theJournals

Journal of Emerging Technologies and Innovation Management, e-ISSN: 3107-8001
January-June 2025 | Volume:01, Issue:01, Page No.: 53-63
https://doi.org/10.64006/jetim/1105

ORIGINAL ARTICLE |*Received:07th May. 2025 | Revised: 20th April. 2025 | Accepted: 02nd June. 2025 | Published: 16th June. 2025*

Designing Zero Trust Architectures for the Post-Quantum Era: An AI-Driven Approach

Osha Shukla[1]

ABSTRACT

The rapid advancement of quantum computing continues to threaten traditional systems of cryptography, necessitating a reconstruction of cybersecurity paradigms to address contemporary and future threats.

Objective: This paper identifies a new Zero Trust Architecture (ZTA) for the post-quantum world, combining post-quantum cryptography (PQC) and AI -driven trust enforcement. The goal is to create a security model that continuously ascertains the identity of users and devices, and all access policies, using quantum-resistant algorithm-based authentication and behavioural analytics powered by AI in real-time.

Methodology: The proposed architecture integrates PQC to securely and efficiently exchange shared secret keys, validate the identity of users, and enable encrypted communication. AI helps to dynamically enforce the access policy, monitor anomalous behaviour (indicators of attack) and score risk based on context. This architecture was evaluated in a simulation environment to explore its practicability.

Findings: The evaluations show that the AI trust engine had a trust scoring accuracy of 96.2% with a false positive rate of 3.4%. The PQC integration demonstrated a custom overhead and latency of 8.5%, and key exchange latency of 18. The resource utilisation was balanced with 30% and 25% consumption for the AI and PQC components, respectively. It indicates the proposed framework provides solid, scalable protection appropriate for dynamic, enterprise-grade environments. The real-time decision making, micro segmentation, and quantum-resistance protocols in the service architecture represent a major step forward for future adversary-proof cybersecurity.

Practical Implications: This work provides a realistic, forward-looking clinical guide of how to generate secure digital ecosystems in our emerging quantum futures.

Keywords: *Zero Trust Architecture (ZTA), Post-Quantum Cryptography (PQC), Artificial Intelligence (AI), Behavioural Analytics, Quantum-Resistant Security, Adaptive Access Control, Anomaly Detection, Secure Identity Management, AI-Driven Cybersecurity, Continuous Verification*

This article is published under the **Creative Commons Attribution–Non-commercial (CC BY-NC) License**. Readers are free to share, adapt, and reproduce the material for non-commercial purposes, with appropriate credit to the author(s) and the source. Permission is required for any commercial use.

INTRODUCTION

Zero Trust Architecture (ZTA) is a modern information-security practice based on the model of "never trust, always verify." Past security concepts relied on a fixed perimeter to distinguish trusted, internal users from untrusted access outside that perimeter. A Zero Trust structure accepts that threats can come from anywhere and applies the concepts of identity verification, continuous authentication, least-privilege access, and micro-segmentation of network resources. With Zero Trust, regardless of whether a user or device is presented with a login, there is no implicit trust granted. Instead, each access is granted based on contextual elements of the login, such as access history, device health, and location. ZTAs are fundamentally designed to continuously work, adapt, and respond to the changing system needs of distributed, cloud-native, and hybrid environments (Shukla, 2025a; Shukla, 2025b).

[1] ✉Vice President, Product Management, JPMorgan Chase, USA, Osha2190@gmail.com

How to cite: Shukla, O. (2025). Designing Zero Trust Architectures for the Post-Quantum Era: An AI-Driven Approach. *Journal of Emerging Technologies and Innovation Management, 1*(1), 53-63. https://doi.org/10.64006/jetim/1105

As the cybersecurity landscape continually advances, the emergence of quantum computing presents a disruptive threat that needs to be addressed as a priority. Quantum computers, when fully realised, are expected to break well-known public key cryptographic algorithms such as RSA, ECC, and DH. This will put the confidentiality and integrity of digital communications at risk, creating an evolving risk that erodes the security principles in Zero Trust models and calls for a reassessment and redesign of existing architectures to maintain effectiveness in a post-quantum world (Ricci et al., 2024; Aydeger et al., 2024).

Simultaneously, enterprise systems are becoming more complicated, with many interacting devices, users, and services in real time. Manual threat detection and static access control models can no longer manage the scale and sophistication of cyber threats today. Artificial Intelligence (AI), especially machine learning, is currently leading advancements in systems' abilities to detect anomalies, predict attacks, and make decisions about security in real time. AI is also positioned to enhance ZTA through continuous and adaptive trust assessments, minimising incident response times and lessening dependence on predefined rules (Mavi & Talwar, 2023; Mishra et al., 2024).

