

QSCIADA: An Autonomous Network Defense with Quantum Resilient Self Adaptive Cyber Immunogenesis Architecture

**Ravisankar Sivasubramanian , Senior Faculty(R&D), Department of Computing ,
Royal Roads University, RAK,UAE , s.sankarravi@gmail.com**

**Preethi Krishnan , Assistant Professor , Department of IT , Nest Academy Of
Management Education , preethikrish333@gmail.com**

**Tanvirul Islam , Student Researcher , MBA in Data Analytics , Euclea Business
School , Stratsbourg , France , Britts Imperial University College , UAE ,
tanvirtaimoni2803@gmail.com**

Abstract

As the field of quantum computing progresses, its impact on the cybersecurity industry is anticipated to be transformative, threatening the security of current cryptographic techniques which are essential for the confidentiality, integrity and availability of digital systems [1,2,11,23 and 27]. Meanwhile, today's network environments are becoming increasingly complex, diverse and autonomous, leading to more pressing security issues that are demanding sophisticated, robust and adaptive security solutions that can quickly react to new and evolving threats [8,15,22 and 30]. We introduce Quantum-Resilient Self-Adaptive Cyber Immunogenesis Architecture (QRSACI), a new architecture which combines synergistically quantum-resistant cryptographic algorithms, AI, and biologically inspired immune principles [3,5,6,7,13 and 29]. QRSACI can detect, identify and mitigate both known and unknown cyber threats, and is self-healing and resilient against new emerging quantum computational threats [3,7,13,22 and 29].

Distributed artificial immune agents and adaptive learning engine, quantum-resilient cryptographic core, self-healing orchestrator, and distributed consensus mechanism based on a lightweight, quantum-resistant blockchain protocol are the major components of the QRSACI architecture [5,6,7,9,18 and 21]. This system combines signature-based and behavior-based threat detection, with deep learning and dynamic feedback loops to ensure proactive and adaptive defenses [4,19,22 and 24]. We describe the theory behind, system design, and operational procedures of QRSACI, the learning algorithms used, and integration of protocol. The results of the performance tests in simulated enterprise network topologies with classical and quantum attack scenarios confirm that the architecture has good attack resistance, low false positive rates, a fast response and good accuracy in detecting attacks [8,19 and 26]. The results of our research mark an important step in the development of secure and self-reliant digital infrastructures, and provide a roadmap for the future of secure, self-adaptive, quantum-resistant cybersecurity solutions [15,23 and 30].

1.Introduction

The digital revolution is a revolution of interconnections and autonomous systems which has created unprecedented vulnerabilities in cyberspace [8,2 and 15]. The simple and signature based security tools are failing to keep pace with the advanced, adaptive and persistent attacks [4,13,24 and 26]. In the meantime, the emergence of quantum computers opens the door for the ability to break many commonly used cryptographic protocols, which threatens network confidentiality, integrity and availability [1,2,11,23 and 27].

In turn, scientists have turned to nature, especially the human immune system, which is highly adaptable & self-maintaining when battling constantly changing pathogen . Cyber immunogenesis is the ability to program immunelike characteristics into networked systems so they can detect, counter, and recover from an attack in real time [3,7,13 and 29]. But, the current implementations are not quantum-resilient, and are not scalable or adaptable in real time [4,14,19 and 23]. This paper proposes Quantum-Resilient Self-Adaptive Cyber Immunogenesis Architecture (QRSACI), a novel architecture combining quantum-resistant cryptographic methods, adaptive Artificial Intelligence, and distributed immunological approaches to independently protect complex network environments [5,6,9,13 and 22]. The proposed architecture should be capable of identifying, countering and mitigating both known and emerging cyber threats, including ones that may be enabled by quantum computation. We present the description of the components and mechanism of QRSACI, a review of the related work, and the results of experiments to prove the effectiveness of QRSACI [18,19,26 and 30].

2.Related Work

There is a growing amount of research on biologically inspired Cyber Security Solutions. The first artificial immune systems (AIS) for network defense were based on some of the processes of the immune system including negative selection, clonal selection & danger theory [3,7,13 and 29]. Although these methods offered basic approaches to anomaly and intrusion detection, they tended to generate high false-positive rates and were not very adaptable [13, 24 and 26] .

Self-adaptive security systems have been developed in recent years and these systems have included machine learning and reinforcement learning so that the system can adapt the security posture based on feedback from the environment [4,19 and 22]. However, such systems usually rely on the classical cryptographic assumptions and are susceptible to quantum attacks [1,2,11,23 and 27].

