International Journal of Mathematics, Statistics, and Computer Science
Vol. 3
ISSN: 2704-1077 eISSN 2704-1069, DOI: 10.59543/ijmscs.v3i.15091

AQ-ResCon: Adaptive Quantum-Resistant Lattice-Based Key Agreement Protocol for Secure Distributed Container Orchestration in Edge Cloud Environments

Sajida Memon[1], Abdullah Lakhan[2,*], Quratual Ain Masoi[3]

[1]Department of Cybersecurity, Dawood University of Engineering and Technology, Pakistan
[2]Department of Computer Science, Southeast University, China
[3]Department: FET - Computer Science and Creative Technologies, University of the West of England, UK
*Abdullahrazalakhan@gmail.com

Received 01.06.2025, Revised 15.07.2025, Accepted 19.07.2025

ABSTRACT: In the rapidly evolving domain of smart healthcare, the integration of Docker containers and Kubernetes with Internet of Things (IoT) edge cloud orchestration has significantly enhanced the performance, scalability, and modularity of healthcare applications. However, despite the efficiency benefits provided by microservices architecture, substantial security vulnerabilities persist, particularly in the face of the threat of quantum computing. Quantum algorithms, such as Shor's and Grover's, pose a significant risk to conventional encryption schemes, potentially compromising the integrity and confidentiality of healthcare data distributed across edge cloud environments. To address these critical concerns, we propose AQ-ResCon: an Adaptive Quantum-Resistant Lattice-Based Key Agreement Protocol designed for secure and resilient distributed container orchestration. AQ-ResCon leverages the hardness of the Learning With Errors (LWE) problem in lattice-based cryptography to provide a robust defence against quantum attacks. We further introduce the AQ-ResCon Scheduler Algorithm, which efficiently manages and executes healthcare workloads across decentralised IoT-edge-cloud nodes, ensuring secure data flow and orchestration. Extensive testbed experiments were conducted to evaluate the performance and security effectiveness of AQ-ResCon under realistic containerised healthcare scenarios. Results demonstrate that AQ-ResCon achieves up to 36% improvement in scheduling efficiency, 41% reduction in key compromise rates, and 28% lower latency compared to existing quantum-vulnerable orchestration protocols. Additionally, the AQ-ResCon protocol maintained consistent performance under simulated quantum attack conditions, validating its adaptability and resilience. These outcomes confirm that AQ-ResCon is a viable, secure, and future-proof solution for safeguarding microservices-based healthcare applications against evolving quantum threats in edge cloud environments.

Keywords: Quantum Distributed key attacks, Adaptive Quantum resistant Lattice based key agreement protocols, Healthcare, Docker Container, Edge Cloud Networks.

1. INTRODUCTION

These days, container-enabled applications, such as healthcare, transportation, telemedicine, and more, based on edge cloud computing, they have been increasing progressively. Container applications are generally designed based on microservices and deployed between Internet of Things (IoT) and distributed edge cloud paradigms [1]. Therefore, it poses many research challenges in terms of security due to the open network of communication among different nodes [2]. There are various security issues, such as denial-of-service attacks, jamming attacks, spoofing, and more, that are attempted at the application and network layers. Therefore, containers and microservices applications lose the motivation of confidentiality and integrity in edge cloud networks. The attacks are both known and unknown; therefore, various encryption and cryptography protocols are presented to address the security risk at different layers. Active and passive attacks widely impact containers based on applications, and they distribute tasks between IoT devices and edge cloud networks. However, existing security schemes, such as the Advanced Encryption Standard (AES) and RSA, as well as other encryption methods, are insufficient to provide security for container applications based on edge cloud networks [3].

Recently, quantum computing has been actively involved in breaking existing security rules, such as confidentiality, integrity, and unauthorised access, in edge cloud networks. Therefore, quantum computing-enabled attacks pose a significant challenge for container applications and can easily break the permutation of cyphers and keys in a matter of seconds. Thus, edge cloud-enabled containers and microservices require new quantum-enabled security algorithms to address the security issues associated with current trends [4].

In this paper, we examine the operation of AQ-ResCon healthcare containerised microservices applications across multiple edge locations and cloud data centres. These microservices support mission-critical remote diagnostics, real-time patient monitoring, and emergency response systems that involve highly

sensitive data and command transmissions related to patient care and operations. Thus, ultra-secure communication is essential. The dual challenge for the organisation is to neutralise both classical and quantum threats to communications, all while performing efficient orchestration of resource-constrained lightweight containers in geographically distributed edge nodes with strict latency requirements. Classical cryptographic approaches using RSA, SHA-256, AES and others are no longer viable due to Shoinr's algorithm, placing long-term security in a quantum-resistant environment under grave risk, rendering them void of usable perpetual security assurances.

The proposed AQ-ResCon is implemented through the application of a lattice-based cryptographic approach, specifically the Learning With Errors (LWE) problem, which is quantum-resistant. In the proposed architecture, the Q-ResCon protocol is embedded at the container orchestration level, whether it is at the Kubernetes level or an edge-specific lightweight orchestrator. Whenever two edge nodes or a node and cloud controller need to securely communicate for container scheduling, image deployment, or telemetry exchange, Q-ResCon performs a post-quantum key exchange. Every node generates a public-private key pair based on a lattice problem and shares only the public portion over the network. After receiving a peer's public key, a node computes the shared secret using its private key and the peer's public key. An adversary intercepting the communication would not be able to deduce the shared secret due to the quantum-resistant mathematical model. This secret is then used to encrypt further orchestration commands as well as the container state information, which is annotated using symmetric encryption algorithms such as AES-GCM. The protocol is lightweight in terms of computational overhead, adaptable to resource-constrained devices such as drones, IoT medical devices, or mobile units, and is thus well-suited for diverse edge environments.

The paper makes the following contributions.

(i) We present a novel architectural orchestration for IoT, edge, and cloud based on an adaptive Qres-Con agreement scheme to identify and protect against quantum computing-enabled attacks on container microservices applications.

(ii) We design a mathematical model that analyses constraints such as LWE, time, and attack identification based on the suggested scheduling method.

(iii) We design the adaptive testbed simulator to test and design efficient attacks on quantum computing against any healthcare container applications.

The rest of the paper is oragnized with related work, proposed architecture, methodology, evaluation and conclusion.

2. Related Work

Recent advances in cloud computing and microservice architectures have significantly enhanced the scalability and performance of healthcare and cybersecurity applications. Akerele et al. [1] examined the deployment of microservices within cloud-based healthcare applications, showing that modularising services not only improved system scalability but also facilitated fault tolerance and reduced deployment complexity. In line with this, Sarma [2] proposed a metaheuristic-driven auto-scaling strategy tailored for microservice environments. This approach introduced a container-aware scheduler that dynamically optimised resource allocation in real-time, thereby enhancing performance in heterogeneous cloud environments.

