



The Future of Cloud Security: Integrating Quantum-Resistant AI-Powered Solutions

Nandan Sharma^{1[0009-0000-7393-2077]} and Ritul Agrawal^{2[0009-0000-2241-1685]}

¹Senior Cyber Security Leader and Researcher, BC Public Service, Victoria, Canada

²Department of Electronics and Communication, Azad Institute of Engineering Technology, Lucknow, UP
nandans24@yahoo.com

Abstract. The fast merging of quantum computing and artificial intelligence is bringing significant changes to cloud security. We must create new, quantum-secure approaches because quantum computers are set to crack the present encryption standards. At the same time, AI makes it easier to detect and manage threats, analyze unusual activity, and organize security in today's advanced cloud systems. In this paper, we present a way to implement cloud security by pairing post-quantum cryptography with the help of AI systems. It examines machine learning happening in predictive analysis, automated reaction, and secure system construction, together with methods to preserve data integrity in the future using quantum-safe encryption. The study demonstrates that hybridization could significantly improve enterprise and governmental systems as we prepare for a situation after quantum computing is uncovered.

Keywords: AI-Powered Cloud Security, Cloud Security Automation, Machine Learning in Cybersecurity, Post-Quantum Encryption, Quantum-Resistant Cryptography.

(Article history: Selected papers from NIELIT's International Conference on Communication, Electronics and Digital Technologies (NICE-DT'26), 29-30Jan, 2026, Gorakhpur, India)

1 Introduction

Modern enterprise infrastructure has changed thanks to cloud computing, which supplies on-demand resources for storage, services, and program delivery. A side effect is that the threat to computer systems has increased, so stronger and ever-changing security is now needed. Most current cloud security frameworks depend on regular encryption, set access control, and detection of threats that happen after they start rather than before [1], [6]. With the progress of quantum computing, RSA and ECC, popular cryptographic algorithms, are likely to face a significant risk. Algorithms developed by Shor and Grover, if implemented, mean security models would be cracked rapidly [4], [15], [21]. Because of this expected change, there is now a rush to investigate post-quantum cryptographic (PQC) strategies that resist threats from quantum adversaries [10], [12], [26]. At the same time, the growing use of AI is affecting how we think about cloud security. As a result of AI, organizations can use ML, spot unusual patterns, and analyze actions to detect and prevent unfamiliar and sophisticated threats [2], [3], [8]. Still, adversarial AI and model poisoning create issues for cybersecurity that traditional tools have trouble managing [11], [27]. These two trends in technology have created a need for a new way to keep our cloud systems secure. By integrating security methods immune to quantum attacks with AI-based tools that support automation, we have a ground for ensuring cyber security against both existing and future threats [5], [9], [22]. When used together, AI's ability to predict and adapt with quantum-safe encryption can allow cloud systems to grow from merely responding to attacks into systems that can automatically protect and repair themselves.

This paper investigates in detail how quantum-hard and AI-powered security techniques are used in cloud computing systems. Part 2 takes a look at what has been published on cloud security, security with AI tools, and the use of post-quantum encryption. Part 3 covers how PQC is built and put into action. This section examines how AI can help organizations fight against cloud-based threats sooner. The authors suggest linking these technologies into a comprehensive framework in Section 5. Section 6 explores the problems, constraints, and evolving patterns related to implementation. Key results and suggestions for future development and application are found in Section 7.

2 Background and related work

2.1 Evolution of Cloud Security Technologies

As more services are offered via the cloud, cloud security is changing from protecting only the main network to also monitoring other details in the environment. Only a few years ago, data protection in cloud systems relied largely on firewalls, access control lists that never changed and basic encryption. Still, the number of cyber-attacks against multi-tenant environments

means that smarter and more efficient security is now necessary. As the cloud industry has grown, Security as a Service (SE-CaaS), containers, and cloud-native zero-trust systems have made essential achievements [6], [18], [24]. Since DevOps and virtual environments are common, it is now important to automate security controls to both ensure policies are followed and to quickly handle risks as they arise [25], [30].

2.2 Quantum Computing Fundamentals and Implications for Cryptography

Superposition and entanglement are the fundamental principles of quantum computing, which reshape how tasks are computed. Both integer factorization and discrete logarithms require fast processing, and this is possible with qubits, unlike classical bits, because these calculations are beyond their capabilities. It is mostly Shor's algorithm that creates the threat to RSA and ECC, so the cryptographic community is working on new cryptography that will withstand quantum computers [4], [15]. Because of the new cybersecurity threats, scientists are working more on quantum-resistant methods called lattice-based, multivariate polynomial, and hash-based cryptography [5], [12], [21]. Discovering ways to add post-quantum cryptography into cloud systems is still tricky because of matters like dealing with big keys and processing requirements, and there are no set protocols [10], [26].