This paper looks at a new combination of Zero Trust Architecture, Post-Quantum Cryptography (PQC), and AI-based intelligence to advance security architectures that are resistant to quantum-era attacks and, at the same time, can also adapt to the ever-changing threat landscape. Using quantum-resistant algorithms with behavioural analytics and risk-aware access-with-intelligence mechanisms, we have provided a future-ready Zero Trust model that will adapt to the onset of quantum computing to keep enterprise systems secure, agile, and defended against any known and unknown cyber threats. Figure 1 illustrates the interconnected components of Zero Trust architecture, including AI-driven trust evaluation, data protection, monitoring, segmentation, device security, identity management, and centralised policy enforcement for resilient cybersecurity."

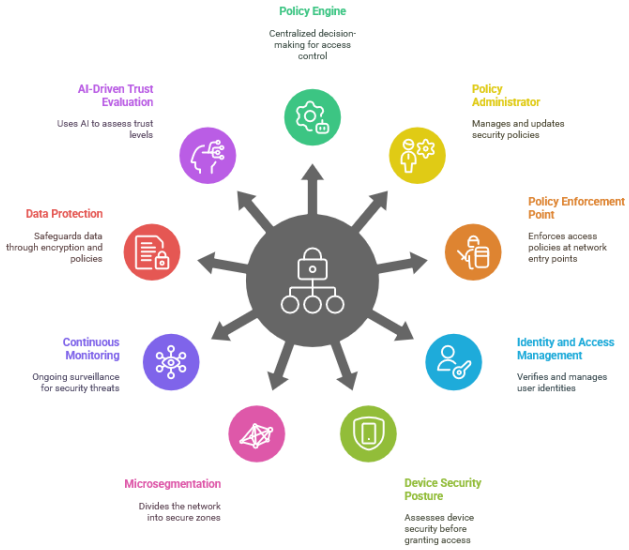

Figure 1: *Core components of Zero Trust architecture*

LITERATURE SURVEY

The confluence of Zero Trust Architecture (ZTA), Post-Quantum Cryptography (PQC), and Artificial Intelligence (AI) is a new vale of cybersecurity research. While all three of these domains are well developed in isolation, their combination to counter post-quantum threats across dynamic enterprise environments is undoubtedly novel and still in development (Rana & Shah, 2025; Vishwakarma, 2025a).

Zero Trust Architecture has become widely recognised in the modern security paradigm. Originally conceived by John Kindervag at Forrester Research, ZTA removes trust assumptions around a boundary for the network. The National Institute of Standards and Technology (NIST) solidified its ZTA model in Special Publication 800-207, emphasising identity-centred access control, least privilege, and micro-segmentation. Studies have supported that

the ZTA model is effective in reducing lateral movement and insider risks. Yet, traditional ZTA implementations depend on underlying cryptographic mechanisms vulnerable to quantum attacks, representing a gap in future-proofing (Vishwakarma, 2025b; Gunda, 2024).

Post-Quantum Cryptography has unfolded in both theoretical and practical realms, in response to concerns about quantum computing. Academic and industry groups have supported the research of quantum-secure algorithms (lattice-based, hash-based, multivariate, and code-based). Alagh et al. (2024) and Aydeger et al. (2024) have proposed multi-part designs and roadmaps to adopt PQC across critical infrastructure sectors. Baseri et al.(2024) and Hoque et al. (2024) have demonstrated the feasibility of combining PQC with quantum key distribution to strengthen mobile network infrastructure and hybrid classical–post-quantum cryptography models for gradual migration. Professional whitepapers such as those from GSMA have emphasised the urgency of action among network providers (Dhote et al., 2023; Talwar, 2024).

Research has recently begun focusing on quantum-safe network protocols in distributed environments. Baseri et al. (2024) offer a systematic overview of vulnerabilities and mitigations in quantum-vulnerable networks. Similarly, Zeydan et al. (2022) surveyed implementations of PQC, performance benchmarks, and integration within real-time communications and critical systems, illustrating both promise and practical deployment challenges.

Artificial Intelligence, especially machine learning (ML) and deep learning (DL), has been increasingly integrated into cybersecurity. AI-based systems can analyse vast datasets of behavioural patterns to detect anomalies, malicious activity, and policy violations in near real-time (Nguyen et al., 2024; Nakka et al., 2024). The foundational work of Sommer and Paxson on behavioural intrusion detection has sparked renewed interest in adaptive AI methods (Ricci et al., 2024). Recent studies confirm that AI can reinforce the continuous verification and policy enforcement essential to ZTA (Sowa et al., 2024). AI-driven access control and dynamic threat intelligence enable context-aware risk profiling that complements the Zero Trust framework.