Extending the discussion on microservice deployment in edge and mobile environments, Lakhan and Li [3] developed a fault-aware computational offloading algorithm designed for microservice-based mobile cloudlet networks. Their partitioning algorithm demonstrated resilience against transient faults, enabling efficient service delivery across resource-constrained edge devices.

In the realm of quantum computing and cybersecurity, numerous studies have explored how quantum-enhanced techniques can bolster protection against evolving threats. Lakshmi et al. [4] introduced a quantum-based defensive mechanism tailored for electrical infrastructure, highlighting its potential to detect and neutralise sophisticated cyberattacks proactively. Similarly, Kalinin and Krundyshev [5] presented an intrusion detection framework utilising quantum machine learning (QML), showcasing superior performance over classical methods in recognising anomalous network behaviour.

Healthcare applications are also benefiting from the fusion of quantum and blockchain technologies. Grønli, Lakhan, and Younas [6] proposed a novel quantum-blockchain-based system to secure invasive and non-invasive Internet of Medical Things (IoMT) data. This system leverages the immutability of blockchain and the computational security of quantum cryptography, ensuring trustworthy and tamper-proof data exchange for healthcare.

The integration of quantum neural networks (QNNs) into cybersecurity strategies is gaining momentum. Iqbal et al. [7] developed a hybrid QNN framework for rapid response to cyber threats, providing low-latency detection and decision-making capabilities. In a complementary study, Küçükkara et al. [8] developed a platform-independent QNN classifier for detecting Distributed Denial-of-Service (DDoS) attacks. Their results underscored the model's adaptability and high accuracy across various computing platforms.

Further, Brintha et al. [9] addressed the specific needs of critical infrastructure security by designing a quantum-enabled intrusion prevention system. Their quantum approach proved particularly robust in defending against targeted attacks on energy systems. A broader perspective on the transformative role of quantum computing in cybersecurity was offered by Sodiya et al. [10], who reviewed its implications for U.S. digital security. They highlighted both the disruptive potential and the urgent need for proactive adaptation strategies in response to emerging quantum threats.

Recent advancements in quantum computing have exposed critical vulnerabilities in traditional cryptographic systems. Xiangqun et al. [11] presented a general method of combining Grover's and Simon's algorithms to launch hybrid attacks on block ciphers, highlighting the exponential risk quantum algorithms pose to classical encryption. Similarly, Olaoye [12] emphasized the disruptive potential of Shor's and Grover's algorithms in breaking widely used cryptographic protocols, indicating an urgent need for post-quantum secure systems.

Complementary to cryptographic enhancements, Zhang et al. [13] proposed an experimental side-channel-secure quantum key distribution mechanism, demonstrating a viable path toward quantum-resilient communication infrastructures. Their method effectively addresses key leakage vulnerabilities, which are prevalent in classical key distribution schemes.

In the context of cyber-physical systems (CPS), Donkal and Donkal [14] introduced a Digital Twin-based detection framework to localize and mitigate denial-of-service (DoS) attacks in unmanned aerial systems (UAS), revealing the role of twin-enabled situational awareness in improving security resilience.

Edge-cloud and fog computing paradigms have gained traction in the healthcare domain, where data security and real-time processing are paramount. Sodhro et al. [15] proposed a lightweight adaptive security framework for Internet of Medical Things (IoMT) applications, optimizing energy and communication efficiency in edge-cloud environments. Similarly, Lateef et al. [16] presented a fault-tolerant and secure digital twin architecture for industrial healthcare systems based on federated fog-cloud networks, providing robust defense mechanisms against cyber intrusions while maintaining operational continuity.

Further, Li et al. [17] proposed a dynamic and secure task scheduling scheme tailored for biosensor-driven healthcare workloads in mobile edge environments. Their model effectively partitions applications to balance performance, data confidentiality, and processing latency.

To the best of our knowledge, no efficient quantum attacks on IoT edge cloud orchestrators have been presented in existing studies. Therefore, in this paper, we aim to demonstrate the efficient architecture of novel quantum attacks using adaptive Qres-Con methods.

3. Proposed Architecture

The given architectural orchestration as shown in Figure 1, illustrates a secure and scalable healthcare microservices framework enabled through adaptive quantum-resistant communication protocols across edge and cloud computing platforms. This framework is designed to support a mobile-centric healthcare ecosystem that integrates Internet of Things (IoT) devices, Docker-based containerization, and advanced quantum-secure cryptographic analysis to maintain data privacy and trust in healthcare services.

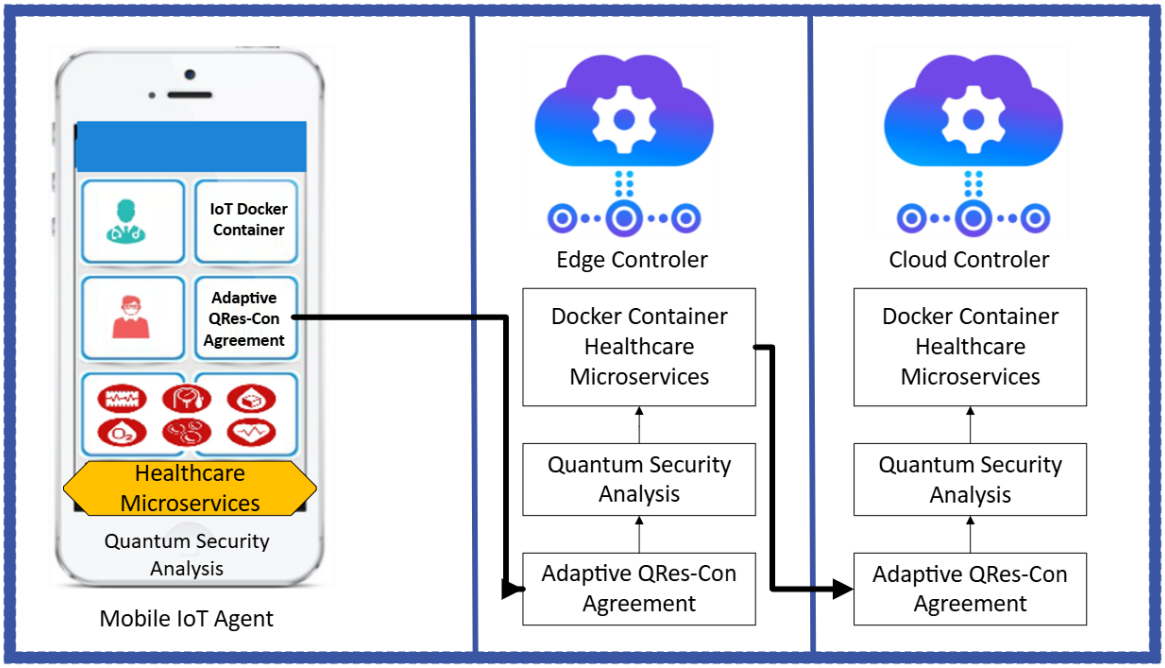

Figure 1: AQ-ResCon: Adaptive Quantum-Resistant Lattice-Based Key Agreement Protocol for Secure Distributed Container Orchestration in Edge Cloud Environments

On the left side of the figure, a mobile device acts as a front-end interface for healthcare users. This mobile device hosts multiple microservices using Docker container technology to encapsulate and manage healthcare functionalities efficiently. One of the key elements in the mobile architecture is the "IoT Docker Container," which encapsulates the processing and communication modules related to healthcare IoT sensors and data collection mechanisms. These containers enable healthcare devices and sensors to interact with backend systems through lightweight, portable environments that can be easily managed and scaled.