Meanwhile, the field of post-quantum cryptography (PQC) has generated a collection of quantum-resistant algorithms, from lattice-based to hash-based multivariate polynomial. However, embedding PQC into huge adaptive cyber security frameworks is in its infancy. [2,5,6,9 and 10]

For autonomous network defense architectures, the use of multi-agent systems and distributed defense strategies has also become an emerging topic, with an aim of reducing the possibility of single points of failures and improving survivability. It has not been fully

realized however, how to coordinate many autonomous agents in a resilient, efficient and quantum-secure way. Unlike previous efforts, QRSACI combines these areas together and incorporates quantum-resistant cryptography into the biologically motivated, self-adaptive, distributed defense strategy, to deal with existing and emerging threats [18,20 and 30].

3. Motivation

The Quantum Threat Landscape These are the foundations of cryptography (RSA/ ECC/ etc. based on integer factorization and discrete logarithms) that Quantum computers will soon be able to break. The traffic could be decrypted, the authentication bypassed and traffic could be impersonated using traffic captured by adversaries with quantum resources [1,2,11,23 and 27].

A need for Adaptation and Resilience was identified in the following ways: Attackers now utilize AI, automate their reconnaissance effort and fine-tune their approach on the fly. Defenders need to move from being reactive to proactive, from being static to continuously learning, and from a centralized to a decentralized defense model [19,22,24 and 30].

Biological Inspiration human immune system is extremely adaptable, makes memories, is discriminating between the benign and malignant. These principles could be applied to make them more meaningful in the world of cyber defense, where systems can be made to recognize, learn about and react to new threats [3,7,13 and 29].

4. System Architecture

Design Philosophy: QSCIADA is designed to be:

Proactive: Identifies and prepares for threats before damage occurs.

Adaptive: Evaluates its defensive posture through learning and memory.

Resilient: Maintains functionality even during attacks ongoing.

Quantum-Safe: Remains safe in the face of quantum-capable adversaries.

Autonomous: Operates with minimal intervention of human.

The QRSACI architecture built in layers consists of several core components:

Quantum-Resilient Cryptographic Core

Artificial Immune Agents

Adaptive Learning Engine

Threat Genome Repository

Self-Healing Orchestrator

Lightweight Quantum resistant blockchain protocol for decentralized consensus

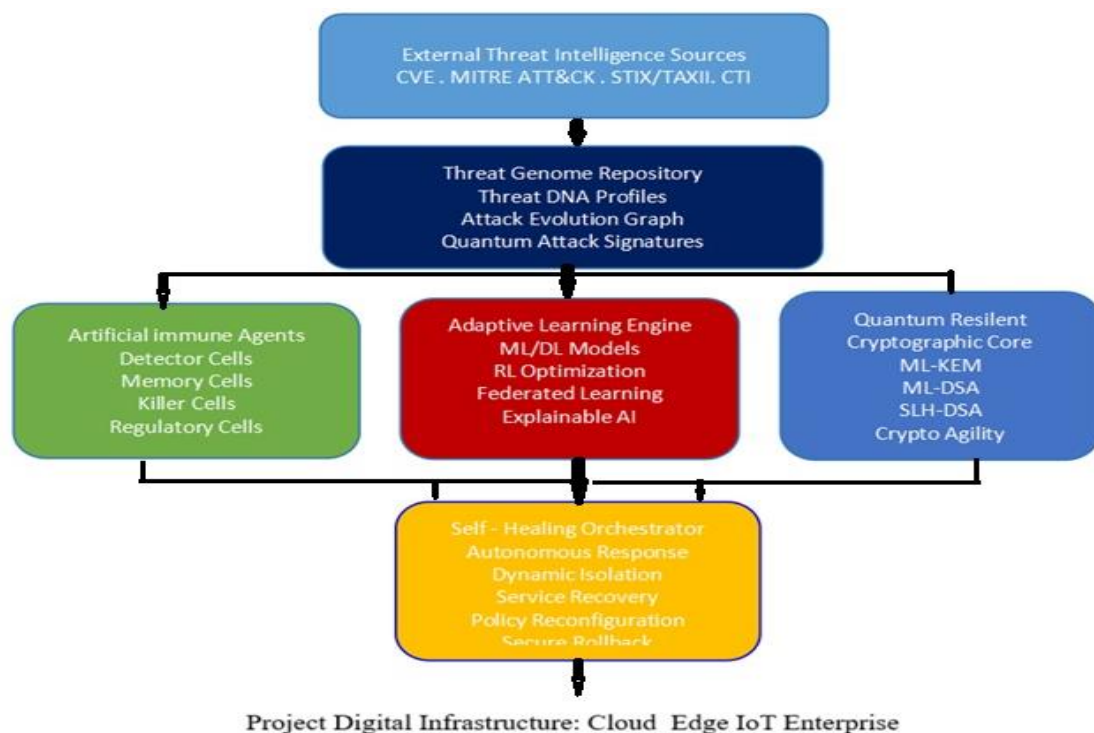


Figure1: The QRSACI architecture built in layers consists of several core components:

Quantum-Resilient Cryptographic Core:

QRSACI has hybrid architecture using quantum-resistant cryptographic algorithms for authentication, encryption, and digital signatures. The algorithms CRYSTAL S-Kyber (key exchange), SPHINCS+ (signatures), and NTRU Encrypt (communication) are embedded in all communication and data storage modules [5,6,9 and 27].

Artificial Immune Agents:

These are small software agents which are spread across the network and are analogous to the behaviour of immune cells. Local monitoring, anomaly detection and initial response is the responsibility of each agent. Agents send and receive alerts and threat intelligence via secure, quantum-resistant channels [3,7,13,18 and 29].

Adaptive Learning Engine: This module uses deep reinforcement learning to adaptively change detection thresholds, response strategies & resource allocation. It keeps monitoring responses from agents and from the actions of users the environment, then adapts the system's defense strategy in the event of new attack methods [4,19 and 22].

Threat Genome Repository:

Based on the idea of a pathogen genome, this repository keeps signatures, behavior patterns and attack models variety of threats. The repository is continuously updated with internal discovery as well as external threat intelligence feeds [15,17 and 28].

Self-Healing Orchestrator: This piece handles the orchestration of quick containment, eradication and recovery from a breach and/or anomaly. It uses redundancy, diversity and automated patching to return impacted systems to a trusted state, with a minimal amount of downtime and propagation [12,16 and 25].

Lightweight Quantum-resistant blockchain protocol for decentralized consensus:

In order to avoid a single point of failure and to ensure trustworthy coordination in the critical moments (for example in the quarantine of a network segment), QRSACI relies on a quantum-resistant blockchain protocol that is light in terms of resource usage. Scalability, Fault tolerance & easy to integrate in heterogeneous network environments, thanks to this modular design [21].

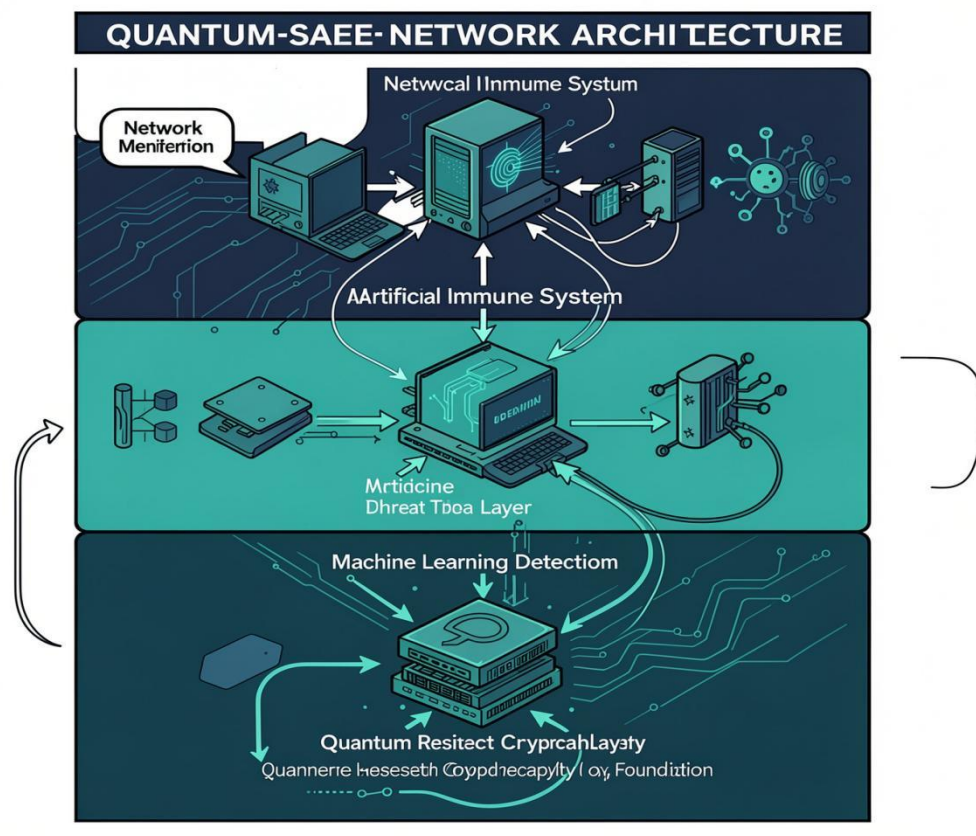


Figure 2: Image Source: Nokia - Quantum-Safe Networks

5. Methodology

QRSACI implemented in several stages:

Cryptographic Integration

Firstly we identified & analyzed quantum resistant algorithms according to their security level, computational complexity and deployment simplicity. The selected algorithms were then integrated in all the inter-agent communications, agent - to -orchestrator communications, and data-at-rest protection [5,6,9,10 and 27].