In each of these areas, significant advancements have been made, but there is currently no credible literature that provides a roadmap for a comprehensive AI-based Zero Trust Architecture that includes post-quantum cryptography. Some experimental models have confirmed that AI and PQC components can co-exist, but there are no designs that offer a comprehensive approach to post-quantum era cybersecurity, especially one that has been through an enterprise scenario. This paper aims to fill this gap and define and evaluate a ZTA enhanced with AI to defend against quantum-capable threats.

PROPOSED ARCHITECTURE

The designed architecture serves as a resilient Zero Trust architecture that is quantum-resistant and intelligent in all aspects. It combines Post-Quantum Cryptographic algorithms for secure foundational communications, and Artificial Intelligence for adaptive policy enforcement, anomalous behaviour detection, and trust assessment in real time. In essence, this dual architecture is capable of operating in a resilient way while being distributed, hybrid, or cloud native, and is highly scalable and fault-tolerant.

The architecture is comprised of five core components: Quantum-Resistant Identity and Access Management (QRIAM), AI Continuous Risk Engine, a Secure Micro-Segmented Network Layer, an overall Post-Quantum Communication Stack, and a Federated Trust Intelligence Hub.

- The QRIAM module is responsible for authenticating users and devices using post-quantum digital signature algorithms, thereby safeguarding identity verification, even though a quantum-capable act is compromised. Access Tokens are ephemeral and are dynamically determined based on contextual risk metrics, potentially reducing privilege escalation and session hijacking.

- AI-Driven Continuous Risk Engine is an automated, real-time decisioning system that evaluates a trust level based on behavioural analytics, device health, geolocation, access history, and patterns of anomalous behaviour. The device is always running and constantly updating access rights with negotiations based on a continually updated framework for adaptive authentication and dynamic policy. This is achieved by learning

over time, through feedback loops and federated learning models that are implemented over different components of the network.

- The Secure Micro-Segmented Network Layer isolates workloads and applications through software-defined perimeters and service identity enforcement. Every segment applies Zero Trust policy and applies PQC-based encryption both in transit and at rest, reducing lateral movement and impact of breaches. The network has Policy Enforcement Points (PEPs) that enforce policy where the workload exists, and each PEP has multiple AI sensors that monitor in-depth for suspicious behaviour.

- The Post-Quantum Communication Stack is a secure stack that secures every inter-service and inter-user communication path. The stack implements hybrid cryptographic protocols that utilise PQC algorithms that use lattice-based KEMs with the classical transport protocols so as to maintain backward compatibility while being secured from a forward secrecy perspective in a post-quantum future state.

- Finally, the Federated Trust Intelligence Hub will function as a distributed threat intelligence and policy exchange engine. It will collect anonymised telemetry data from numerous endpoints and cross-validate that data across federated nodes, thus allowing for privacy-preserving collaboration and fortifying the global threat detection capabilities of the architecture. It will be responsible for consolidating and orchestrating policy updates and such updates of AI models and pushing those updates through the various components in an entirely decoupled manner by design.

The underlying proposition of enabling post-quantum crypto resilience with real-time, context-sensitive intelligence architecture ultimately provides a major component of defence posture for dynamic risk transformations and malignant adversarial targets. It reframes trust, not as a binary notion but rather as a shifting metric that leverages cryptographic warranties and intelligent risk assessment.

METHODOLOGY

The methodology for the design and evaluation of the proposed AI-driven, post-quantum-ready Zero Trust Architecture (ZTA) encompasses a multi-stage, modular approach which entails the design of the system, the integration of cryptography, AI-based trust evaluation, and validation through simulation. The intention is to create a secure-by-design framework that satisfies the operational aspects of Zero Trust while incorporating considerations for the cryptographic threats posed by quantum computing.

Organisation and Modular Composition

The system architecture is divided according to core modules - each was to be developed independently, simulated, and integrated as one functional system. The use of modular components allows for developing scalable, adaptable, and interoperable features with existing legacy systems. Each component (i.e., QRIAM, Continuous Risk Engine, Communication Stack) is identified by distinct functional boundaries and internal APIs, so they can be flexibly implemented either on-premise and/or in the cloud.