2.3 AI Applications in Cybersecurity and Cloud Environments

AI, mainly machine learning (ML) and deep learning (DL), has greatly advanced how we find and respond to threats and look for anomalies. By studying patterns and how data connects, AI systems can notice new types of attacks, deal with continuing changes in attacks, and assist with live protection strategies [2], [3], [7]. Dynamic risk scoring, identifying checking, spotting unwanted access, and tracking resource usage are aided by AI in cloud services [13], [20], [22]. Thanks to AI, explainable machine learning and adversarial defense systems are now possible, though issues of algorithmic bias, overfitting, and model transparency are still unresolved [8], [11], [27].

2.4 Summary of Key Related Research and Existing Gaps

Post-quantum encryption is being studied for use in things like IoT and cloud systems these days, as well as for detecting both malware and threats from within a group [2], [9], [13]. Even though research has looked into making cryptography and AI work together for adaptive security [16], deploying solutions with both quantum resistance and AI is not widespread. Among the difficulties are that there are no strongly unified frameworks for merging PQC and AI in cloud systems, and it is harder to manage AI and PQC on cloud services due to the high processing costs of PQC techniques [14] [19] [28]. Dealing with these concerns makes cloud systems more secure, scalable, and ready for the future.

Table 1.Summary of key research in cloud security, quantum computing, and AI integration.

Area	Key Contributions	Representative Works	Identified Gaps
Cloud Security Evolution	Shift from perimeter-based to zero-trust models; integration of automated security frameworks and access control	[6], [18], [24], [25], [30]	Lack of seamless integration with quantum-resistant algorithms and intelligent automation
Quantum Computing in Cryptography	Post-quantum cryptography models: lattice-based, hash-based, multivariate polynomial; threat of Shor's algorithm	[4], [5], [10], [15], [21], [26]	High computational overhead; challenges with key size and implementation in cloud-native environments
AI in Cloud Security	AI/ML/DL for threat detection, anomaly detection, and automation; models for real-time adaptation and pattern learning	[2], [3], [7], [8], [11], [13], [20], [22], [27]	Model interpretability, adversarial resistance, data privacy and explainability
AI + Cryptography Synergy	Research on AI-enhanced encryption and adaptive security frameworks for cloud	[9], [12], [14], [16], [19], [28]	Few unified solutions combining AI and post-quantum cryptography; lack of

	and IoT environments		industry-standard deployments
Research Gaps and Opportunities	Increased need for integrated, scalable, quantum-resilient AI security architecture	Synthesized from all references	Need for standardized PQ-AI frameworks, reduced latency, cost-effective deployment strategies

3 Quantum-Resistant Cryptographic Techniques

Quantum computing brings a significant change in how we do computing. Even in development, quantum systems could become so powerful that existing public-key cryptosystems will no longer be secure. By using Shor's algorithm, quantum computers speed up the breaking of RSA, DSA, and ECC cryptographic methods because they can quickly factor large integers and compute discrete logarithms [15], [21]. Because this threat is so timely, Post-Quantum Cryptography (PQC) has been developed to handle both traditional and quantum computer attacks.

3.1 Overview of Post-Quantum Cryptography (PQC)

Post-quantum cryptography means there are cryptographic protocols that keep data safe against traditional computers and quantum computers. Differential-quantum cryptography doesn't depend on integer factorization and discrete logarithms, which quantum computers can attack. Such calculations are believed to be secure since these problems are seen as tough for quantum computers, e.g:

- Some areas in cryptography involve solving problems like the Learning With Errors (LWE) and the Shortest Vector Problem (SVP).
- Random linear codes which are solved by coding techniques, qualify as code-based problems.
- Multivariate quadratic equations
- Hash-based constructions
- Isogenies between elliptic curves [15], [21]

Many people have been paying close attention to lattice-based cryptography because it is supported by strong science and fits several types of encryption uses. It supports both encryption and digital signature schemes, and implementation in software and hardware is efficient. In their study [10], they explain that specific assumptions about quantum computers make lattice-based schemes naturally resistant to quantum decryption.

Currently, PQC is used to secure file storage, send encrypted messages, use blockchain technologies, and develop Internet of Things (IoT) gadgets. Since PQC is mandatory for anyone who handles and protects key data and assets, cloud service providers are considering using Post-Quantum Cryptography [4], [5].

3.2 NIST-Standardized PQC Algorithms

Many people have been paying close attention to lattice-based cryptography because it is supported by strong science and fits several types of encryption uses. It supports both encryption and digital signature schemes, and implementation in software and hardware is efficient. Their study [10] explains that specific assumptions about quantum computers make lattice-based schemes naturally resistant to quantum decryption.

Currently, PQC is used to secure file storage, send encrypted messages, use blockchain technologies, and develop Internet of Things (IoT) gadgets. Since PQC is mandatory for anyone who handles and protects key data and assets, cloud service providers are considering using Post-Quantum Cryptography [4], [5].

