing				🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

Table 3 : Presents the expected thesis outline will include the following parts:

Table 3: Expected thesis outline.

Chapter 1	General Introduction
Chapter 2	Background and literature review for O-RAN architecture, O-RAN security, and Quantum Computing Threats.
Chapter 3	Detection & mitigation of Quantum Computing Threats in O-RAN networks.
Chapter 4	Simulation, performance evaluation, and results analysis of Securing O-RAN against Quantum Computing Threats.
Chapter 5	Conclusion and future work.
	References.

10. REFERENCES

[1] M. Polese, L. Bonati, S. D'Oro, S. Basagni, and T. Melodia, "Understanding O-RAN: Architecture, Interfaces, Algorithms, Security, and Research Challenges," *IEEE Communications Surveys and Tutorials*, vol. 25, no. 2, pp. 1376–1411, 2023, doi: 10.1109/COMST.2023.3239220.

[2] H. Park, T.-H. Nguyen, and L. Park, "An Investigation on Open-RAN Specifications: Use Cases, Security Threats, Requirements, Discussions," *Computer Modeling in Engineering & Sciences*, vol. 141, no. 1, pp. 13–41, Aug. 2024, doi: 10.32604/CMES.2024.052394.

[3] B. Bhushan, S. K. Sharma, R. Kumar, and I. Priyadarshini, Eds., *5G and Beyond*. in Springer Tracts in Electrical and Electronics Engineering. Singapore: Springer Nature Singapore, 2023. doi: 10.1007/978-981-99-3668-7.

[4] C. Paar, J. Pelzl, and T. Güneysu, "Understanding Cryptography," *Understanding Cryptography*, 2024, doi: 10.1007/978-3-662-69007-9.

[5] O-RAN ALLIANCE, "O-RAN: Towards an Open and Smart RAN," Sep. 2018, *O-RAN Alliance*. [Online]. Available: https://mediastorage.o-ran.org/white-papers/O-RAN.White-Paper-2018-10.pdf

[6] O-RAN ALLIANCE, "Zero Trust Architecture (ZTA) for Secure O-RAN," Sep. 2024, *O-RAN Alliance*. [Online]. Available: https://mediastorage.o-ran.org/white-papers/O-RAN.WG11.ZTA%20for%20Secure%20O-RAN%20White%20Paper-2024-05.pdf

[7] J. Groen, B. Kim, and K. Chowdhury, "The Cost of Securing O-RAN," in *ICC 2023 - IEEE International Conference on Communications*, 2023, pp. 5444–5449. doi: 10.1109/ICC45041.2023.10279036.

[8] Y.-Z. Chen, T. Y.-H. Chen, P.-J. Su, and C.-T. Liu, "A Brief Survey of Open Radio Access Network (O-RAN) Security," 2023. [Online]. Available: https://arxiv.org/abs/2311.02311

[9] J. Groen *et al.*, "Securing O-RAN Open Interfaces," 2024. [Online]. Available: https://arxiv.org/abs/2404.15076

[10] J. Groen *et al.*, "Implementing and Evaluating Security in O-RAN: Interfaces, Intelligence, and Platforms," 2024. [Online]. Available: https://arxiv.org/abs/2304.11125

[11] C.-F. Hung, Y.-R. Chen, C.-H. Tseng, and S.-M. Cheng, "Security Threats to xApps Access Control and E2 Interface in O-RAN," *IEEE Open Journal of the Communications Society*, vol. 5, pp. 1197–1203, 2024, doi: 10.1109/OJCOMS.2024.3364840.

[12] K. Thimmaraju, A. Shaik, S. Flück, P. J. F. Mora, C. Werling, and J.-P. Seifert, "Security Testing The O-RAN Near-Real Time RIC & A1 Interface," in *WiSec '24: Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks* , in WiSec '24. New York, NY, USA: Association for Computing Machinery, 2024, pp. 277–287. doi: 10.1145/3643833.3656118.

[13] F. Klement *et al.*, "Open or not open: Are conventional radio access networks more secure and trustworthy than Open-RAN?," Apr. 2022, Accessed: Sep. 28, 2024. [Online]. Available: https://arxiv.org/abs/2204.12227v3

[14] M. Liyanage, A. Braeken, S. Shahabuddin, and P. Ranaweera, "Open RAN security: Challenges and opportunities," *Journal of Network and Computer Applications*, vol. 214, p. 103621, May 2023, doi: 10.1016/J.JNCA.2023.103621.

[15] O-RAN ALLIANCE, "Research Report on Quantum Security," Sep. 2023. Accessed: Oct. 03, 2024. [Online]. Available: https://mediastorage.o-ran.org/ngrg-rr/nGRG-RR-2023-04-Quantum-Security-v1_1.pdf

[16] L. Bonati, M. Polese, S. D'Oro, S. Basagni, and T. Melodia, "OpenRAN Gym: AI/ML development, data collection, and testing for O-RAN on PAWR platforms," *Computer Networks*, vol. 220, p. 109502, Jan. 2023, doi: 10.1016/J.COMNET.2022.109502.

[17] A. Lacava *et al.*, "Programmable and Customized Intelligence for Traffic Steering in 5G Networks Using Open RAN Architectures", Accessed: Oct. 30, 2024. [Online]. Available: https://gerrit.o-ran-

[18] L. Bonati *et al.*, "Colosseum: Large-Scale Wireless Experimentation Through Hardware-in-the-Loop Network Emulation", Accessed: Oct. 30, 2024. [Online]. Available: https://www.colosseum.net

[19] Subramani, S., M, S., A, K., & Svn, S. K. (2023). Review of Security Methods Based on Classical Cryptography and Quantum Cryptography. Cybernetics and Systems, 1–19. https://doi.org/10.1080/01969722.2023.2166261

[20] Z. Yang, H. Alfauri, B. Farkiani, R. Jain, R. D. Pietro and A. Erbad, "A Survey and Comparison of Post-Quantum and Quantum Blockchains," in IEEE Communications Surveys & Tutorials, vol. 26, no. 2, pp. 967-1002, Secondquarter 2024, doi: 10.1109/COMST.2023.3325761.

[21] B. Halak, T. Gibson, M. Henley, C. -B. Botea, B. Heath and S. Khan, "Evaluation of Performance, Energy, and Computation Costs of Quantum-Attack Resilient Encryption Algorithms for Embedded Devices," in IEEE Access, vol. 12, pp. 8791-8805, 2024, doi: 10.1109/ACCESS.2024.3350775.