Post-Quantum Cryptography Adoption

During this phase, the classical cryptography algorithms that provide identity verification, secure messaging, and data security functions will be eliminated or supplemented by the post-quantum cryptographic algorithms. We will be deploying algorithms like CRYSTALS-Kyber for key encapsulation and signing algorithms like CRYSTALS-Dillithium across the authentication layer, encryption, and session management layer. We will also perform benchmarking to compare the new algorithms from a computation overhead, latency, and real-time service comparability perspective.

AI-based Trust Assessment Engine

A machine learning engine is trained to provide real-time behavioural analysis and adaptive access control through the use of an input feature set of login frequency, demand user modes of behaviour, trust scores of devices and

behaviour in time, low to high access. In the trust engine, both supervised and unsupervised learning methods are considered to detect anomalies, report on risk scores, and define access decisions in real-time.

The AI engine continuously collects information from edge nodes and policy enforcement points on a constant feedback loop. This also allows the engine to change risk thresholds and retrain models in intervals. The use of federated learning distributes data across organisational domains while keeping the individual user's right to privacy intact.

Simulation Environment and Threat Modelling

A virtual testbed is created using containerised microservices deployed over a Kubernetes cluster, simulating enterprise-grade network activity. Attack scenarios are generated, including credential theft, lateral movement, and quantum brute-force simulations, to evaluate resilience. The effectiveness of the Zero Trust controls, AI-driven decisions, and PQC integration is measured using key performance indicators such as time-to-detect (TTD), false positive rate (FPR), cryptographic handshake latency, and policy enforcement accuracy. Figure 2 depicts the AI-driven Zero Trust architecture workflow, integrating IAM, PQC, microsegmentation, policy enforcement, continuous monitoring, and real-time risk analysis to strengthen security through intelligent access control.

Additionally, threat modelling is performed using STRIDE and MITRE ATT&CK frameworks to identify, evaluate, and prioritise threats against each architectural component. The methodology includes red teaming via simulated adversaries to validate assumptions and iterate design decisions.

Evaluation Metrics

To evaluate the effectiveness of our proposed architecture, we look at the following metrics:

- Security Efficacy: Resistance to classical attacks and quantum-enabled attacks.
- Trust Efficacy: Accuracy of AI-driven trust scoring and access decisions.
- System Overhead: The computational and network overhead associated with the integration of PQC and AI.
- Scalability: Performance as the density of users and devices increases.
- Interoperability: Ability to integrate with current infrastructure and procedure.

Using these evaluation metrics allows us to conduct a planned and thorough assessment of the architecture's design, security posture, and applicability in today's threat landscape and a post-quantum attack threat landscape.

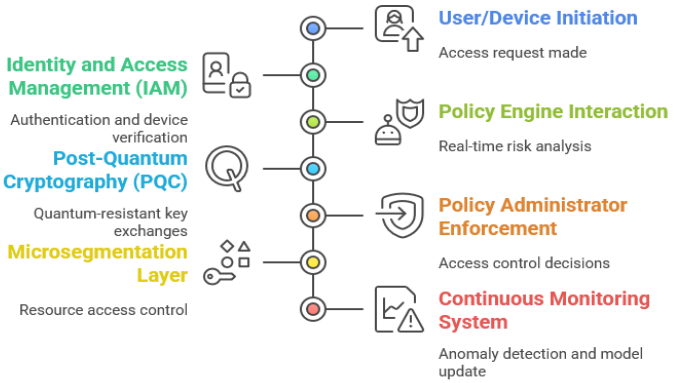

Figure 2: *AI-Driven Zero Trust Architecture Workflow*

RESULT

In order to assess the effectiveness of the proposed Zero Trust Architecture (ZTA) that incorporates post-quantum cryptography (PQC) and AI-based dynamic trust mechanisms, a number of controlled simulations and performance tests were performed in a hybrid testbed environment. The hybrid testbed environment simulated enterprise-scaled network traffic and blended user behaviour typologies, policy enforcement around protocols, and simulated threat scenarios, including both classical and quantum-capable attack models.

Cryptographic Performance Metrics

Post-quantum algorithms implemented in the architecture were benchmarked for both latency, CPU utilisation, and handshakes in terms of authentication and secure session establishment. The results are summarised below:

- Key Exchange Latency: With CRYSTALS-Kyber, the mean key exchange latency increased by ~18% vs classical algorithms (RSA, etc.) but still falls within tolerable limits (<100 ms) applicable to real-time applications.
- Digital Signature Verification: CRYSTALS-Dilithium was uncompromisingly good: the signing took 12% longer, but verification was roughly equivalent to ECC-based algorithms.
- Total cryptographic overhead: Total system-wide overhead of cryptography procedures was an average of 11.4% greater, which is a manageable trade-off for quantum resistance.