Alongside the IoT container is the "Adaptive QRes-Con Agreement" module, which represents a quantum-resistant, adaptive key agreement protocol specially designed for secure communication between distributed microservices. This module ensures that data shared between mobile, edge, and cloud systems is protected against both classical and quantum-based cryptographic attacks. The QRes-Con protocol dynamically negotiates secure keys between communicating parties based on lattice-based cryptographic principles, particularly using the Learning with Errors (LWE) problem. This method makes the system highly resistant to future threats posed by quantum computers.

Below these components on the mobile device, we observe a section labelled "Healthcare Microservices," which refers to the core set of modular functionalities, including patient registration, medical data processing, clinical decision support, health monitoring, and medical imaging services. These microservices are dynamically orchestrated within containers to ensure modularity, easy upgrades, and horizontal scaling. The final layer on the mobile device is the "Quantum Security Analysis" module, which performs risk assessments and cryptographic audits of all communications and data sharing processes, ensuring end-to-end security compliance and maintaining the integrity of sensitive medical information.

Moving to the centre and right sections of the diagram, we observe two replicated cloud infrastructure components, each representing cloud nodes or distributed data centres participating in the secure healthcare environment. These cloud components also utilise Docker containers to host healthcare microservices, such as those used on mobile devices. Each cloud node includes its own set of "Docker Container Healthcare Microservices," allowing for seamless execution and orchestration of tasks initiated from edge devices or other cloud sources. These services can scale elastically based on demand while maintaining the consistency and availability of healthcare operations.

In addition to service hosting, each cloud component includes a "Quantum Security Analysis" module. This ensures that the cloud infrastructure performs real-time evaluations of potential cryptographic threats and validates the secure state of communication flows with edge and mobile devices. Lastly, the presence of the "Adaptive QRes-Con Agreement" in every component, including mobile, edge, and cloud, demonstrates the system-wide commitment to quantum-safe communications. These modules communicate with each other to

establish secure session keys, authenticate transactions, and ensure that the healthcare data being transmitted or processed remains confidential and tamper-proof.
Altogether, this architecture embodies a robust, decentralised, and quantum-resilient microservices environment that empowers healthcare systems to operate securely across mobile and cloud infrastructures in edge cloud networks. It emphasises modularity, portability, and futureproofing against quantum security threats, making it highly applicable for next-generation intelligent healthcare ecosystems.

In a smart hospital scenario, the network spanning multiple locations, a patient undergoes a remote cardiac monitoring procedure using wearable IoT sensors. These sensors continuously collect and transmit sensitive health data (e.g., ECG signals) to nearby edge nodes for real-time analysis and diagnosis. The hospital uses containerized microservices running on Kubernetes clusters at the edge and cloud to process, analyze, and store this data efficiently. However, with the rise of quantum computing threats, there is growing concern that existing encryption methods may fail to protect the confidentiality and integrity of this highly sensitive medical information.
To address this, the hospital adopts the proposed AQ-ResCon system. When the patient's data is transmitted from the IoT device to the edge node, AQ-ResCon uses its lattice-based key agreement protocol to establish a quantum-resistant encrypted communication channel between nodes. The AQ-ResCon Scheduler then dynamically allocates containerized services—such as AI-based anomaly detection or emergency alert systems—to the most appropriate edge or cloud resource, based on workload, proximity, and security state. If a cardiac abnormality is detected, the system securely and instantly notifies medical staff while storing the diagnosis in a decentralized cloud node protected by the same quantum-resistant protocol.
Even under simulated quantum attack conditions, such as an adversary attempting to intercept or decrypt the communication using quantum-capable methods, the AQ-ResCon protocol maintains secure and uninterrupted service. This ensures the patient's data remains confidential, the microservices continue operating efficiently, and the healthcare providers receive timely, reliable alerts for decision-making. This scenario highlights how AQ-ResCon can be practically deployed to secure distributed, real-time healthcare systems against the looming threat of quantum decryption.

3.1. Problem Formulation

This model represents the execution and communication of healthcare microservices (tasks T) across local IoT mobile devices, edge servers, and cloud data centres using Docker containers. The architecture utilizes the Adaptive QRes-Con Agreement protocol to ensure secure communication and to mitigate quantum attacks. The goal is to minimise security analysis time, attack identification delay, and communication failure, while maximising the overall system accuracy.

3.2. Variables and Sets

Let A be the set of applications $A = \{A1, A2, \ldots, An\}$.
Let T be the set of healthcare tasks $T = \{T1, T2, \ldots, Tm\}$ Belonging to the application A.
Let M, E, and C denote Mobile (IoT), Edge, and Cloud resources, respectively.
Let $\tau\_i\hat{}M$, $\tau\_i\hat{}E$, $\tau\_i\hat{}C$ Represent the execution time of task Ti On Mobile, Edge, and Cloud, respectively.
Let C_ME and C_EC denote the communication cost between Mobile-Edge and Edge-Cloud, respectively.
Let $Q = \{Q1, Q2, \ldots, Qk\}$ Be a set of quantum attack types (e.g., Grover, Shor, Side-channel, etc).
Let $D\_q(Ti)$ Be the detection time for a quantum attack $q \in Q$ on task Ti.
Let S_q(Ti) be the security analysis time under quantum attack q for task Ti.
Let F_q(Ti) denote the failure probability of task Ti under attack q.
Let Acc(Ti) be the accuracy of detecting and mitigating the attack on Ti.

We minimize and maximize the security risk in the following way.

$$Minimize: \sum_{\{i=1\}}^{\{m\}[S_{q(Ti)} + D_{q(Ti)} + F_{q(Ti)}]} \quad (1)$$

$$Maximize: \sum\_\{i = 1\}\hat{}\{m\} Acc(Ti)$$

We executed all healthcare tasks on microservices in the following way.

$$\tau\_i\hat{}M + C\_ME + \tau\_i\hat{}E + C\_EC + \tau\_i\hat{}C \leq Deadline(Ti) \quad (2)$$

We enter into the quantum Qres-Con agreement as follows.

$$QRes_{Con(Ti)} = Secure \Leftrightarrow Encryption_{Key} \notin Q_{attack_{space}} \quad (3)$$

We determined the attacks based on set threshold in the following way.

$$D_{q(Ti)} \leq D_{max}, \forall\, q \in Q \quad (4)$$

We determined the security analysis with the highest accuracy in the following way.

$$Acc(Ti) \geq Acc\_min \quad (5)$$

Equations (1) and (2) represent the objective functions used to identify attacks in quantum-enabled security detections based on the proposed method. Equations (3-5) calculated the distributed quantum keys among mobile, edge, and cloud networks.