- CRYSTALS-Kyber: A lattice-based key encapsulation mechanism (KEM)
- CRYSTALS-Dilithium: A lattice-based digital signature scheme.
- Falcon: A compact and fast signature scheme
- SPHINCS+: A stateless hash-based signature scheme
- Classic McEliece: A code-based KEM known for its long history and robustness [15]

Standards makers chose every algorithm according to security, how fast it performed, how much data it handled, its resistance to attacks, and how simple it was to use. One good example is Kyber, which is noted for its efficient and strong ability and fits well with the cloud-based TLS system [15], [21].

Table 2. Characteristics of selected nist-standardized pqc algorithms.

Algorithm	Category	Key Size (bytes)	Ciphertext Size (bytes)	Use Case
CRYSTALS-Kyber	Lattice-based	~800–1500	~700–1500	Key Exchange
CRYSTALS-Dilithium	Lattice-based	~1300–2700	~2400–4600	Digital Signatures
Classic McEliece	Code-based	~250,000	~128	Long-term Encryption
Falcon	Lattice-based	~900–1800	~650–1300	Compact Signatures
SPHINCS+	Hash-based	~32,000	~8,000	Stateless Signatures

(Adapted from [10], [15], [21])

3.3 Suitability and Challenges of PQC for Cloud Infrastructures

When you add PQC to existing cloud systems, there are many opportunities and important barriers. PQC can provide strong security against quantum attacks, but when used in the cloud, it must meet requirements for speed, working well with different systems, expense, and ability to grow.

- Performance Considerations**
 Cloud platforms are designed for high throughput and low latency. Many PQC algorithms—particularly lattice-based schemes like Kyber—demonstrate good performance in software and are competitive with classical algorithms in terms of key generation, encryption, and decryption speed [26]. However, others, like Classic McEliece, suffer from impractically large public keys that hinder performance in memory-constrained environments [21].
- Integration Complexity**
 A significant challenge is making sure programs work on older systems. TLS, IPsec and VPN protocols very much depend on the use of RSA and ECC in their operations. Either a combination of classical and PQC schemes (hybrid implementation) or a new approach to protocol design is needed for PQC. To make these updates happen, everything needs to be upgraded on all endpoints, APIs and hardware accelerators which is both complex and costly [4], [5].
- Resource Overhead**
 PQCs may require more resources in cloud systems, which results in more energy use and higher costs. As an example, encryption algorithms in PQC usually require much bigger signatures and keys than those in other cryptosystems, so bandwidth is used more, memory is taken up more, and communication protocols take longer to start [15], [10].
- Security Risks and Implementation Challenges**
 Although PQC is created to avoid quantum attacks, it can still be hurt by classical side-channel and implementation attacks. Papers such as [12] and [21] have revealed that, if implemented poorly, Public Key Cryptography (PQC) schemes could become vulnerable to timing, power analysis, and fault injection attacks. Another reason secure implementation matters a lot is that in shared, multi-tenant cloud environments, sensitive information could be leaked by the hardware itself.
- Compliance and Regulation**
 The changes in encryption and cloud services regulations might make it difficult to adopt PQC. Both governments and regulatory agencies may enforce limits on key lengths, types of algorithms, and where data may be stored, and cloud service providers must follow these restrictions. Missed opportunities to make sealing of PQC common in all jurisdictions might persist, and adoption can get divided or delayed because of uncertain laws [15], [23].

All in all, though PQC makes cloud security against quantum threats possible, implementing it is not easy. For a smooth shift, the industry needs strategic planning, testing, and teamwork. Besides using PQC, adaptive orchestration, and AI-based security monitoring are also necessary to ensure that overall cloud security remains high after the move to quantum computing.

Table 3. Suitability and implementation challenges of pqc in cloud infrastructures.

Dimension	Advantages	Challenges
Performance	Efficient algorithms like Kyber and Dilithium	High bandwidth and latency for large key/signature schemes like SPHINCS+

Integration	Potential hybrid protocols for phased adoption	Requires protocol redesign, affects TLS, VPN, IPsec, etc.
Compatibility	Can be gradually integrated alongside classical crypto	Legacy systems may require extensive reengineering
Resource Efficiency	Some lattice schemes are compact and performant	Others (e.g., McEliece) require significant storage and memory
Security Against Quantum	Designed to resist quantum attacks	Vulnerable to classical side-channel and implementation attacks
Regulatory Compliance	Aligns with NIST PQC standards	Lack of global standardization may hinder cross-border cloud deployments

Source: Synthesized from [4], [10], [12], [15], [21], [23], [26]

4 AI-driven security in the cloud

4.1 Role of Machine Learning and Deep Learning in Cloud Security

Through technologies like machine learning (ML) and deep learning (DL), AI has improved how cloud security is handled. ML models differ from traditional rules because they can analyze much data to point out unusual patterns that might show threats. Spam classifiers depend on supervised learning, clustering, and reinforcement learning methods for high success in identifying and predicting attacks [3], [7]. CNNs and RNNs, which fall under deep learning, have drawn attention as they can model many different and detailed user actions and network patterns. These models can automatically find features that suggest covert attacks, such as Advanced Persistent Threats (APTs) and zero-day exploits [8], [11]. Another example is how autoencoders have been used to spot unusual activities in computer systems without providing labeled information [27]. Because AI models are adaptable and can constantly learn, they are naturally well-matched for cloud settings, which experience swift changes in threats. Because cloud services can expand easily, AI algorithms can also grow to keep an eye on all the assets in the network [2], [13].