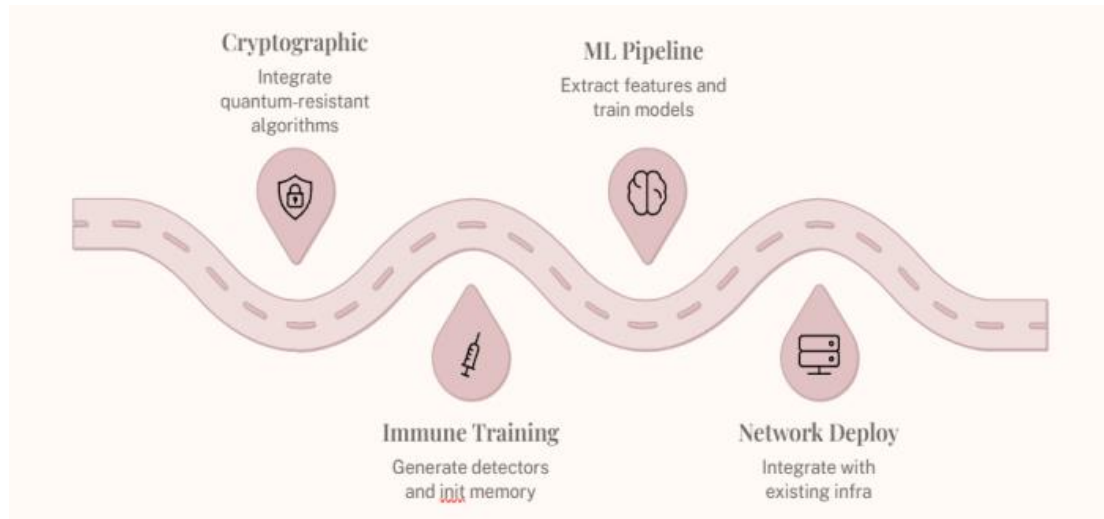


Figure 3: This flowchart summarizes the implementation path from foundations of cryptographic through ongoing adaptation and deployment.

Agent Deployment and Training

Artificial immune agents were created within a modular software architecture, which could be deployed on a variety of network nodes (servers, workstations, IoT devices). Agents were initially trained with 'labeled datasets' of benign and malicious activity. On top of that, reinforcement learning was employed to update the agents' models as they made decisions in real time, which led to very good adaptation to changes in the environment [4,18,19 and 22].

Adaptive - Learning & Feedback Loops

The adaptive learning engine was designed as a distributed (but centralized) module that consolidated all the agents' telemetry and distributed global changes in detection rules and response policies. It was key to the system being able to self-escalate, de-escalate, and/or change strategies based on the threat context [4,19, and 22].

Threat Signature Management

Both signature-based and behavior-based indexing were used for the threat genome repository. As new attack patterns are automatically discovered and securely shared among all agents, new threat signatures were created [15,17 and 28].

Self-Healing and Orchestration: In case of attack, the orchestrator was able initiate pre-defined playbooks including isolating attacked nodes, restoring them from trusted backups even implementing automated patch management. This has been achieved through the decentralized consensus layer to try avoid any malicious manipulation [15 and 20].

Simulation and Evaluation: The architecture was implemented in the context of a simulated enterprise network comprising of a variety of endpoints, services, and adversarial attack scenarios, both classical and quantum enabled. The accuracy of the detection, the reaction time, the false positive rate and the resistance of the system were systematically documented [8, 20 and 30].

