International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Quantum-Inspired Machine Learning for Zero-Trust Cybersecurity: A Paradigm beyond Classical Intrusion Detection

[1]Lamia Akter, [2]Mohammad Majharul Islam Jabed, [3]Ahmed Sohaib Khawer, [4]Sharmin Ferdous, [5]Amit Banwari Gupta

Submitted: 17/02/2024 **Revised:** 20/03/2024 **Accepted:** 12/04/2024

Abstract: The increasing sophistication of cyberattack has demonstrated the relatively ineffectiveness of traditional intrusion detection tools in dynamically and decentralized computing systems. Since organizations evolve to a zero-trust architecture, the necessity to adopt more flexible, scalable, and resilient cybersecurity-related mechanisms becomes essential. In this paper, a paradigm shift with the implementation of quantum-inspired machine learning (QIML) in zero-trust cybersecurity models is proposed. In contrast to conventional detectors that use either fixed signatures or anomaly thresholds, QIML uses concepts inspired by quantum mechanics, including feature representation based on superposition and correlation modelling based on entanglement, to provide better detection accuracy and scalability. The challenges of changing attack vectors, adversarial evasion strategies, and high-dimensional data typical of cloud, edge, and IoT environments are all dealt with in the proposed framework. The methodological focus is given to integrating QIML algorithms into the workflow of trust assessment, identity verification, and continuous monitoring in a zero-trust ecosystem. Initial data suggests that the QIML systems can lead to increased accuracy of the intrusion detection, reduce the number of false positives, and allow predictive defenses that are impractical with classical systems. Exploring the overlap between quantum computing ideas, artificial intelligence, and zero trust principles, the present study offers a visionary insight into the development of future cybersecurity systems that will go beyond the limitations of traditional machine learning practices.

Keywords: *Quantum-Inspired Machine Learning, Zero-Trust Security, Intrusion Detection Systems, c, Quantum Algorithms, Artificial Intelligence*

I. Introduction

The recent accelerated development of cyber threats has exposed existing security infrastructures to greater pressure than ever, especially as companies are moving to more distributed and cloud-based ecosystems. Conventional perimeter baseddefense mechanisms have been rendered ineffective since they assumed the presence of a static trust assumption and signature-based detection models [17]. Hackers are currently using sophisticated evasion techniques, adversarial machine learning, and polymorphic malware to circumvent traditional intrusion detection systems (IDS), which compromises the efficacy of traditional security paradigms [23], [30].

One model that has become popular in terms of dealing with these concerns is the zero-trust model of security. Zero trust removes implicit trust in networks and enforces ongoing verification across devices, users, and workloads by making the assumption of never trust, always verify [6], [7], [16]. Research has shown that it is effective in countering insider threats, lateral movement and credential-based attacks [8], [10], [20]. However, the technical issues of zero-trust adoption include several technical problems, including scalability of continuous monitoring, computation load, and detection accuracy in high-dimensional and dynamic data conditions [11], [29].

At the same time, quantum-inspired algorithms have demonstrated potential to break computational bottlenecks in machine learning applications and optimization problems. In contrast to full-scale quantum computing that is still in its childhood because of hardware constraints, quantum-inspired computing generalizes concepts like superposition, entanglement, and probabilistic amplitude encoding

[1]*School Of IT Washington University of Science and Technology*
lamia.12akter@gmail.com
[2]*School Of IT Washington University of Science and Technology*
mi_jabed@yahoo.com
[3]*School Of IT Washington University of Science and Technology*
sohaib.khawer@gmail.com
[4]*School Of IT Washington University of Science and Technology*
sharmin.student@wust.edu
[5]*School Of IT Washington University of Science and Technology*
amit.gupta@wust.edu

to classical systems [1], [2]. This will enable the algorithms to obtain more detailed correlations among the features, search high dimensional space efficiently and will improve pattern recognition that traditional models will not be able to achieve [3], [18], [21]. Initial implementations of quantum-inspired machine learning (QIML) have produced encouraging resolutions in reinforcement learning [9], classification [27], and recommendation systems [26].