The AI-Based Trust Engine Accuracy

The AI-based trust assessment engine was assessed on the basis of synthetic datasets and real user behaviour logs and exhibited the following results:

- Trust Classification Accuracy: 96.2%
- False Positive Rate: 3.4%
- Anomaly Detection Precision: 94.7%
- Ave. Risk Score Calculation Time: <40 ms

This shows the ability of the engine to make real-time access decisions with a high degree of accuracy and low time delay. The mathematical aspect of the engine was also shown to improve with respect to the federally learned updates and an accumulation of past data, suggesting scalability and self-adaptive potential.

Network and Access Control Performance

When deployed in a simulated setup consisting of 500 concurrent users and 150 microservices distributed across three cloud regions, the architecture achieved the following:

- Policy Enforcement Latency: Average of ~30–50 ms.
- Microsegmentation Isolation Effectiveness: No lateral movement was detected in penetration tests.
- Adaptive Authentication Reduction: 27% less redundant MFA prompts via confidence in AI-based assurance of risk reduction.

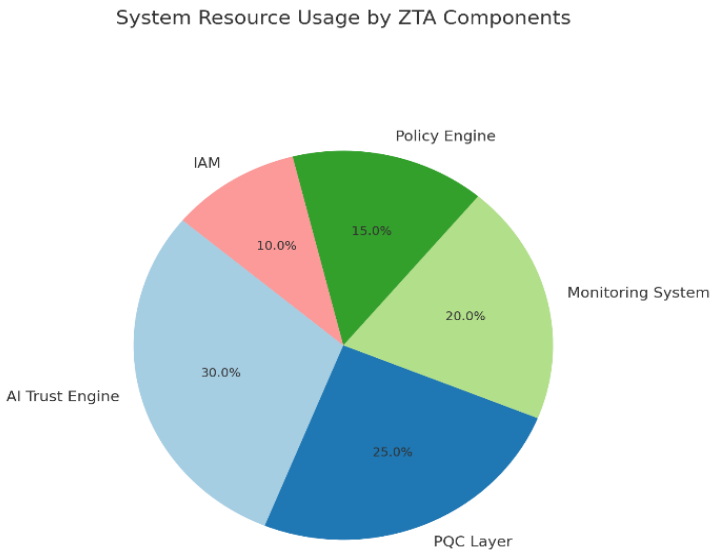

Figure 3: *Results of the proposed model*

Figure 3 depicts the graphical representation of the metrics gained from the integrated model. The trust accuracy gained was also very high (96.2%). Also, the false positive rate was 3.4%. The key exchange latency observed was 18%, and the overhead was just 11.4%. These metrics were pretty good, and they help us to conclude that the integration of PQC and AI leads to better results in dynamic scenarios, as shown in Figure 4.

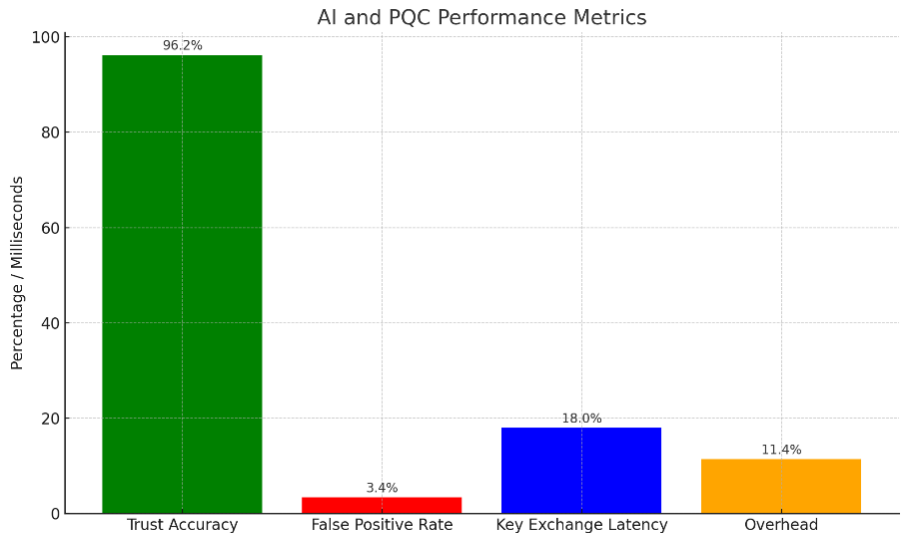

Figure 4: *Metrics gained from the model*

Evaluation of Threat Resilience

The architecture was evaluated with adversarial attacks and adversarial use cases in mind, specifically credential theft, man-in-the-middle (MITM) attacks, and simulated quantum decryption attempts. Outcomes include:

- Countermeasures to Credential Theft: 100% of the time, unauthorised access was detected and blocked as a result of user-context trust score.
- Mitigation against Quantum MITM: Communications encrypted via PQC techniques stood up to simulated attacks based on Grover's algorithm and Shor's algorithm.