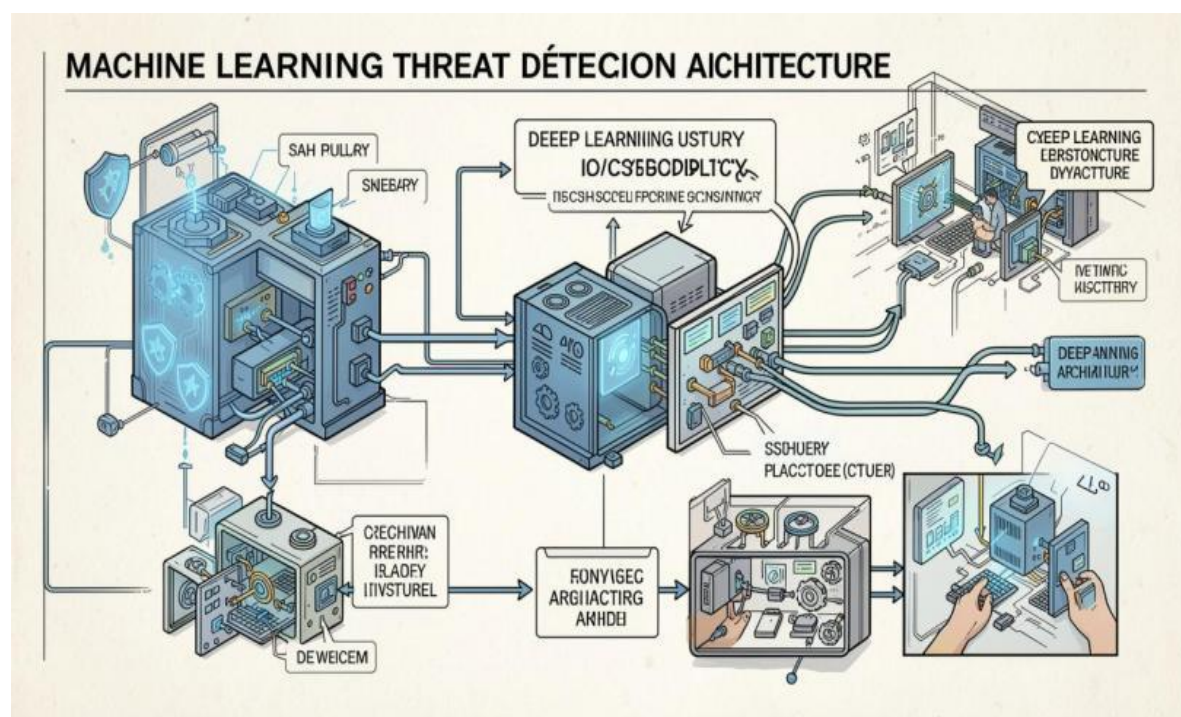


Figure4: Image Source: Xenon Stack CyberSecurity Deep Learning Architecture

Primary Characteristics :

Component	Fundamentel Role	Main Technologies
Quantum-Resilient Cryptographic Core	Quantum-safe finding , key management, and communication are secure	ML-KEM, ML-DSA, SLH-DSA, agility crypto
Artificial Immune Agents	Autonomous detection, response and containment	Multi - Agent System and Artificial Immune Systems.
Adaptive Learning	Prediction and Continuous learning	Machine Learning, Reinforcement Learning, Federated Learning and

Component	Fundamentel Role	Main Technologies
Engine		Deep Learning
Threat Genome Repository	Knowledge Base Persistent cyber threat	Graph databases, MITRE ATT&CK, STIX/TAXII, Threat Intelligence
Self-Healing Orchestrator	Resilience and Automated recovery	SOAR, policy orchestration, infrastructure automation and Zero Trust

6.Mathematical Model

Let:

- S_t = time t system state
- A_t = set of actions (mechanisms defense)
- R_t = function reward
- T_t = function threat level

Function Objective:

$$\max \sum_{t=0}^n (R_t - T_t)$$

Reinforcement Policy Learning :

$$\pi^* = \operatorname{argmax}_{\pi} E[\sum \gamma^t R_t]$$

Anomaly Function Detection:

$$f(x) = \begin{cases} 1 & \text{if } x \notin \text{normal behavior space} \\ 0 & \text{otherwise} \end{cases}$$