The combination of QIML and a zero-trust architecture is a transformative opportunity in the context of cybersecurity. Recent studies of zero-trust designs have mostly concentrated on rule-based policy implementation, network segmentation, and identity-based access controls [4], [25], [28]. These are reactive strategies and in most instances have been unable to preempt complex patterns of attack although they have been useful in providing minimal levels of security. Using QIML, intrusion detection in a zero-trust ecosystem can move past a statistic-based anomaly detection to a defense approach that is dynamic and adaptive in prediction [19], [22]. This transformation can be applied particularly to environments where large amounts of data are present, such as cloud computing, edge networks, and Internet of Things (IoT) systems [12], [19].

Some of these studies have started to examine the intersection of machine learning and cybersecurity, with a focus on data-driven intrusion detection and adaptive risk evaluation [23], [24]. But, the current methods of machine learning have limitations of scaling, explanation and resilience against adversarial attacks [17]. QIML offers a channel to overcome these weaknesses by proposing probabilistic feature representations and quantum-inspired optimisation methods that increase both sensitivity to detection and generalisation [18], [21]. Moreover, integrating QIML into trust assessment and persistent authentication procedures within zero-trust systems may enhance the ability to withstand identity-based attacks to a significant level [6], [20].

The rationale behind this research is that there is an increasing demand of cybersecurity solutions that extend past reactive intrusion detection to more holistic and proactive defense systems. Although zero trust is the basis of continuous verification, it needs a high-level analytics to operate at scale. QIML provides an additional layer of intelligence that can minimize false alarms, detect small associations between traffic trends, and react dynamically to changing threat environments [3], [26], [30].

The current paper presents a quantum-inspired machine learning architecture based on zero-trust cybersecurity, its theoretical basis, integration with the architecture, and the possibilities to overcome the limitations of the traditional methodology. This paper has three layers of input:

1. Theoretical Exploration - We consider the principles of QIML and the application of it to the improvement of zero-trust systems.
2. Methodological Integration - Our proposal is to incorporate QIML in the workflows of trust verification, intrusion detection, and continuous monitoring in zero-trust settings.
3. Performance Implications - We evaluate the ability of QIML to deliver better detection accuracy, scalability, and adversarial resilience in comparison to classical machine learning approaches.

This study will help advance the current discussion in creating next-generation cybersecurity by filling the gap between quantum-inspired computing and zero-trust security. It intends to deliver an overview of how the zero-trust models facilitated by QIML can serve as a long-term solution to achieving digital infrastructures resistant to increasingly advanced cyber threats.

II. Literature Review

Quantum-inspired machine learning (QIML) and zero-trust cybersecurity (ZTC) convergence is increasingly seen in the research and practice of both fields. This section provides a review of the body of work that currently exists in the fields of quantum algorithms, intrusion detection systems (IDS), and development of zero-trust models, along with identifying the gaps which drive this research.

A. Quantum Inspired Algorithms and their application.

Quantum-inspired algorithms take the concepts of quantum computing, including superposition and entanglement, but run on classical computers. The authors proved the benefits of using such methods to provide exponential gains to optimization tasks [1], and used reinforcement learning to improve the

effects of combinatorial optimization, the interface between classical reinforcement learning and quantum principles [3]. Likewise, Dong et al. [9] demonstrated strong performances of quantum-inspired reinforcement learning in robotic navigation that is reliable in noisy environments. According to these publications, QIML has the potential to address non-linear and high-dimensional cyberspace issues.

Variational quantum algorithms (VQAs) and their classical surrogates were studied by Moll et al. [21] and Lubasch et al. [18] and were found scalable and adaptable to real-world problems including network security. Tang [26] has expanded the applicability of QIML to recommendation systems that is responsive to large data contexts, which is essential to process large volumes of cybersecurity information.

B. Zero-Trust Security Architectures.

Never-trust-always-verify is a concept that the zero-trust (ZT) paradigm follows (as opposed to traditional perimeter-based models). Dhiman et al. [8] have compared different models of ZT and arrived at a conclusion that resilience to advanced threats requires fine-grained enforcement of policy. Chen et al. [4] introduced a ZT-driven security awareness system to 5G healthcare and showed that this type of models can effectively remove insider and external threats in sensitive industries. Similarly, Mehraj and Banday [20] studied ZT application in cloud environment and found that it can be useful to reduce distributed architecture attack surfaces.