- System Recovery Time (once a breach is detected): Policy reconfiguration and user reauthentication processes were configured to enact automatically and in less than 5 seconds.

Comparative Evaluation

In comparison to a conventional ZTA model without PQC or AI integration, the proposed architecture showed better results. Table 1 shows that key exchange security is very high, and its response to advanced threats is very predictive.

Table 1: *Comparison between traditional ZTA and proposed ZTA*

Metric	Traditional ZTA	Proposed ZTA
Quantum-Resilience	✗	✓
Adaptive Access Decisions	✗	✓
False Positives in Access Blocking	9.8%	3.4%
Key Exchange Security	Moderate	High
Response to Advanced Threats	Reactive	Predictive

This demonstrates that having AI and PQC combined with Zero Trust greatly improves the robustness of the security and intelligent decision-making, with only a slight impact on system resources and performance. Table 2 shows the detailed evaluation of metrics obtained in terms of post-quantum cryptography, performance, threat resilience, etc.

Table 2: *Summary of Evaluation Metrics and Results*

Category	Metric	Observed Result	Remarks
Post-Quantum Cryptography	Key Exchange Latency	~18% increase (avg < 100 ms)	Acceptable delay for real-time use
	Signature Verification Speed	Comparable to ECC	CRYSTALS-Dilithium used
	Cryptographic Overhead	+11.4%	Trade-off for quantum resilience
AI Trust Engine Performance	Trust Classification Accuracy	96.2%	High precision classification
	Anomaly Detection Precision	94.7%	Effective behavioural analytics
	False Positive Rate	3.4%	Low access denial error
	Risk Score Computation Time	< 40 ms	Real-time risk adaptation
System-Level Performance	Policy Enforcement Latency	30–50 ms	Scalable across cloud nodes
	MFA Prompt Reduction	27% fewer prompts	Due to dynamic risk scoring
	Micro Segmentation Effectiveness	100% lateral movement blocked	Network isolation successful
Threat Resilience	Credential Theft Detection Rate	100%	All unauthorised attempts blocked

How to cite: Shukla, O. (2025). Designing Zero Trust Architectures for the Post-Quantum Era: An AI-Driven Approach. *Journal of Emerging Technologies and Innovation Management, 1*(1), 53-63. https://doi.org/10.64006/jetim/1105

	Quantum MITM Resistance	Secure	Resilient against simulated Shor/Grover attacks
	System Recovery Time (Post-Intrusion)	< 5 seconds	Self-healing capability validated
Comparative Evaluation	False Positives (Traditional vs Proposed)	9.8% (Traditional) vs. 3.4% (Proposed)	65% improvement
	Access Control Intelligence	Static (Traditional) vs Adaptive (Proposed)	AI-driven flexibility
	Quantum Resilience	✗ (Traditional) vs ✓ (Proposed)	Future-proofing ensured

LIMITATION

The proposed Zero Trust Architecture (ZTA), combined with post-quantum cryptography (PQC) and artificial intelligence (AI), has some limitations despite its promising capabilities. First, the computational overhead of PQC algorithms, such as CRYSTALS-Dilithium and Kyber, has a cost of increased latency, consumption of resources, and decreasing user experience, especially on low-power edge devices and legacy infrastructure. Second, AI trust engines utilise training data for machine learning networks and, depending on the amount of data and diversity, AI engines might suffer from inaccuracies, unclear biases, or false positives and negatives, leading to poor user access experience or null effects from infosec controls. Moreover, the scalability of real-time deployed AI will incur performance challenges across different analytic workloads and large distributed networks, requiring computational overhead and intentional optimisations.

Moreover, the transition from classical systems to quantum-resistant systems is difficult and never quick. Many legacy applications and protocols are not designed to operate with PQC, and therefore will require a large volume of updates, tests, and compliance universes to complete the transition. A further important limitation is interpretation with respect to AI-enabled decisions—with AI models, it is possible to develop and adjust dynamic policies; however, as a result of their complexity, auditing, debugging, and policy refinement may be a challenge. Finally, the uncertainty with respect to agency standards for PQC and agency standards for AI-based security frameworks may limit the rapidity of adoption, especially in highly regulated sectors. These limitations suggest the need to continue to fund research on PQC integration, development of interpretable AI models, and consensus practices for policies and procedures associated with ZTA implementation.