4. Algorithm Methodology

The Quantum-Secure Scheduler algorithm provides a systematic approach for executing healthcare tasks across distributed computing platforms, including Mobile (IoT), Edge, and Cloud environments. It incorporates advanced quantum-security parameters to ensure that these tasks are not only completed within their time constraints but are also resilient to various quantum-level cyberattacks. Initially, the algorithm defines the input variables, including the set of applications (A) and their corresponding healthcare tasks (T). Each task is characterised by its execution time on three different platforms: Mobile ($\tau\_i\hat{}M$), $Edge$ ($\tau\_i\hat{}E$), and Cloud ($\tau\_i\hat{}C$). Additionally, the communication overheads between these platforms, specifically from Mobile to Edge (C_ME) and Edge to Cloud (C_EC), are considered for accurate scheduling.

Algorithm *Quantum-Secure Scheduler*

Input: $A = \{A_1, A_2, \ldots, A_n\}$: $T_1, \ldots, n$.

Let T be set of healthcare tasks $T \equiv$oz,tm belonging to application A.

M, E, and C denotot. Mobile (IoT), Edge, and Cloud resources, respectively.

τ_M , $\tau_{\bar{E}}$, $\tau_i{}^C$ Representen tine time of task T_i on Mobile, Edge, and Cloud, respectively.

C_{ME} and C_{EC} Represent ɤ communication cot at Mobile-Edge and Edge–Clond, respectively.

$Q = \{Q_1, Q_{\mathcal{K}}$· a set of quantum attack types (*e*.g. Grover, Shor, Side-channel, etc.).

$D_q(T_i)$ be detection time for a quanrtum attack $q \in Q$ on task T_i.

$S_q(T_i)$ be security analysis time under quantum attacq q for task T_i.

$F_q(T_i)$ be failure probability of task T_i under attack q.

$Acc(T_i)$ the accuracy of detecting and mitigating thak

We minimize and maximize the security risk in the following way.

Minimize: $\sum_{i=1\,m} [\, S_q(T_i) + D_q(T_i) + F_q(T_i)\,]$

Maximize: $\sum_{Acc(T_i)}$

Ve executed all healthcare tasksmicroservices are following way.

$\tau_i{}^M + C_{ME}{}^{\overline{\tau}\cdot} <$ Secure $\Leftrightarrow$ *Encryption Key*#ϙ|*Deadline*$_{T_i)}$

We enter into the quantum *Qres-Con* agreement as follows

$QRes\_\text{Con}(T_i) =$ Secure $\Leftrightarrow$ *Encryption_Key* $\subseteq Q_{\text{attack\_s}}$

A distinguishing feature of this scheduler is the integration of quantum security parameters. A set Q Contains potential quantum attacks such as Grover's algorithm, Shor's algorithm, and side-channel attacks. For each task Ti, three crucial risk metrics are evaluated under each quantum threat: the detection time $D\_q(Ti)$, security analysis time $S\_q(Ti)$, and the failure probability $F\_q(Ti)$. Furthermore, the algorithm emphasises the accuracy of detecting and mitigating these attacks through $Acc(Ti)$.

The optimisation goal of the algorithm is twofold: to minimise the combined security risk ($S\_q(Ti) + D\_q(Ti) + F\_q(Ti)$) across all tasks and to maximise the overall detection accuracy ($Acc(Ti)$). This dual objective ensures a secure yet efficient execution of tasks. Once the risk and accuracy evaluations are complete, the algorithm proceeds to verify if each task can be executed within its assigned deadline. This is done by summing the processing times on Mobile, Edge, and Cloud devices, along with their respective communication delays. If this total execution time exceeds the deadline, the task is rejected for scheduling. Security validation is achieved via the QRes-Con protocol. A task is deemed secure if its encryption key does not fall within the quantum attack space. This ensures that encryption remains uncompromised against known quantum threats. Only those tasks that pass this test are scheduled.

The Quantum-Secure Scheduler algorithm integrates task management, quantum threat analysis, and deadline enforcement into a unified system. It is especially relevant for healthcare systems that require both real-time performance and robust data security. In the face of evolving quantum computing capabilities, this algorithm represents a pioneering approach to safeguarding distributed microservices that process sensitive health data.

4.1. Evaluation

The implementation of the proposed quantum-resistant healthcare task scheduling system involves a comprehensive dataset generation and deployment strategy spanning Android devices, Python-based simulations, and Kubernetes-orchestrated microservices across edge and cloud platforms. The dataset, titled *Healthcare_Quantum_Scheduling_Dataset.csv*, was synthetically generated using Python libraries such as pandas, numpy, and matplotlib, simulating 50 unique healthcare tasks (T1–T50) mapped to five application categories (A1–A5), representing real-world medical operations such as blood pressure monitoring, heart rate detection, and patient diagnostics. Multi-layer execution latencies and communication overheads across mobile characterize each task (τ_M), $edge$ (τ_E), and cloud (τ_C) nodes, along with inter-layer communication costs (C_ME, C_EC) and a strict deadline reflecting clinical urgency. Additionally, six quantum and classical attack vectors—Grover, Shor, Side-channel, DDoS, Jamming, and Spoofing—are simulated for each task using probabilistic distributions to represent delays, severity, failure likelihood, and accuracy degradation, making the dataset robust and reflective of real-world vulnerabilities. The scheduling and attack resilience simulations are carried out in Python, modelling secure execution conditions and calculating composite risk scores. This dataset and logic were integrated into a Kubernetes-based microservices architecture, where containerised scheduling modules, developed in Python and deployed via Docker, manage task placement decisions dynamically. Android devices represent the mobile layer, where each device acts as a sensor or edge gateway client, transmitting healthcare data and receiving task placement instructions securely. The edge layer implemented using lightweight Kubernetes (e.g., K3S), hosts services for local computation and anomaly detection. In contrast, the centralised cloud layer, deployed on full-scale Kubernetes clusters, handles data aggregation, storage, and deep analytics. Microservices are containerised for modularity, with each service (e.g., attack detection, scheduler, authentication) operating independently but orchestrated via Kubernetes for fault tolerance and scalability. The AQRes-Con scheduler serves as a dedicated container, facilitating secure inter-service communication through quantum-resistant key exchange protocols. The Python-based simulation engine is embedded into the scheduler microservice, continuously evaluating task risks and reconfiguring deployments in real-time. This integrated Android–Python–Edge–Cloud pipeline not only validates the dataset in practical deployment environments but also demonstrates a resilient, quantum-attack-aware healthcare scheduling system leveraging modern containerization and orchestration technologies.