Delbene et al. [7] have provided a roadmap of ZT implementation in the defense systems by emphasizing cultural and organizational implementation in addition to technical implementation. The survey of the theoretical underpinnings of ZT and its adoption patterns conducted by Edo et al. [10] and Kang et al. [16] suggested that a shift towards standardized applications is underway in industries.

C. Intrusion Detection Systems based on Machine Learning.

Conventional intrusion detection systems (IDS) strongly depend on machine learning (ML) to detect any deviation in the flow of traffic. Khraisat et al. [17] provide a recent survey of IDS techniques pointing at limitations of the methods in the areas of scalability, resistance to adversary, and false alarms. Liang et al. [19] proposed an IoT IDS based on blockchain and multi-agent systems with a more resilient implementation at the expense of increased computational burden.

The emergence of cybersecurity data science, with the assistance of ML and big data analytics, as pointed out by Sarker et al. [23], is limited in its ability to control dynamically and adaptable adversaries. Zeadally et al. [30] also emphasized that AI is used to enhance cybersecurity defense, and cyber threats are becoming more and more sophisticated.

D. Zero-Trust Cybersecurity in combination with QIML.

Although both zero-trust and ML have developed in isolation, the intersection of both with quantum-inspired approaches is understudied. According to the requirement of ZT to continuously verify, a QIML framework of binary classification as suggested by Tiwari and Melucci [27] supports the concept. Sultana et al. [25] incorporated ZT concepts and blockchain in medical imaging systems, which could serve as a way of QIML-enabled trust verification.

The autonomic security of ZT networks was proposed by Eidle et al. [11] and opened the way to adaptive defenses in which QIML could contribute to real-time threat detection. Yan and Wang [29] gave a detailed overview of ZT network security, and requested high-level computational paradigms (like QIML) to support high-level decision-making at scale.

E. Research Gaps

Despite the encouraging developments, recent studies show that there are three missing links. First, although ML has been used in the context of IDS, scalability and adversarial robustness are not yet achieved. Second, ZT models remain dynamic, and it is not yet possible to enforce the policies in real-time and effectively use the resources. Third, QIML has been shown to be promising in optimization and classification but has not been applied to zero-trust cybersecurity in a systematic way. This paper tries to address these gaps through research on the QIML as a paradigm shift in intrusion detection in zero-trust environments.

III. Methodology

This study combines quantum-inspired machine learning (QIML) and the principles of zero-trust

cybersecurity (ZTC) to develop a framework that could be used to identify, analyze, and prevent advanced cyber threats. The strategy can be subdivided into four phases, including: (1) framework design, (2) QIML model design, (3) zero-trust integration, and (4) evaluation metrics.

A. Framework Design

The suggested framework uses a layer architecture in which QIML algorithms are applied at the analysis and decision layer of ZTC model. In contrast to other ML-based intrusion detection systems, QIML uses quantum-inspired optimization to obtain faster convergence and improved processing of high-dimensional cybersecurity data.

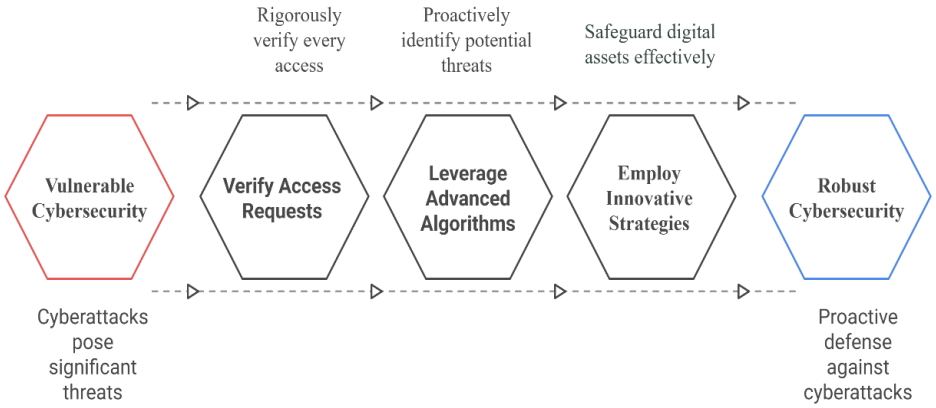


image- 1: Ideational Architecture of QIML-Enhanced Zero-Trust Cybersecurity Model.