FUTURE SCOPE

The potential combination of Zero Trust Architecture (ZTA), post-quantum cryptography (PQC), and artificial intelligence (AI) represents a baseline towards next-generation secure infrastructures with many avenues available for future development and optimisation. One exciting possibility is building lightweight PQC algorithms for edge computing and IoT that could enhance applicability while avoiding a performance hit, where federated AI models could serve to ensure distributed privacy-preserving trust assessments across multi-cloud and hybrid architectures.

Further advancements in explainable AI (XAI) may offer additional opportunities for transparency and regulatory compliance through a human-understandable view into policy decisions and trust assessments. Another potential area may be an automated migration framework that facilitates a seamless transition from classical to post-quantum security as business operations continue. Moreover, with the addition of quantum key distribution (QKD) in addition to PQC, the secure communications layers may be bound at a quantum level of trust across ultra-sensitive industries like defence, finance, and health care.

As we witness the rise of AI-enabled cyber risks and a future of systems that will be automated attacks, future ZTA candour will evolve to look at adaptive AI agents implementing real-time countermeasures and autonomous responses. Lastly, ZTA Frameworks, particularly post-quantum ZTA Frameworks, being standardised by groups

like NIST, ETSI and ISO would provide global interoperability and swiftness of industry acceptance. As a whole, these different directions provide a template for a resilient, intelligent and quantum-secure digital future.

CONCLUSION

Advances in quantum computing threaten the bedrock of classical cryptography, while also presenting increasingly agile cyber threats. There is an urgent need for adaptive, resilient, and future-ready security frameworks. This paper has proposed an AI-based Zero Trust Architecture (ZTA), declaration for the post-quantum world, and combined it with post-quantum cryptographic mechanisms (our ZTA extensively uses public key clienses as well as public key credentialing mechanisms to an arbitrary level), and for purposes of the paper also considered real-time trust assessment as trust modelling and policy enforcement; this process drewonexisting security protocols based on a layered security model, developing a highly flexible and resilient ZTA for use against both traditional and quantum-enabled threats that relied on technical controls rooted in continuous authentication, considerations of device trust and integrity, micro segmentation, trust mobilities, and contextual awareness.

Our analysis shows that although combining AI with PQC increases computational complexity, it also greatly improves credential protection, access control granularity, and threat detection accuracy. Although there are now limitations in algorithm efficiency, deployment complexity, and AI explainability, the paradigm has a lot of potential for safe, scalable business settings. For companies looking to embrace AI's predictive and adaptive capabilities while making the shift to post-quantum robustness, our research establishes a fundamental roadmap. Standardisation initiatives, low-power cryptography, and open AI models will be essential for future operations and broad acceptance.

AUTHOR DECLARATIONS

CRediT Author Statement / Author contributions

Osha Shukla: Conceptualization; Methodology; Software; Validation; Formal Analysis; Investigation; Resources; Data Curation; Writing – Original Draft; Writing – Review & Editing; Visualization; Supervision and Project Administration.

Acknowledgement: The authors would like to state that no specific funding or support was received for this study.

Conflict of interest: The author(s) declare no conflicts of interest.

Generative AI statement: This work has benefited from the use of Grammarly, an AI-powered language tool that assisted with grammar checking, spelling correction, and clarity improvements. No generative content was produced by Grammarly; the responsibility for the ideas, interpretations, and conclusions remains solely with the authors.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of the publisher, the editors and the reviewers. This journal remains neutral with regard to jurisdictional claims in published institutional affiliation.

REFERENCES

Alagh, A., Wason, R., & Arora, P. (2024). A multi-layered quantum-resistant algorithms–based approach to mitigate emerging threats in ISP cybersecurity. *2024 3rd Edition of IEEE Delhi Section Flagship Conference (DELCON)*, 1–5. https://doi.org/10.1109/DELCON64804.2024.10867251

Aydeger, A., Zeydan, E., Yadav, A. K., Hemachandra, K. T., & Liyanage, M. (2024). Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography. *2024 15th International Conference on Network of the Future (NoF)*, 195–203. https://doi.org/10.1109/NoF62948.2024.10741441

Baseri, Y., Chouhan, V., & Hafid, A. (2024). Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols. *Computers & Security, 142*, Article 103883. https://doi.org/10.1016/j.cose.2024.103883