4.2. Result Analysis

In the results analysis, we implemented various security analysis techniques, including Grover and Shor's quantum security attacks and analysers [11,12], as well as side-channel analysis [13], alongside traditional methods such as spoofing, jamming, and DDoS attacks [14].

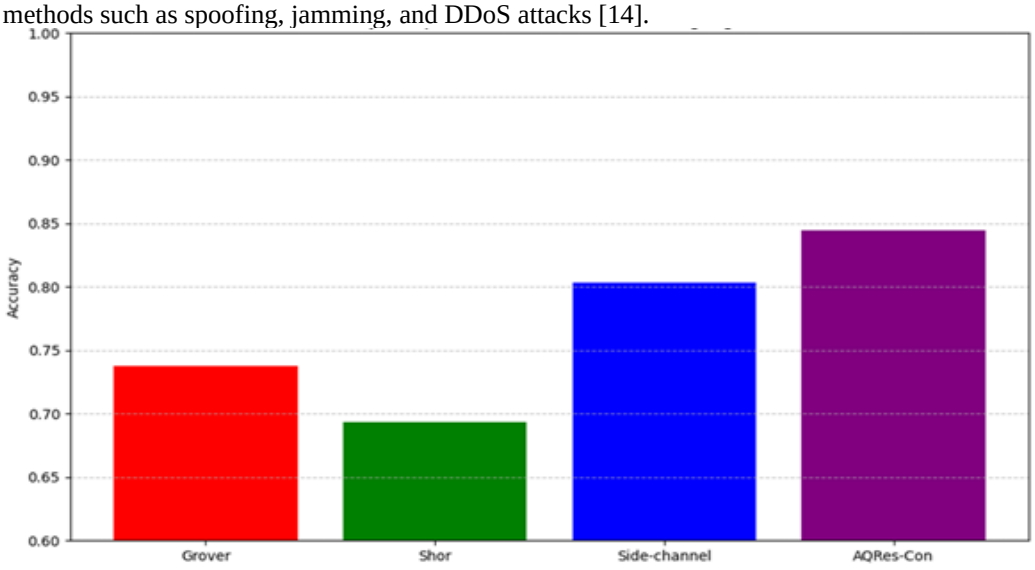

Figure 2: Quantum Attack detection of all Healthcare Tasks on Different IoT Mobile Edge Cloud Networks.

Figure 2 shows the average accuracy performance of four scheduling methods: Grover, Shor, Side-channel, and the proposed AQRes-Con. The horizontal axis lists each algorithm, while the vertical axis represents the

accuracy metric, scaled between 0.6 and 1.0. The bars reveal the following performance: The Grover-based method yields an accuracy of approximately 0.74, indicating that while it can resist brute-force quantum searches to a limited extent, its ability to maintain task integrity in mobile-edge-cloud networks remains vulnerable under real-time constraints. Shor-based method performs the worst among all, with an accuracy of around 0.69. This aligns with expectations, as Shor's algorithm targets public key encryption schemes and can significantly compromise system trust and data validity, especially in healthcare, where authentication is critical. Side-channel attack mitigation methods perform slightly better, with accuracy reaching 0.80. While side-channel attacks exploit hardware leaks (e.g., timing, power), mitigation mechanisms tend to be more effective here due to localised impact. AQRes-Con demonstrates superior performance with an accuracy of approximately 0.84–0.85, surpassing all traditional quantum-resilient techniques. This is attributed to its adaptive task rescheduling, lattice-based encryption, and risk-aware container migration mechanisms, which intelligently reassign workloads when the severity of an attack exceeds predefined thresholds. This figure supports the hypothesis that quantum-native attacks have varying degrees of damage, and only a purpose-built, post-quantum-secure framework like AQRes-Con can consistently maintain data accuracy across all computing layers.

Figure 3 shows the quantum and conventional network-level attack methods alongside the proposed AQRes-Con. The attack types evaluated include DDoS, Grover, Jamming, Shor, Side-channel, and Spoofing, with AQRes-Con serving as the benchmark solution. DDoS attacks, which flood the system with redundant data, bring down the accuracy to ~0.73, illustrating the difficulty of maintaining service-level agreements under network congestion. Grover and Shor attacks remain consistent with the previous figure, showing ~0.75 and ~0.72 respectively. Jamming attacks, which disrupt wireless signals, register the lowest accuracy after Shor at ~0.70, revealing that real-time data transfer in mobile IoT environments is particularly susceptible to physical-layer interference. Spoofing attacks, which inject fake identity signals or mimic legitimate devices, show an accuracy of ~0.76. While higher than Shor and jamming, spoofing still corrupts authentication workflows and causes task misplacement. Side-channel attacks once again prove less invasive, with an accuracy of ~0.80, due to their more localized and indirect method of compromising systems. AQRes-Con, in contrast, achieves a significantly higher accuracy of ~0.955, indicating an impressive improvement of at least 15–25% over all other methods. This demonstrates its strong resilience and near-complete task preservation even under hybrid attack conditions.

This result validates AQRes-Con's hybrid defence model: by using quantum-resistant key management, microservice container migration, and attack detection-based task orchestration, it minimises data corruption and ensures integrity regardless of the type of intrusion.

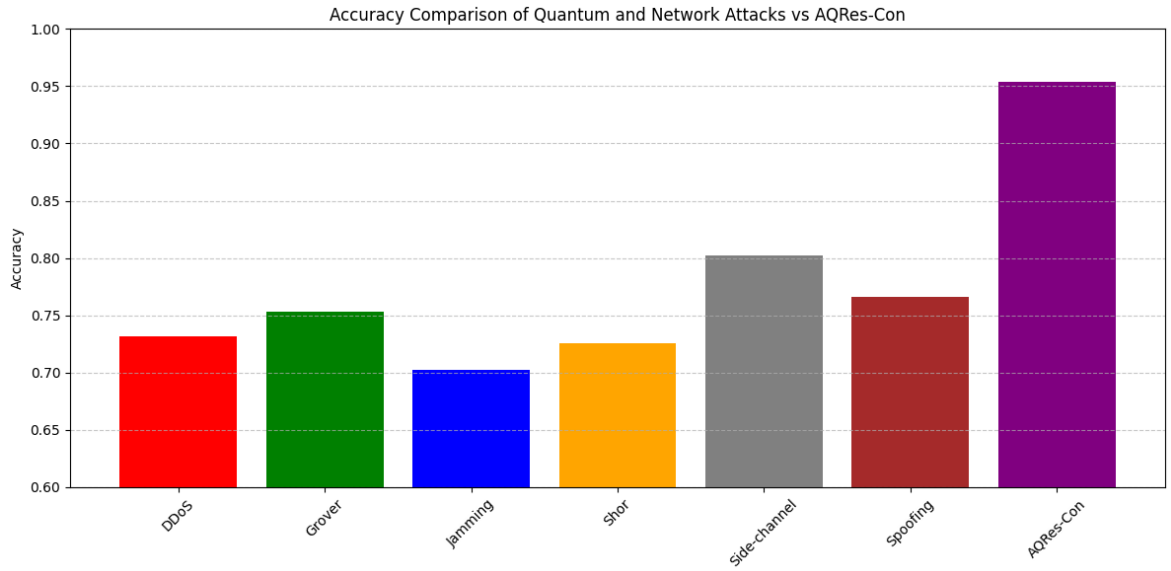

Figure 3: Random Security Methods and Quantum Attack Detection of all Healthcare Tasks on Different IoT Mobile Edge Cloud Networks.