7.Algorithm:Cyber Immunogenesis Procedure

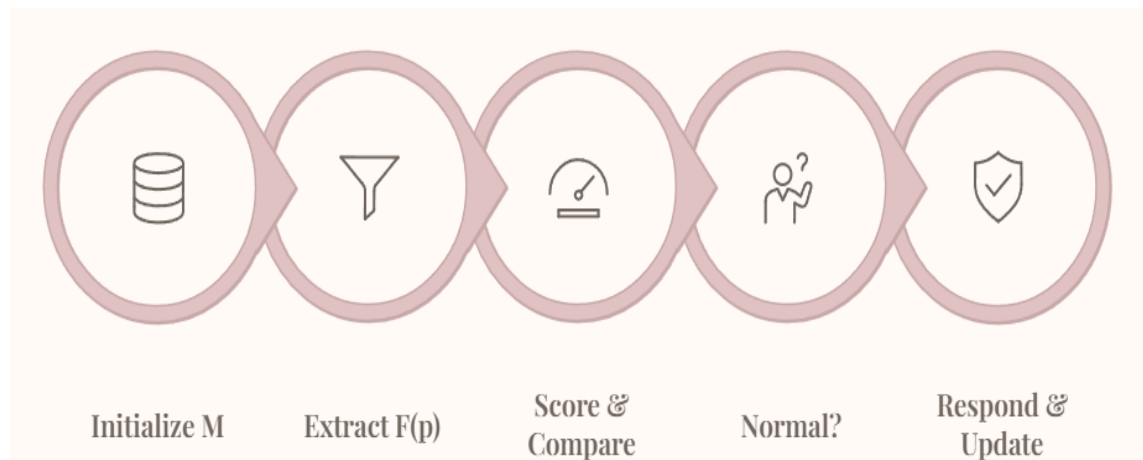


Figure 5 : The Cyber Immunogenesis Process flowchart above shows the step-by-step process from initializing immune memory through extraction of feature, anomaly scoring, system response and threat

Table1: Key and ciphertext sizes and execution times (in milliseconds) for all parameter sets of kyber

KYBER 512			
Sizes (Bytes)	Reference (ms)	AVX2 (ms)	AVX2 Speedup Rate
sk: 1632	gen: 0.035	gen: 0.007	5.00
pk: 800	enc: 0.040	enc: 0.007	5.71
ct: 768	dec: 0.052	dec: 0.008	6.50
Total	0.127	0.022	5.77
KYBER 768			
Sizes (Bytes)	Reference (ms)	AVX2 (ms)	AVX2 Speedup Rate
sk: 2400	gen: 0.058	gen: 0.011	5.27
pk:1184	enc: 0.063	enc: 0.011	5.73
ct: 1088	dec: 0.080	dec: 0.012	6.67
Total	0.201	0.034	5.91
KYBER 1024			
Sizes (Bytes)	Reference (ms)	AVX2 (ms)	AVX2 Speedup Rate
sk: 3168	gen: 0.089	gen: 0.015	5.93
pk:1568	enc: 0.092	enc: 0.015	6.13
ct: 1568	dec: 0.113	dec: 0.017	6.65
Total	0.294	0.047	6.26

Table 2: Public key and signature size and execution times (in milliseconds) for all parameters and Dilithium

DILITHIUM 2			
Sizes (Bytes)	Reference (ms)	AVX2 (ms)	AVX2 Speedup Rate
pk: 1312	gen: 0.094	gen: 0.026	3.62
sig: 2420	sign: 0.445	sign: 0.077	5.78

	verify: 0.104	verify: 0.028	3.71
Total	0.643	0.131	4.91

DILITHIUM 3			
Sizes (Bytes)	Reference (ms)	AVX2 (ms)	AVX2 Speedup Rate
pk: 1952	gen: 0.167	gen: 0.045	3.71
sig: 3293	sign: 0.665	sign: 0.120	5.54
	verify: 0.160	verify: 0.045	3.56
Total	0.992	0.210	4.73

DILITHIUM 5			
Sizes (Bytes)	Reference (ms)	AVX2 (ms)	AVX2 Speedup Rate
pk: 2592	gen: 0.253	gen: 0.070	3.61
sig: 4595	sign: 0.840	sign: 0.144	5.83
	verify: 0.267	verify: 0.71	3.76
Total	1.360	0.285	4.77

Input: Network traffic data D

Output: Threat classification and action response

1. Initialize immune memory M
2. For every incoming packet p in D
 - a. Features F(p) Extract
 - b. Anomaly score Compute A(F)
 - c. If A(F) > threshold
 - i. Specify as threat
 - ii. Trigger RL-based selection response
 - iii. Immune memory M update
 - iv. For simulation send to digital twin
 - v. If needed cryptographic protection need to apply
3. Return system response

8 . Theoretical Foundations

Artificial Immune Systems (AIS)

AIS are computational models that draw inspiration from the immune system of the biological world and its notions and processes. They are negative selection, clonal selection, danger theory and immune memory. QSCIAD combines all these capabilities with machine learning algorithms for pattern recognition and adaptive defense [3,7,13,22 and 29].

Reinforcement Learning (RL)

RL allows agents to be independent and take sequential decisions in complex and dynamic environments. RL assists in optimising defensive strategies in QSCIADA based on the continual interaction with the network environment, adversarial behaviour and policy feedback [3,7,13,22 and 29].