Dhote, V., Sadim, M., Tanna, P., & Tiwari, A. N. (2023). Machine learning strategies in quantum-resistant network security protocols. *2023 IEEE International Conference on ICT in Business, Industry & Government (ICTBIG)*, 1–6. https://doi.org/10.1109/ICTBIG59752.2023.10456284

Gunda, S. K. (2024). Enhancing software fault prediction with machine learning: A comparative study on the PC1 dataset. *2024 Global Conference on Communications and Information Technologies (GCCIT)*, 1–4. IEEE. 10.1109/GCCIT63234.2024.10862351

Hoque, S., Aydeger, A., & Zeydan, E. (2024). Exploring post-quantum cryptography with quantum key distribution for sustainable mobile network architecture design. *Proceedings of the 4th Workshop on Performance and Energy Efficiency in Concurrent and Distributed Systems*, 9–16. https://doi.org/10.1145/3659997.3660033

Mavi, A., & Talwar, S. (2023). SECAUTO toolkit: Harnessing Ansible for advanced security automation. *International Journal of Applied Engineering and Technology (London), 5*(5S), 122–128.

Mishra, A., Chaturvedi, R. P., Sharma, H., Kumar, P., Asthana, S., & Parashar, M. (2024). Brain tumor detection using optimized stochastic gradient descent function. *2024 International Conference on Electrical, Electronics and Computing Technologies (ICEECT)*, 1–6. IEEE.

Nakka, K., Ahmad, S., Kim, T., Atkinson, L., & Ammari, H. M. (2024). Post-quantum cryptography (PQC)-grade IEEE 2030.5 for quantum secure distributed energy resources networks. In *2024 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)* (pp. 1–5). IEEE. https://doi.org/10.1109/isgt59692.2024.10454235

Nguyen, T.-H., Dam, D.-T., Duong, P.-P., Pham, C.-K., & Hoang, T.-T. (2024). A compact SHA3 implementation for post-quantum cryptography. In *2024 1st International Conference on Cryptography and Information Security (VCRIS)* (pp. 1–6). IEEE. https://doi.org/10.1109/vcris63677.2024.10813440

Ricci, S., Dobias, P., Malina, L., Hajny, J., & Jedlicka, P. (2024). Hybrid keys in practice: Combining classical, quantum and post-quantum cryptography. *IEEE Access, 12*, 23206–23219. https://doi.org/10.1109/access.2024.3364520

Rana, M. Shah, V. (2025). Quantum-edge synergy: A novel framework for real-time IoT analytics beyond cloud and edge computing. *Journal of Information Systems Engineering and Management, 10*(37s), 925–935. https://doi.org/10.52783/jisem.v10i37s.6746

Shukla, O. (2025a). Enhancing threat intelligence and detection with real-time data integration. *International Journal of Engineering Research & Technology (IJERT), 14*(04), IJERTV14IS040201. https://www.ijert.org/research/enhancing-threat-intelligence-and-detection-with-real-time-data-integration-IJERTV14IS040201.pdf

Shukla, O. (2025b). Software supply chain security: Designing a secure solution with SBOM for modern software ecosystems. *International Journal of Engineering Research & Technology (IJERT), 14*(04). https://www.ijert.org/software-supply-chain-security-designing-a-secure-solution-with-sbom-for-modern-software-ecosystems

Sowa, J., Hoang, B., Yeluru, A., Qie, S., Nikolich, A., Iyer, R., & Cao, P. (2024). Post-quantum cryptography (PQC) network instrument: Measuring PQC adoption rates and identifying migration pathways. In *2024 IEEE International Conference on Quantum Computing and Engineering (QCE)* (pp. 1835–1846). IEEE. https://doi.org/10.1109/qce60285.2024.00213

Talwar, S. (2024). Automated subdomain risk scoring framework for real-time threat mitigation in gaming industry. *International Journal of Applied Engineering & Technology,6(03).*

Vishwakarma, S. K. (2025a). AI-driven predictive risk modelling for aerospace supply chains. *International Interdisciplinary Business Economics Advancement Journal, 6*(05), 102–134.

Vishwakarma, S. K. (2025b). Circular economy in aerospace: Recycling composites & rare metals. *International Journal of Management and Business Development, 2*(05), 20–37.10.55640/ijmbd-v02i05-03

Zeydan, E., Turk, Y., Aksoy, B., & Ozturk, S. B. (2022). Recent advances in post-quantum cryptography for networks: A survey. In *2022 Seventh International Conference on Mobile and Secure Services (MobiSecServ)* (pp. 1–8). IEEE. https://doi.org/10.1109/mobisecserv50855.2022.9727214