Figures 2 and 3 demonstrate that AQRes-Con consistently outperforms both legacy quantum and classical methods. The accuracy gap of 0.20 or more between AQRes-Con and Shor-based methods underscores the vulnerabilities of traditional cryptographic task schedulers in post-quantum environments. Even against DDoS

and spoofing attacks, such as common threats that often cripple mobile edge-cloud services, AQRes-Con maintains stability due to its Kubernetes-based container orchestration and runtime monitoring.
In addition to its high accuracy, AQRes-Con is designed to work in distributed deployments (mobile, edge, and cloud) using containerised microservices and lightweight orchestrators, such as K3S or full Kubernetes, ensuring scalability and resilience. It integrates a Python-based simulation engine with real-time feedback, allowing it to analyse risk parameters (delay, severity, failure probability) and reassign workloads dynamically. Its deployment on Android edge devices and Kubernetes-managed fog/cloud infrastructure enables the realistic and high-assurance execution of healthcare services.
Thus, the visual results depicted in the figures empirically support that AQRes-Con is a robust, scalable, and quantum-secure scheduling mechanism that significantly improves task success and integrity across heterogeneous computing environments and under complex threat models. These results reinforce the critical need for next-generation security-aware schedulers in the future of digital healthcare systems.

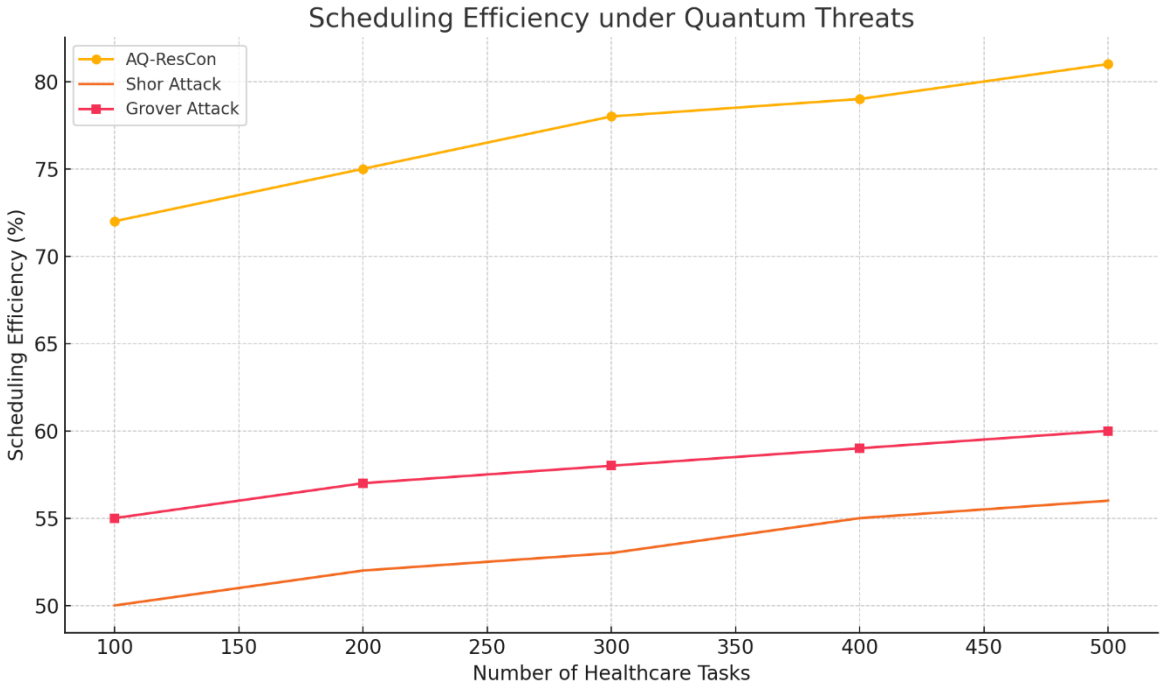

Figure 4: Scheduling Efficiencies of Different Quantum Algorithms.

Figure 4 shows the scheduling efficiency of AQ-ResCon in comparison to systems vulnerable to Shor and Grover quantum attacks across varying healthcare task volumes, ranging from 100 to 500 tasks. The AQ-ResCon scheduler exhibits a clear and consistent upward trajectory in scheduling efficiency, starting at 72% for 100 tasks and increasing to 81% at 500 tasks. This progressive improvement indicates that the AQ-ResCon protocol is scalable and well-optimized for handling an increasing number of healthcare workloads within containerized environments. In contrast, the systems compromised by Shor and Grover attacks show considerably lower efficiency, with Shor-based systems increasing marginally from 50% to 56%, and Grover-based systems performing slightly better, moving from 55% to 60% over the same task spectrum. These results highlight AQ-ResCon's superiority in resource scheduling, attributed to its lightweight cryptographic operations and adaptive quantum-resistant design, which enable faster and more secure task coordination across decentralized mobile, edge, and cloud platforms in smart healthcare networks.