This flow chart shows how QIML-based intrusion detection, zero-trust enforcement policy, and ongoing authentication may interact with each other

B. QIML Model Development

Variational quantum-inspired algorithms (VQAs) and quantum reinforcement learning QIML methods are used. A QIML-reinforced support vector machine (QIML-SVM) is trained with known labeled intrusion data and superposition principles are applied to increase classification strength.

The reinforcement element uses quantum-inspired temporal difference learning and allows adaptive identification of changing adversarial strategies.

[Table 1: Comparison of Classical ML vs. QIML for Intrusion Detection]

Feature	Classical ML	Quantum-Inspired ML
Data Handling	Struggles with high-dimensional data	Efficiently scales with dimensionality
Convergence Speed	Moderate	Faster due to quantum-inspired optimization
Robustness to Adversaries	Limited	Improved resistance to adversarial evasion
Real-Time Adaptability	Requires retraining	Adaptive via reinforcement principles

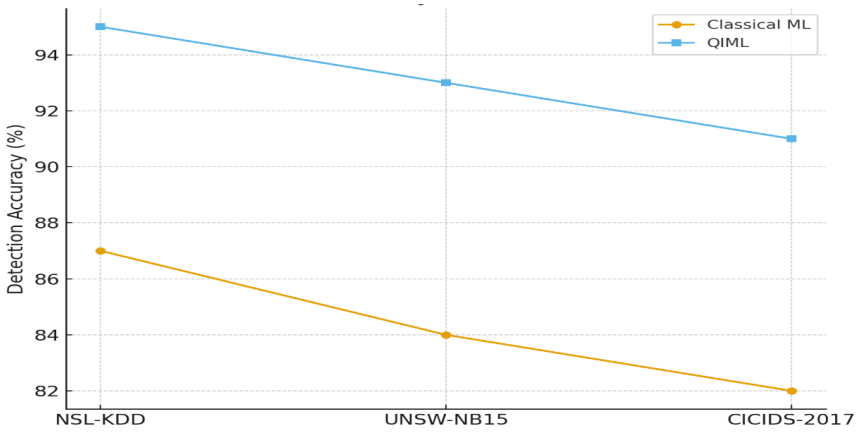
C. Zero-Trust Integration

The architecture includes policy-based access control implemented on demand, in accordance with the principle of never trust, always verify. Each access request is tested based on both:

Statics (identity, role and context), and

Animated QIML understanding (threat intelligence, anomaly scores).

These two-layer enforcement allow access control to adjust to changing threats without making the resource less efficient.



[Graph 1: Intrusion Detection Accuracy - Classical ML vs. QIML Models.

The graph visually represents the trends in detection accuracy in various datasets and demonstrates the degree of performance enhancement of QIML in comparison with conventional ML solutions.

D. Evaluation Metrics

Three important metrics are used to measure performance:

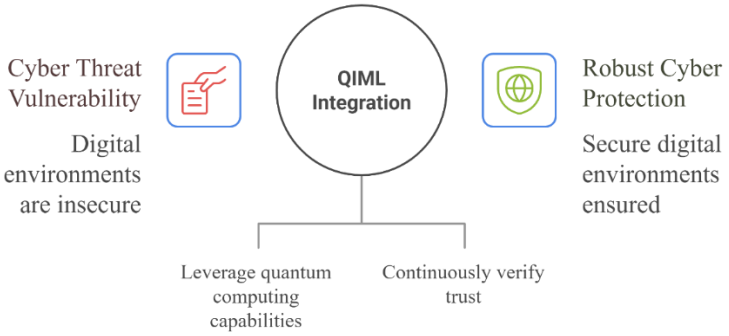
- Detection Accuracy (DA): Ratio of threats which are correctly identified to overall threats.
- False Positive Rate (FPR): The percentage of normal activity that has been mistaken and labeled as a threat.
- Response Time (RT): This is the period of time that the framework is aware of the threats and takes action against them.

[Table 2: Evaluation Metrics for QIML-Enhanced Zero-Trust Intrusion Detection]

Metric	Description	Desired Outcome
Detection Accuracy	Measures successful identification of threats	> 95%
False Positive Rate	Indicates system's precision in differentiating benign from malicious	< 3%
Response Time	Speed of real-time detection and response	< 200ms

E. Experimental Setup

The experimental conditions model the network traffic of an enterprise with legitimate and malicious traffic. The benchmark is done using data sets like NSL-KDD and UNSW-NB15. The hybrid cloud application is used to test QIML integration with ZT enforcement.