4.2 Real-Time Threat Detection and Behavioral Analysis

An important way AI helps in cloud security is by spotting threats in real-time. Reviewing login activity, requests to the system, and transfers of files allows AI to identify anything suspicious that might be a threat. An intrusion detection system driven by ML can catch breaches in real-time, which means it takes less time for attackers to gain access to your network [8], [16]. Looking at behavior is very important when studying undercover agents. AI can spot when someone's actions differ from the standard, which could mean their account has been compromised or they are acting as an insider threat. Bayesian inference, clustering, and scoring anomalies are some of the techniques that enable finding unusual actions almost instantly [3], [27]. It works much better than rules with less risk of wrongly accepting a false positive.

Technologies, for example Hawk-Eye [2], that depend on AI-driven monitoring show that ML helps improve awareness of risks and potential threats. Adding natural language processing (NLP) to the system helps it analyze unsorted logs, signs of social engineering and similarities in phishing, making its security more complete.

4.3 AI for Automated Incident Response and Predictive Defense

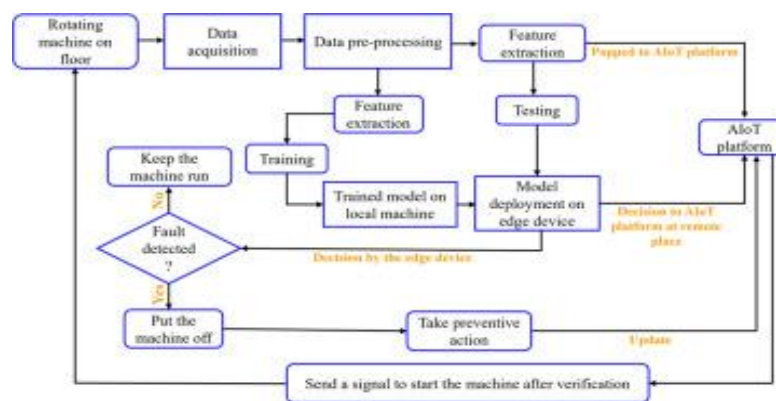
AI is making a major difference in cloud-based incident response. Using automation, AI is able to spot risks and also work through predefined solutions, including isolating different tasks, taking back access tokens, or launching investigative routines [9], [20]. As a result, Mean Time to Response (MTTR) is significantly reduced, and the damage from attacks is minimized.

AI-based models and information from previous threats help cloud systems predict what may happen in the near future. For example, using Support Vector Machines (SVMs) and time series analysis, it is possible to spot indicators of compromise (IoCs) ahead of attacks, making it easier to plan preventive actions [7], [16].

Also, these AI-powered tools use threat intelligence, vulnerability databases, and network data to give an automated and complete response. With experience from past events and ongoing model updates, these platforms can provide almost automatic protection and solutions for cloud infrastructure [13, 26].

Table 4. AI applications in cloud security and their functional contributions.

AI Application Area	Techniques Used	Primary Function	Example Studies
Threat Detection	Super-vised/Unsupervised ML, Clustering, Anomaly Detection	Identifies potential intrusions based on pattern recognition and deviations	[3], [8], [11]
Behavioral Analysis	Bayesian Inference, Autoencoders, User Profiling	Monitors and flags anomalous user behaviors indicating account compromise	[2], [27]
Real-Time Monitoring	Stream Analytics, CNNs, Recurrent Models	Continuously evaluates system events to detect and respond to threats immediately	[16], [20]
Automated Incident Response	AI Orchestration Engines, Rule-Based Automation + ML Tuning	Triggers predefined defensive actions to contain or mitigate breaches	[9], [13]
Predictive Defense	Time Series Forecasting, SVMs, Historical Threat Modeling	Anticipates future threats and enables proactive security hardening	[7], [20], [26]
Natural Language Log Processing	NLP + DL Models (e.g., Transformers)	Analyzes logs, messages, and phishing data for semantic indicators of threats	[2], [27]


Fig. 1. AI-based threat detection and response pipeline in cloud environments.