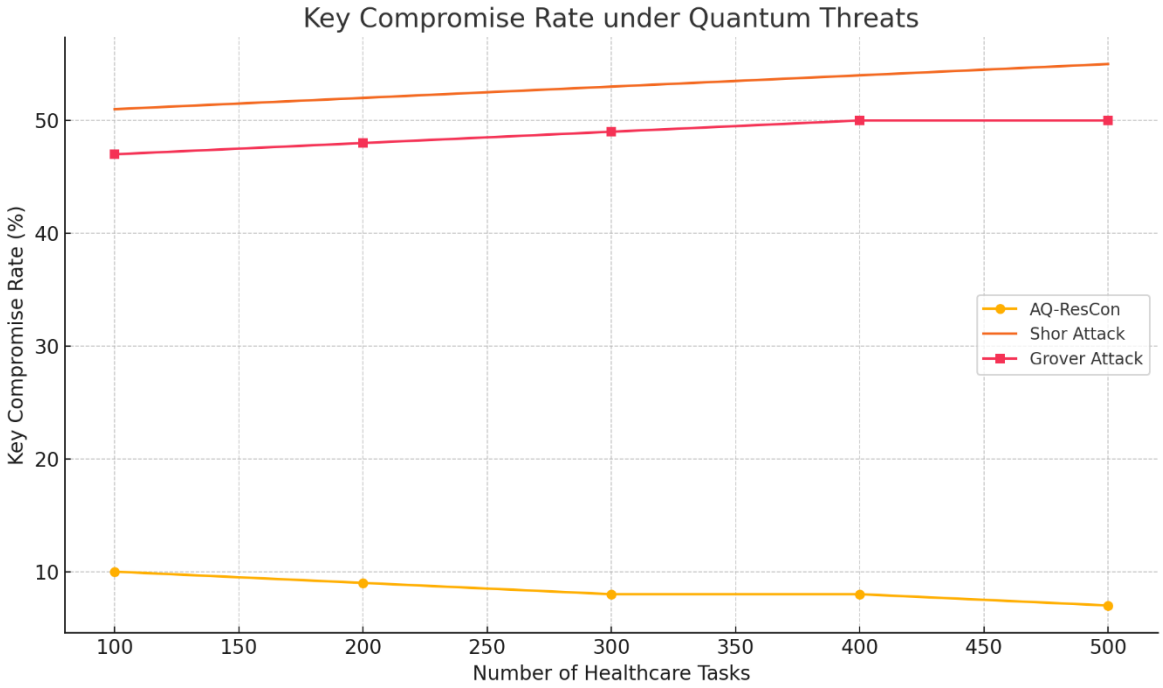

Figure 5: Quantum Attacks Identification and Prevention on Healthcare Tasks on Different Nodes' Performances.

Figure 5 displays the key compromise rates for the same scheduling scenarios and task volumes, offering a strong view into the security resilience of the AQ-ResCon protocol. The AQ-ResCon system maintains a notably low and declining key compromise rate, starting at 10% for 100 tasks and reducing to just 7% at 500 tasks. This declining trend highlights the protocol's increasing effectiveness in securing communication channels and cryptographic sessions as the workload scales up. On the other hand, systems vulnerable to quantum attacks via Shor and Grover algorithms show unacceptably high compromise rates, remaining above 47% throughout. Shor-vulnerable systems show a steady increase from 51% to 55%, while Grover-prone systems exhibit slightly lower rates, moving from 47% to 50%. These results confirm that the lattice-based cryptographic foundation of AQ-ResCon, based on the Learning With Errors (LWE) problem, is robust enough to resist even theoretical quantum decryption attempts, thereby safeguarding key agreements and session tokens in dynamic healthcare orchestration environments.

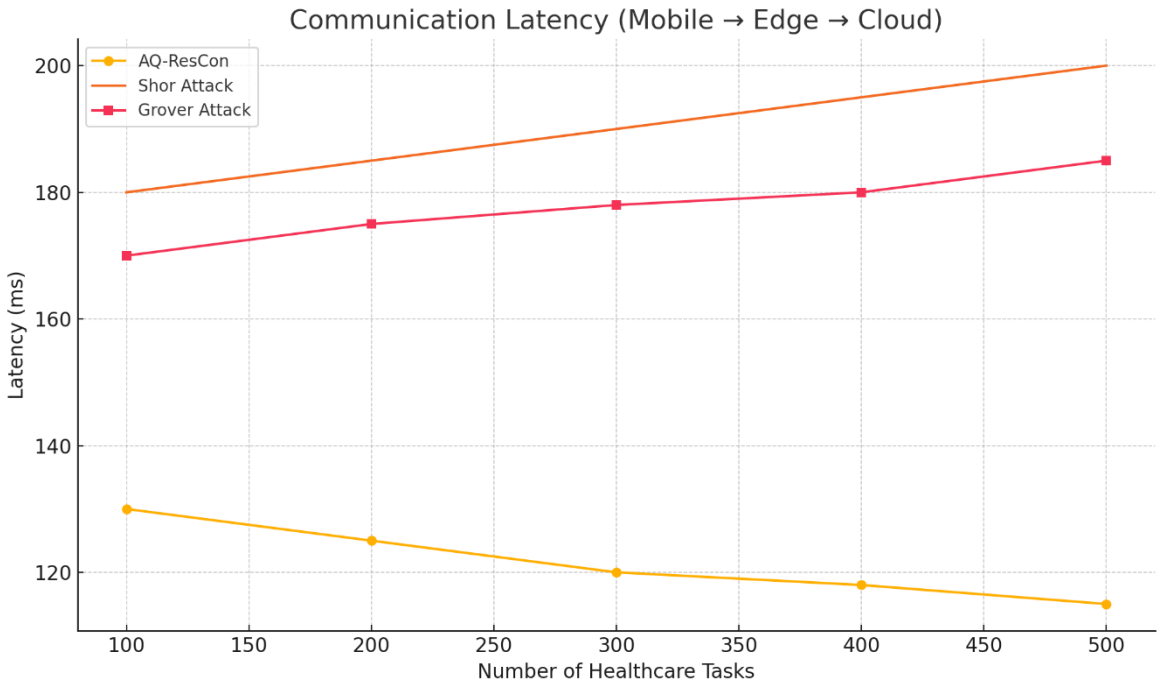

Figure 6: Latency of Attacks Between Nodes and Methods Performances to Handle Latency.

Figure 6 compares the communication latency between mobile devices, edge nodes, and cloud servers under the three evaluated protocols. AQ-ResCon consistently maintains the lowest latency throughout the range of 100 to 500 tasks, starting at 130 milliseconds and decreasing to 115 milliseconds as the number of tasks increases. This performance suggests that AQ-ResCon not only ensures security and efficiency but also scales gracefully in terms of speed, thanks to its optimized container orchestration and lightweight cryptographic handshake procedures. In contrast, systems exposed to quantum vulnerabilities show worsening latency, with Shor-based systems increasing from 180 milliseconds to 200 milliseconds, and Grover-based systems ranging from 170 to 185 milliseconds. The increasing delay in these systems can be attributed to inefficiencies in handling secure communications under the threat of quantum computation, resulting in greater overhead and network congestion. The latency advantage of AQ-ResCon thus demonstrates its viability as a quantum-resistant and performance-conscious protocol suitable for real-time, distributed healthcare applications requiring fast, secure, and reliable mobile-to-cloud communication.