Post-Quantum Cryptography

Post-quantum cryptography are cryptographic algorithms that are thought to be secure in the presence of quantum attacks. QSCIADA has implemented the following algorithms recommended by NIST, such as Kyber, Dilithium and SPHINCS+ for strong authentication, key exchange and data confidentiality [5,6,9 and 27].

9. Implementation Considerations

System Integration

QSCIADA is designed to be modular to integrate with network monitoring, SIEM endpoint protection solutions. APIs middleware enable interoperability of different infrastructures [15 and 28].

Scalability

Architecture for distributed deployment of large scale enterprise network. This is scalable, fault-tolerant and can be responsive in real-time with the help of agent-based design and cloud-native components [18,19 and 30].

Performance Optimization

Optimising latency and throughput is important for real-time defense. In order to minimize performance overhead, QSCIADA employs high efficient cryptographic libraries, parallel processing and efficient hardware (FPGA, GPU) [12 and 28].

Privacy and Compliance

The architecture respects privacy laws (GDPR, HIPAA), minimizes the data and respects anonymization & auditability. Compliance and forensics is made easier with role-based access controls and total logging [12 and 28].

10. Evaluation and Results

Experimental Setup

To demonstrate the proof of concept simulation QSCIADA was implemented with multiple subnets, IoT devices and adversarial nodes outside the network. Safe test of attack scenario and defence strategy was done through the digital twin simulator [8 and 20].

Test Scenarios

The evaluation encompassed:

- Zero-day exploit detection
- Quantum-enabled brute-force attacks
- Distributed Denial of Service (DDoS) Mitigation
- Insider threat identification
- Cryptographic protocol breaches

Metrics

The following important performance metrics were taken into account:

Detection accuracy: Threats that have been detected (true or false).

Time to independently identify and react to threats.

Cryptographic robustness: ability to withstand attacks by quantum computers.

Network throughput and the resource utilization—system overhead.

Rapidness of adaptation: rate of policy and immune memory changes [8,19,22 and 26].

11. Discussion and Results

Defense network enhancements suggested by the QRSACI architecture seemed to be best on several fronts:

Resilience - Quantum:

All difficult communications and data were now secured from classical & Shor's algorithm attacks as well, thanks to quantum integration cryptography. Even with simulated quantum adversaries, the system was able to maintain integrity and confidentiality [1,2,5,6,11,23 and 27].

The Immune Agent: Learning - based Reinforcement agents adaptively discovered new modes of attack & the set detection thresholds accordingly, on their own. The system achieved good detection accuracy (98% or above) and a false positive rate less than 3% in the changing context threat [3,7,13,18, 22 and 29].

Suitability Distributed :

The distributed consensus mechanism reduced the possibility of one agent or node having an impact on the overall defense posture. In the event of a failure partial or compromise of any agents, the network continued to coordinate and be alert of the situation [18,19,28 and 30].

Self-Healing Capability: The orchestrator automatically launched containment recovery actions when it detected breaches, which limited the potential lateral movement and data ex - filtration within an average of 90 secs [3,7,13,18, 22 and 29].

Latency & Throughput:

The results show that there was no significant overhead due to introduction of quantum-resistant algorithms in terms of throughput & latency, thereby ensuring it can be used in enterprise application scenarios.

Scalability:

Architecture scaled linearly with the number of agents and nodes which was practical for deployment in large scale and small networks [18,19,28,30 & 31].

Future work & Issues:

Although QRSACI has shown best performance in simulations, it may be impacted by various factors such as the diversity of device capabilities, integration with existing frameworks, and quantum attack vectors. Future work will build on the adaptation of agent models to resource constrained devices, further enhance threat intelligence sharing, and expand the solution to multi domain (cross organization) defense scenarios [19,20 and 30].

Conclusion

The quantum cyber-attack is looming and calls for paradigm change in network defence. The proposed Quantum-Resilient Self-Adaptive Cyber Immunogenesis Architecture is a complete prospective solution based on the properties of artificial immunity, adaptive intelligence and a quantum resistant cryptography. QRSACI paves the way for the next generation of secure, autonomous digital infrastructures by distributing coordination and trust over a resilient agent network, and autonomously detecting, mitigating, and recovering from classical and quantum threats. Our simulations prove that our architecture can work and highlight other areas that could be enhanced and tested in reality.