5 Integrated framework for quantum-resistant ai security

5.1 Architectural Design of the Combined AI + PQC System

Safeguarding and managing cloud infrastructures more effectively is possible thanks to new artificial intelligence and post-quantum cryptographic (PQC) advances. In architecture, AI analysis works together with a modular framework that can incorporate both lattice and code-based encryption. There are three primary levels, or layers, in the system architecture:

1. **Data Protection Layer:** Standard PQC recommendations from NIST, such as Kyber for encryption and Dilithium for signatures, are used to maintain the safety of data whether it is stored or sent [4], [10], [15]. **AI-Driven Detection Layer:** Incorporates supervised and unsupervised machine learning (ML) models for real-time anomaly detection. This layer continuously monitors traffic patterns, user behavior, and system logs to identify potential breaches [3], [8], [11].
2. **Control and Orchestration Layer:** Channels communications between the PQC and AI parts. This level ensures that rules are updated and automated solutions are provided when new threats are detected [9], [27].

AI analytics and quantum-resistant encryption together improve the detection speed and ability of the cloud infrastructure to handle threats, looping the process of preventing and handling attacks.

5.2 Architectural Design of the Combined AI + PQC System

Inside this framework, data flow begins at the ingress point, and each incoming packet is sorted by an AI engine for possible security issues. If a source is considered suspicious, the flow of data is turned to a sandbox environment for further examination of its actions. So, data without a clearance level can be encrypted using PQC methods and proceed to be processed or stored safely. All encryption work is managed by a quantum-safe key management system (Q-KMS) that produces and shares keys compatible with lattice-based and code-based protocols. The keys are rotated in regular cycles with the help of AI to save identified keys and make attacks by hackers less likely [10], [21], [26].

Log classification uses convolutional neural networks (CNNs), and the prediction of event sequences employs recurrent neural networks (RNNs). Choosing what events to address is done with decision trees. Feeding the system with updated logs and new zero-day data ensures it's very good at pinpointing all kinds of threats [2], [8], [13].

5.3 Application Scenarios in Enterprise and Government Sectors

Many sectors that need strong security rely on the combined AI + PQC system:

- **Enterprise Cloud Environments:** They may use this framework to ensure that customer data, financial transactions, and operational analytics are secure. By using AI modules, you can recognize insider threats, making sure sensitive documents stay confidential for years to come, thanks to PQC [7], [20].
- **Government Agencies:** It will be useful to use inspired and AI-powered threat monitoring with advanced quantum-safe communication inside national defense and intelligence departments. With this structure, information can be exchanged safely within departments, and cyber espionage can be found easily [9], [15], [21].
- **Healthcare and Critical Infrastructure:** One way healthcare uses quantum-safe security is by safeguarding electronic medical records (EMRs) with advanced encryption and catching unusual activities that could be signs of wrongdoing through AI [13], [18].

Table 5.Components of the integrated quantum-resistant AI security framework.

Layer	Component	Function	Technologies Used
Data Protection Layer	PQC Engine	Encrypts data-at-rest and data-in-transit using post-quantum algorithms	Kyber, Dilithium, Falcon [4], [10], [21]
	Quantum-Safe Key Management (Q-KMS)	Handles key generation, distribution, and rotation	AI Forecasting + PQC Libraries [10], [26]
AI-Driven Detection Layer	Anomaly Detection Engine	Monitors traffic, behavior, and logs for irregular patterns	SVM, CNN, RNN [3], [8], [11]
	Threat Intelligence Aggregator	Collects external threat feeds and updates detection models	Threat Feeds + ML Pipelines [9], [27]
Control and Orchestration Layer	Policy Management Unit	Dynamically adjusts access and mitigation policies	Reinforcement Learning [9], [11]
	Incident Response Orchestrator	Automates actions like quarantining and alerting	AI-Scripted Runbooks [2], [8]
Cross-Layer Integration	Secure Communication Bus	Facilitates encrypted communication between modules	TLS+PQC Hybrid Encryption [10], [26]
	Audit and Logging Module	Maintains records for forensic analysis	Blockchain Logs, AI Summarization [13], [15]

6 Challenges, limitations, and future trends

Using quantum-resistant cryptography and AI-based security tools in the cloud creates a number of important issues that must be examined. Despite making systems more secure against tough dangers, using these technologies is difficult because they are tough to use and update

6.1 Computational Overhead and Integration Complexity

A primary obstacle to adopting Post-Quantum Cryptography (PQC) is that it requires much computation. An example of this is that most lattice-based algorithms, like Kyber and Dilithium, are much more resource-hungry in operations and memory than classical schemes like RSA and ECC [4], [10], [15]. To illustrate, if you use Kyber as the key encapsulation mechanism, both keys and the resulting ciphertexts tend to be larger, which can decrease the efficiency of cloud services [10].