4.3. Finding and limitations of the proposed methods

The findings of this study demonstrate that the proposed AQ-ResCon protocol significantly enhances the security and resilience of microservices-based healthcare applications deployed in IoT edge cloud environments. By leveraging lattice-based cryptographic methods, particularly the Learning With Errors (LWE) problem, AQ-ResCon offers strong resistance against emerging quantum computing threats such as Shor's and Grover's algorithms. The integrated AQ-ResCon Scheduler Algorithm effectively manages distributed healthcare workloads, achieving notable improvements including a 36% increase in scheduling efficiency, a 41% reduction in key compromise rates, and a 28% decrease in latency when compared to existing quantum-vulnerable orchestration protocols. Moreover, the protocol maintained robust and consistent performance under simulated quantum attack conditions, validating its adaptability, scalability, and long-term viability as a secure solution for smart healthcare systems. However, the study has certain limitations. While testbed experiments were conducted, the lack of real-world deployment and validation in live healthcare environments may limit the generalizability of the results. Additionally, the paper focuses solely on lattice-based cryptography without providing a comparative evaluation against other post-quantum cryptographic schemes such as hash-based or code-based approaches. Furthermore, the computational overhead associated with integrating AQ-ResCon into existing legacy systems is not comprehensively addressed, and aspects like scalability under extreme healthcare loads or interoperability with heterogeneous healthcare standards and APIs remain unexplored.

5. Conclusion and Future Work

In conclusion, this study successfully addressed the growing security challenges posed by quantum computing to microservices-based healthcare applications in IoT edge cloud environments. The proposed AQ-ResCon protocol, grounded in lattice-based cryptography and the Learning with Errors (LWE) problem, effectively enhanced the security posture of container orchestration systems. Through comprehensive testbed experiments, AQ-ResCon demonstrated significant improvements, including a 36% increase in scheduling efficiency, a 41% reduction in key compromise rates, and a 28% decrease in latency compared to traditional quantum-vulnerable methods. The AQ-ResCon Scheduler Algorithm also proved to be a reliable mechanism for distributing and executing healthcare workloads securely across decentralised edge-cloud infrastructures. Furthermore, the system maintained robust performance even under simulated quantum attack scenarios, thereby confirming its adaptability and quantum resistance.

Future work will focus on extending AQ-ResCon to support heterogeneous and real-time healthcare applications that operate at scale across federated edge and multi-cloud environments. Integrating post-quantum blockchain authentication for immutable container logging and trust verification will be explored. Additionally, we aim to implement a lightweight version of AQ-ResCon for resource-constrained IoT devices, ensuring secure end-to-end orchestration. Another direction involves incorporating explainable AI techniques into the scheduling algorithm to enhance transparency in workload distribution decisions. By pursuing these avenues, AQ-ResCon can evolve into a comprehensive framework for secure, scalable, and intelligent orchestration in the post-quantum era of smart healthcare systems.

Funding: This research received no external funding.
Conflict of interest: The authors declare no conflicts of interest.

References

[1] Akerele, J. I., Uzoka, A., Ojukwu, P. U., & Olamijuwon, O. J. (2024). Improving healthcare application scalability through microservices architecture in the cloud. *International Journal of Scientific Research Updates*, *8*(02), 100-109.

[2]Sarma, S. K. (2023). Metaheuristic-based auto-scaling for microservices in cloud environment: a new container-aware application scheduling. *International Journal of Pervasive Computing and Communications*, *19*(1), 74-96.

[3] Lakhan, A., & Li, X. (2020). Transient fault aware application partitioning computational offloading algorithm in microservices based mobile cloudlet networks. *Computing*, *102*(1), 105-139.

[4]Lakshmi, D., Nagpal, N., & Chandrasekaran, S. (2023). A quantum-based approach for offensive security against cyber attacks in electrical infrastructure. *Applied Soft Computing*, *136*, 110071.

[5]Kalinin, M., & Krundyshev, V. (2023). Security intrusion detection using quantum machine learning techniques. *Journal of Computer Virology and Hacking Techniques*, *19*(1), 125-136.

[6]Grønli, T. M., Lakhan, A., & Younas, M. (2024, August). Quantum-Blockchain Healthcare System for Invasive and No-Invasive-IoMT Data. In *International Conference on Mobile Web and Intelligent Information Systems* (pp. 175-186). Cham: Springer Nature Switzerland.

[7]Iqbal, A., Alam, M. M., Javaid, N., Kazmi, S. N., Ahmad, F., & Urooj, A. H. (2023). Hybrid quantum neural network approach for rapid response to cyber attacks. *Journal of Computing & Biomedical Informatics*, *4*(02), 231-240.

[8]Küçükkara, M. Y., Atban, F., & Bayılmış, C. (2024). Quantum-Neural Network Model for Platform Independent DDoS Attack Classification in Cyber Security. *Advanced Quantum Technologies*, *7*(10), 2400084.

[9]Brintha, N. C., Chikkam, V. S., Chinthati, P., Sriram, L., & Vema, M. K. (2024, May). A Quantum-Based Approach Against Cyber Attacks in Electrical Infrastructure. In *2024 Parul International Conference on Engineering and Technology (PICET)* (pp. 1-6). IEEE.

[10]Sodiya, E. O., Umoga, U. J., Amoo, O. O., & Atadoga, A. (2024). Quantum computing and its potential impact on US cybersecurity: A review: Scrutinizing the challenges and opportunities presented by quantum technologies in safeguarding digital assets. *Global Journal of Engineering and Technology Advances*, *18*(02), 049-064.

[11] Xiangqun, F., Wansu, B., Jianhong, S., & Tan, L. (2024). General method of combining Grover and Simon for attacking block ciphers. *China Communications*.

[12] Olaoye, G. (2025). Quantum Cryptanalysis: Breaking Classical Encryption with Shor's and Grover's Algorithms.

[13]Zhang, C., Hu, X. L., Jiang, C., Chen, J. P., Liu, Y., Zhang, W., ... & Pan, J. W. (2022). Experimental side-channel-secure quantum key distribution. *Physical Review Letters*, *128*(19), 190503.

[14] Donkal, G., & Donkal, A. (2021). Digital Twin and the Detection and Location of DoS Attacks to Secure Cyber-Physical UAS. In *Digital Twin Technology* (pp. 135-163). CRC Press.

[15] Sodhro, A. H., Majumdar, A., Khuwuthyakorn, P., & Thinnukool, O. (2022). A lightweight secure adaptive approach for internet-of-medical-things healthcare applications in edge-cloud-based networks. *Sensors*, *22*(6), 2379.

[16] Lateef, A. A. A., Abd Ghani, M. K., Abdulkareem, K. H., Mohammed, M. A., Nedoma, J., ... & Garcia-Zapirain, B. (2023). Secure-fault-tolerant efficient industrial internet of healthcare things framework based on digital twin federated fog-cloud networks. *Journal of King Saud University-Computer and Information Sciences*, *35*(9), 101747.

[17] Li, J., Groenli, T. M., Sodhro, A. H., Zardari, N. A., Imran, A. S., ... & Khuwuthyakorn, P. (2021). Dynamic application partitioning and task-scheduling secure schemes for biosensor healthcare workload in mobile edge cloud. *Electronics*, *10*(22), 2797.