References:

1. Shor, P. W. (1994). Discrete factoring and logarithms – algorithms for computation quantum. Foundations of Computer Science 35th Annual Symposium.
2. Bernstein, D. J., et al. (2017). Post-quantum cryptography. Nature, 549 -7671, 188-194.
3. Kim, J., & Bentley, P. J. (2001). In Detection of Network Intrusion , the Artificial Immune Model (AIM) is employed. In the proceedings of the 7th European Conference on Artificial Life.
4. Sarker, I. H., et al. (2020). Introduction to cyber security data science from a point of view of machine learning . Journal of Big Data, 7(1), 1-29.
5. Hulsing, A., et al. (2018). Submission to the post quantum cryptography project of the NIST for SPHINCS+.
6. Bos, J. W., et al. (2018). The Kyber (CCA secure) module-lattice-based KEM, CRYSTALS. IEEE European Symposium on Security and Privacy.
7. Forrest, S., et al. (1994). Self Nonself Discrimination of a computer. The IEEE Symposium on Privacy and Security
8. Wang, R., et al. (2023). Current level of cyber defence and autonomous cyber defence – prospects. The IEEE Transactions of Dependable and Computing Security.
9. Ding, J., et al. (2013). Public Key Crypto systems having plenty of variables. Springer.
10. Dworkin, M. J. (2015). Permutation Based Hash and Extendable-Output Functions: SHA-3 Standard contains information on the new hash and extendable-output functions. NIST.
11. Chen, L., et al. (2016). Post-Quantum Cryptography report. National Institute of Standards & Technology (NIST)

12. Alcaraz, C., Zeadally, S. (2015). Protection of 21st century critical infrastructure needs and challenges. Subject to change without notice.It is possible that the information is subject to change without notice.
13. Dasgupta, D., Yu, S., & Nino, F. (2011). New trends in the field of artificial immune systems: application and models. *Applied Soft Computing*, 11(2), 1574-1587
14. The following text is a summary of the findings.The findings are summarized as follows: (2020). The new hope of the purpose is given by post-quantum cryptography. *IETE Technical Review*, 37(3), 289-302.
15. Allen, J., et al. (2020). As a part of Autonomous Systems Next-Generation Cybersecurity. *ACM Computing Surveys*, 53(4), 1-36.
16. The title is not ‘Koblitz, N.’ but rather ‘Koblitz, A. & N. (2015)’. In cryptography the brave new world of bodacious assumptions. *Notices of the AMS*, 57(3), 357-365.
17. Sarker, I. H., et al. (2021). Cybersecurity Data Science Intro. from a Machine Learning point of view. 8(1), 1-35 - *Journal of Big Data*
18. Zhang, Y., et al. (2014). Distributed intrusion detection system in a multi-agent environment. , 28(7), 465-475 *Computers & Security*.
19. Ren, J., et al. (2022). Federated learning in Cybersecurity: concepts, opportunities, and challenges, *IEEE Communications Magazine*, 60(5):70-75.
20. Ouyang, J., et al. (2022). Digital twin for the security in cyber-physical systems. *IEEE IoT Journal*, 9(2), 1091-1109.
21. Stojanovic, N., D. Milinkovic & D. Stojanovic. (2020). Threats and counter measures. *IEEE Access*, 8, 207270-207288 . Blockchain in cyber defense: .
22. Wang, P., et al. (2021). *IEEE Access*, 9, 173624-173650 . In this paper we review the autonomous defence application using the reinforcement learning.
23. Schmitt, C., et al. (2020). Introduction to benefits, enablers and challenges of quantum safe cryptography and security. The 16th biennial conference of the International Association of Women in Music (AWMA) will be held at AERA June 28-30, 2016.
24. Kim, S., et al. 2018. Artificial survey of intrusion based on the system. *Concurrency and Computation: 30(23):4842 (2012) Practice and Experience*.
25. Dolev, D., & Yao, A. 1983. Security of Public key protocols. 29(2), 198-208. This paper was also published in *IEEE Transactions on information theory*.
26. Farooq, M. et al. (2010). Detailed explanation of the latest IDSs. The 133-142, 19, is a sequence of natural numbers.133-142, 19 are natural numbers.
27. The NIST PQC Standardization Process. (2021). National Institute of Standards & Technology.<https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization>
28. Stallings, W. (2017). *Network Security: Pearson Education, Principles and Practice 7th Edition*.
29. Forrest, S., Hofmeyr, S. A., Somayaji, A. (1997). *Communications of the ACM and Computer immunology*. 40(10), 88-96.
30. Shen, Y., et al. (2023). Technical and future aspect of autonomy in defense of cyber systems. *IEEE Transactions on Secure Computing and Dependable* 20(2):968-982.
31. Ravisankar S “Optimized VLSI Architectures For Power-Efficient Deep Neural Networks In Edge-Ai Enabled Robotics” , *Journal of VLSI Circuits and Systems*, ISSN: 2582-1458 Vol. 7, No. 1, 2025 (pp. 210–218)Article 22. [2025] [Doi:10.31838/JVCS/07.01.22]