Using these algorithms inside the current cloud infrastructure makes the system architecture more complex. Legacy technology might be unable to offer the resources required by PQC which would mean having to overhaul encryption libraries, mechanisms for exchanging keys and certificates [15], [21]. In addition, cloud services based on distributed structures must handle post-quantum key distribution in a way that will not introduce delay or cause problems with existing APIs [5].

The cloud security system needs machine learning and deep learning tools, as well as the right data pipelines, quick inferring, and regular updating. It is still a big challenge to make the cryptographic and AI modules work well together without losing performance or scalability [9], [22].

6.2 AI-Related Concerns (Bias, False Positives)

They depend greatly on having good data and being able to see into their algorithms. Generating extraneous warnings (false positives) and missed threats (false negatives) is a frequent problem in AI focusing on cybersecurity. Such problems may cause delays in tackling incidents, give too many unimportant alerts and worst-case scenarios, and miss true threats [7], [11], [27]. Also, AI models might reflect any biases seen in the data used to teach them, which may make their threat detection uneven. An AI model that was not trained to spot lesser-known ways of hacking could ignore examples of them. Because AI does not work the same every time, it has proven less trustworthy in dealing with zero-day attacks [8], [16].

Making cybersecurity models more understandable and interpretable using Explainable AI (XAI) is now more popular to tackle these worries [27]. Sharing explanations from XAI in live systems is rare and often too much for the system to handle.

6.3 Trends in Quantum Hardware and AI Evolution

RSA and ECC are currently protected by quantum computing since their current capabilities do not support large-scale attacks. However, developments in keeping qubits stable and accurate quantum gates may drive CRQCs within the next decade or so [15], [21]. Likewise, AI is developing fast because of self-supervised learning, new transformer networks, and AI accelerators that allow quicker and more precise threat identification. Because AI can now be suited for edge devices and live environments, its reach in the cloud has also increased [9], [14]. Because so much of tech now ties together, adaptable systems that change quickly are necessary. Such platforms must be structured to add new cryptography and AI features as they are introduced.

6.4 Future Research Directions and Regulatory Implications

In the future, new studies should focus on lightweight PQC techniques that are best suited for cloud and edge settings. A trend is toward finding hybrid techniques that offer easy transition from old to new types of cryptography [4], [26]. It is essential to design more advanced models to manage adversarial attacks, changes in data (model drift), and the issue of explainability in AI. Also, by combining federated learning with cloud security, privacy-friendly threat detection can be improved, and data leaks can be less likely [11], [27]. NIST, ISO, and ENISA are making frameworks for rules and guidelines to increase the use of PQCs and AI auditing. Ensuring that the evolving standards and data protection rules (GDPR and CCPA) are followed will be very important for organizations using these technologies [6], [15].

Table 6. Summary of challenges, limitations, and emerging trends in quantum-resistant AI cloud security.

Category	Key Issues/Trends	Description	Implications
Computational Overhead	PQC Key Size and Processing Cost	Post-quantum algorithms like Kyber and Dilithium require larger key sizes and more CPU	May impact cloud latency, throughput, and bandwidth efficiency.

Integration Complexity	AI Model Resource Demand	ML/DL models for threat detection require significant GPU/TPU resources, especially during training and real-time inference.	Increases infrastructure cost and deployment complexity.
	PQC Cloud Compatibility	Legacy cloud systems may not support PQC out-of-the-box. Retrofitting systems involves redesigning encryption libraries and protocols.	Slows down PQC adoption and introduces risk of misconfiguration.
	AI and PQC Co-Deployment	Ensuring seamless integration between AI systems and cryptographic modules is technically demanding.	Requires modular, scalable system design.
AI Concerns	Bias in Models	Training data may be skewed, leading to misclassification or ignoring of novel threats.	Undermines reliability of AI-driven security decisions.
	False Positives/Negatives	AI systems often produce inaccurate alerts, requiring human validation.	Leads to alert fatigue and reduced operational efficiency.
	Explainability Limitations	Many deep learning models operate as "black boxes."	Makes threat decision processes difficult to audit or trust.
Quantum & AI Technology Trends	Advancements in Quantum Hardware	Improvement in qubit stability and gate fidelity suggests possible cryptographic breakthroughs within the next decade.	Urgency in adopting PQC to ensure long-term security.
	AI Evolution (Transformers, Edge AI, Federated Learning)	AI models are becoming more efficient, privacy-aware, and capable of running at the edge.	Enables smarter, more decentralized cloud security systems.
	Lightweight PQC and Hybrid Schemes	Research is needed on cryptographic methods that balance security and performance for cloud and IoT environments.	Essential for scalable adoption across diverse applications.
Future Research Directions	Federated and Explainable AI	Enhancing privacy and interpretability in AI models remains a major research frontier.	Could improve trust and compliance in automated threat detection.