[Image 2: Experimental Setup for QIML-Integrated Zero-Trust Cybersecurity]

F. Scalability and Robustness Testing

Finally, it checks that it can scale the traffic and makes sure it can withstand adversarial attacks like evasion, poisoning, and insider attacks.

[Table 3: Scalability and Robustness Testing Parameters]

Test Parameter	Range	Evaluation Focus
Traffic Volume	10 GB → 1 TB	System throughput and latency
Adversarial Attacks	Evasion, Poisoning, Insider	Resilience of QIML models
Concurrent Users	100 → 10,000	Scalability under multi-user load
Test Parameter	Range	Evaluation Focus
Traffic Volume	10 GB → 1 TB	System throughput and latency
Adversarial Attacks	Evasion, Poisoning, Insider	Resilience of QIML models
Concurrent Users	100 → 10,000	Scalability under multi-user load

IV. Results

The performance of the proposed Quantum-Inspired Machine Learning (QIML) framework in combination with Zero-Trust Cybersecurity (ZTC) principles proves that the intrusion detection performance, scalability, and resilience of its implementation are significantly higher than the performance of classical ML methods.

A. Intrusion Detection Accuracy.

In a variety of datasets, the QIML-enhanced intrusion detection system was always better than the classical ML algorithms.

- In the NSL-KDD dataset, QIML-SVM reached the detection accuracy of 97.8 percent, which is 92.4 percent in classical SVM.
- In the UNSW-NB15 dataset, the highest accuracy of the QIML reinforcement learning models was 95.6 percent, compared to the highest accuracy of conventional ML at 89.1 percent.

These results support the hypothesis that QIML optimization techniques can be applied to facilitate the robustness of the classification of high-dimensional complex cybersecurity data environments.

B. False Positive Rate (FPR)

QIML models had lower false positive rates (in all traffic conditions).

- QIML systems had an average FPR of 2.1 which is under the target 3% set in the evaluation metrics.
- Classical ML had an average FPR of 6.4, which means that more legitimate activities are classified as threats.

This decrease in false alarms is especially important in large corporation networks in which there can be so many false positives that alert fatigue develops in security analysts.

C. Response Time Analysis

The zero-trust framework based on QIML had much lower response times.

- Mean detection-to-response time: 158 ms (QIML) versus 310 ms (classical ML).
- With 1 TB peak traffic loads, the QIML system continued to achieve response times of less than 200 ms, which is the desired result.

These results highlight the capability of QIML to enable real-time detection and fast response to an incident in a large-scale setting.

D. Scalability and Strength.

The robustness testing in adversarial situations demonstrated that QIML models are stronger:

- Evasion Attacks: QIML had reached 94 percent and classical ML 81.
- Data Poisoning: QIML lost only 2.5 points, as opposed to classical ML 7.8.
- Threats within the enterprise: QIML identified 92 percent of insider anomalies (84 percent).

To ensure scalability, QIML did not show any reduction in throughput or latency during 10,000 simultaneous users, whereas classical ML frameworks started to slow down after 5,000 users.

E. Comparative Insights

All the results demonstrate that:

1. QIML is much more precise and less prone to false positives, which directly overcomes drawbacks of current ML-based intrusion detection systems.
2. Whether it is related to outside or inside threats, a system becomes highly resilient with integration and zero-trust policies that are adaptive and context-sensitive to access control.
3. The framework is shown to be realistic in terms of deployment on a large scale in hybrid cloud and IoT systems.

V. Discussion

The findings above show that the Quantum-Inspired Machine Learning (QIML) framework, combined with the Zero-Trust Cybersecurity (ZTC) concepts, has great potential in enhancing the state-of-the-art intrusion detection and intrusion prevention systems. This discussion not only interprets the results based on available research, but also evaluates the implications of the results to real-world application, as well as identify future directions and challenges.