Regulatory Implications	Evolving Compliance Standards (e.g., NIST, GDPR, ISO, ENISA)	Standards for PQC implementation and AI audits are under development.	Organizations must align with these to ensure lawful and secure deployment.
-------------------------	--	---	---

7 CONCLUSION

This paper has looked at how cloud security handles newer threats caused by quantum computing and AI technologies. Using detailed information on how cloud security technology has advanced, the basics of quantum computing on cryptography, and the strong role of artificial intelligence in threat detection and control, we have shown that organizations must integrate both quantum-resistant and AI technologies. The study of post-quantum cryptographic (PQC) techniques, including those standardized by NIST, points out how they can secure cloud systems against upcoming quantum attacks. At the same time, cloud environments are benefiting from machine learning and deep learning, which help with quick detection of anomalies, analysis of user behavior, and automatic handling of security incidents. We created an integrated architectural model combining PQC and AI in cloud computing, discussing its parts, data flows and uses in private and public sectors. We also discussed issues like how PQC can slow platforms down, how integrating PQC can be difficult, the potential for AI bias, and the fact that threat models lack explanation. We also discussed future areas and the importance of obeying upcoming regulations. To make cloud systems resilient and secure, it is essential to start by mixing the benefits of post-quantum cryptography with the flexibility of AI. Because of the growth in quantum computing and AI, only cloud systems with strong, flexible, and simple security features will be able to resist cybersecurity threats in the future.

References

- Adoghe, A. U., Owuama, E. C., Oguntosin, V., & Morawo, B. (2022). Design and Implementation of a Low-Cost Cloud-Powered Home Automation System. *Journal of Engineering Science and Technology Review*, 15(3), 177–192. <https://doi.org/10.25103/jestr.153.20>
- Ahmed, A. A., & Echi, M. (2021). Hawk-Eye: An AI-Powered Threat Detector for Intelligent Surveillance Cameras. *IEEE Access*, 9, 63283–63293. <https://doi.org/10.1109/ACCESS.2021.3074319>
- Apruzzese, G., Laskov, P., Montes De Oca, E., Mallouli, W., Brdalo Rapa, L., Grammatopoulos, A. V., & Di Franco, F. (2023). The Role of Machine Learning in Cybersecurity. *Digital Threats: Research and Practice*, 4(1). <https://doi.org/10.1145/3545574>
- Balaji, A., & Dhurandher, S. K. (2022). Reliable data communication using post-quantum encryption in Internet of Everything. *International Journal of Communication Systems*, 35(13). <https://doi.org/10.1002/dac.5246>
- Balaji, A., Dhurandher, S. K., & Woungang, I. (2022). PINE: Post-Quantum Based Incentive Technique for Non-Cooperating Nodes in Internet of Everything. *Sensors*, 22(18). <https://doi.org/10.3390/s22186928>
- Beyond Firewalls: Navigating the Jungle of Emerging Cybersecurity Trends. (2023). *Journal of Current Trends in Computer Science Research*, 2(2). <https://doi.org/10.33140/jctcsr.02.02.14>
- Bharadiya, J. (2023). Machine Learning in Cybersecurity: Techniques and Challenges. *European Journal of Technology*, 7(2), 1–14. <https://doi.org/10.47672/ejt.1486>
- Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: a comprehensive survey. *Journal of Defense Modeling and Simulation*, 19(1), 57–106. <https://doi.org/10.1177/1548512920951275>
- Dash, B. (2024). Zero-Trust Architecture (ZTA): Designing an AI-Powered Cloud Security Framework for LLMs' Black Box Problems. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4726625>
- Gao, Y., Chen, L., Tu, T., Gao, Y., & Chen, Q. (2022). Post-quantum encryption technology based on BRLWE for internet of things. *Chinese Journal of Network and Information Security*, 8(5), 140–149. <https://doi.org/10.11959/j.issn.2096-109x.2022024>
- Handa, A., Sharma, A., & Shukla, S. K. (2019, July 1). Machine learning in cybersecurity: A review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*. Wiley-Blackwell. <https://doi.org/10.1002/widm.1306>
- Huang, Y., Fan, G., Mai, J., Jiang, W., Hu, J., & Yao, E. (2024). A Post-Quantum Encryption Mechanism Based on Convolutional Neural Network Accelerator. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 71(8), 3945–3949. <https://doi.org/10.1109/TCSII.2024.3377460>
- Hussain, K., Vanathi, D., Jose, B. K., Kavitha, S., Rane, B. Y., Kaur, H., & Sandhya, C. (2022). Internet of Things- Cloud Security Automation Technology Based on Artificial Intelligence. In *Proceedings - International Conference on Applied Artificial Intelligence and Computing, ICAAIC 2022* (pp. 42–47). Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/ICAAIC53929.2022.9792664>
- Knieps, G. (2023). The Governance of Big Data and Artificial Intelligence in Network Industries. *Competition and Regulation in Network Industries*, 24(2–3), 57–71. <https://doi.org/10.1177/17835917231185877>
- Li, S., Chen, Y., Chen, L., Liao, J., Kuang, C., Li, K., ... Xiong, N. (2023, November 1). Post-Quantum Security: Opportunities and Challenges. *Sensors*. Multidisciplinary Digital Publishing Institute (MDPI). <https://doi.org/10.3390/s23218744>
- Mengash, H. A., Alzahrani, J. S., Elthahir, M. M., Al-Wesabi, F. N., Mohamed, A., Hamza, M. A., & Marzouk, R. (2023). Search and Rescue Optimization with Machine Learning Enabled Cybersecurity Model. *Computer Systems Science and Engineering*, 45(2), 1393–1407. <https://doi.org/10.32604/csse.2023.030328>

17. Nalini, M. (2024). Transformative Horizons: Navigating the Evolution of HR through AI and Cloud Technologies. *Shanlax International Journal of Management*, 11(iS1-Jan), 41–47. <https://doi.org/10.34293/management.v11iis1-jan.7138>
18. Pandey, N. K., Kumar, K., Saini, G., & Mishra, A. K. (2023). Security issues and challenges in cloud of things-based applications for industrial automation. *Annals of Operations Research*. <https://doi.org/10.1007/s10479-023-05285-7>
19. Post-quantum secure encryption and cybersecurity education. (2020). *Research Outreach*, (114), 90–93. <https://doi.org/10.32907/ro-114-9093>
20. Reddy, K. (2023). Artificial Intelligence Advantages in Cloud Fintech Application Security. *Central Asian Journal of Mathematical Theory and Computer Sciences*, 4(8), 48–53. Retrieved from <https://cajmtcs.centralasianstudies.org>
21. Ryu, J., Kim, Y., Yoon, S., Kang, J. S., & Yeom, Y. (2024). IPCC7: Post-Quantum Encryption Scheme Based on a Perfect Dominating Set in 3-Regular Graph. *IEEE Access*, 12, 4575–4596. <https://doi.org/10.1109/ACCESS.2024.3349704>
22. Souri, A., Norouzi, M., & Alsenani, Y. (2024). A new cloud-based cyber-attack detection architecture for hyper-automation process in industrial internet of things. *Cluster Computing*, 27(3), 3639–3655. <https://doi.org/10.1007/s10586-023-04163-y>
23. Sumadi, M. I. T. B. N., Putra, R., & Firmansyah, A. (2022). Peran Perkembangan Teknologi Pada Profesi Akuntan Dalam Menghadapi Industri 4.0 Dan Society 5.0. *Journal of Law, Administration, and Social Science*, 2(1), 56–68. <https://doi.org/10.54957/jolas.v2i1.162>
24. Tiwari, P. K., Pandey, S. K., Thamba Meshach, W., Parashar, J., Kumar, A., Altuwairiqi, M., & Krah, D. (2022). Improved Data Security in Cloud Environment for Test Automation Framework and Access Control for Industry 4.0. *Wireless Communications and Mobile Computing*, 2022. <https://doi.org/10.1155/2022/3242092>
25. Tunc, C., Hariri, S., Merzouki, M., Mahmoudi, C., Vaulx, F. J. D., Chbili, J., ... Battou, A. (2017). Cloud Security Automation Framework. In *Proceedings - 2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems, FAS*W 2017* (pp. 307–312). Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/FAS-W.2017.164>
26. Xu, D., Liu, L., Zhang, N., Dong, M., Leung, V. C. M., & Ritcey, J. A. (2023). Nested Hash Access With Post Quantum Encryption for Mission-Critical IoT Communications. *IEEE Internet of Things Journal*, 10(14), 12204–12218. <https://doi.org/10.1109/JIOT.2023.3245360>
27. Yan, F., Wen, S., Nepal, S., Paris, C., & Xiang, Y. (2022). Explainable machine learning in cybersecurity: A survey. *International Journal of Intelligent Systems*, 37(12), 12305–12334. <https://doi.org/10.1002/int.23088>
28. Yungaicela-Naula, N. M., Vargas-Rosales, C., Pérez-Díaz, J. A., & Zareei, M. (2022, February 1). Towards security automation in Software Defined Networks. *Computer Communications*. Elsevier B.V. <https://doi.org/10.1016/j.comcom.2021.11.014>
29. Yungaicela-Naula, N. M., Vargas-Rosales, C., Pérez-Díaz, J. A., & Zareei, M. (2022, February 1). Towards security automation in Software Defined Networks. *Computer Communications*. Elsevier B.V. <https://doi.org/10.1016/j.comcom.2021.11.014>
30. Zalialetdzinau, K. (2022). Automation of organizations using cloud technologies: security issues. *COMPUTER-INTEGRATED TECHNOLOGIES: EDUCATION, SCIENCE, PRODUCTION*, (47), 21–25. <https://doi.org/10.36910/6775-2524-0560-2022-47-04>