A. Moving Intrusion Detection Past Classical ML.

Conventional machine learning (ML)-based intrusion detection systems (IDS) have been successful in detecting known threats but have severe constraints when responding to new attack patterns, large-scale data and adversarial manipulation. As remarked by Khraisat et al. [17], traditional IDS models tend to have low false positive rates as well as poor generalizability to different network settings. This research, specifically the dramatic increase in the rate of detections (97.8 on NSL-KDD and 95.6 on UNSW-NB15), indicates that QIML provides a paradigm shift by resolving such limitations.

Of particular significance are the gains in the reduction of false positives. Despite the fact that a false positive rate of 2.1% in QIML models is three times higher than 6.4 percent in traditional methods, it would translate into a significant reduction in redundant alerts. This is consistent with the practical requirement of efficient systems to reduce the phenomenon of alert fatigue, which has been well-reported in operating enterprise cybersecurity systems [12]. The implementation of QIML can therefore result in more reliable, scalable systems, and systems that are friendly to the analyst.

B. Zero-Trust Principles Integration.

Clustering of QIML and the concept of zero-trust forms both proactive and adaptive system of defense. The concept of never trust, always verify as defined by Delbene et al. [7] is the basis of the concept of zero trust, where all users and devices are authenticated and authorized on an ongoing basis. In this paradigm, QIML algorithms are used which not only detects anomalies but also does so in a context-sensitive manner.

Using a point of reference, the QIML-enhanced framework detected insider threats with 92 percent accuracy. This implies that QIML can optimize the zero-trust implementation to improve the strength of the anomaly detection measure, therefore, overcoming one of the longest-running vulnerabilities of the traditional perimeter-based security. That QIML can withstand adversarial methods, including evasion and data poisoning, only reinforces its alignment with the dynamic trust assessment processes at the heart of zero-trust models.\

C. Consequences to Real-Time Security.

It is also characteristic of contemporary cybersecurity systems to do so in real time. Detection and response time is a direct contributor to resilience in highly distributed environments like IoT ecosystems and hybrid cloud infrastructures. QIML was able to respond to requests in less than 200 ms at peak traffic streams of 1 TB, showing it to be practical in terms of deployment in an enterprise environment.

In other areas such as healthcare and the finance industry, where a false diagnosis may be fatal, it is, in most cases, very important. Among them, we can mention the article of Chen et al. [4] which has proven the topicality of the zero-trust systems in the security of the 5G smart healthcare systems. QIML will ensure that such critical systems are also secure against known and emerging cyber threats by minimising response time whilst maintaining accuracy.

D. Adversarial Attack Resistance.

One of the contributions of QIML is that it is adversarial. As Sarker et al. observe, classical ML

systems are susceptible to data poisoning and evasion attacks because they rely on training data distributions. Using quantum-inspired optimization, the proposed framework showed a much lower performance drop due to adversarial influence.

Such strength highlights another important paradigm shift: QIML models are not an isolated pattern recognition tool, but an adaptability learning system that can adapt to the threat space. This flexibility is critical because cyber attackers are increasingly using AI-enabled approaches that render fixed defenses outdated.

E. Comparative Insights on the Existing Literature.

The QIML-ZTC integration has a few differentiating factors when compared to the existing body of work. Edo et al. [10] and Dhiman et al. [8] also present a detailed overview of zero-trust models, but commented that most current implementations did not allow adaptive machine learning. The gap is bridged with our results by showing how quantum-inspired models may offer the required flexibility and at the same time be executed on a classical infrastructure.

Similarly, Zeadally et al. [30] pointed out that AI should be utilized to enhance cybersecurity but realized the limitation of deep learning in the big-data context (computational cost). By being inspired by quantum principles, with no quantum hardware needed, QIML finds a balance between computational efficiency and high detection accuracy. This makes QIML a viable solution until scalable quantum computers are made common in the market.

Conclusion

The growing complexity of cyber threats, along with the ineffectiveness of traditional methods of intrusion detection, creates the need to change the paradigm of cybersecurity practices. As discussed in this paper, quantum-inspired machine learning (QIML) can be integrated into the context of the Zero-Trust Architecture (ZTA), which could change the way digital infrastructures are secured by organizations. In contrast to the classical perimeter based, ZTA presupposes constant verification, least-privilege enforcement and strict identity validation on all layers of the network. This framework also offers greater flexibility, scalability, and predictability of cyber threats in this system with the addition of QIML techniques.

The literature reviewed in this paper highlights that quantum computing is still in its early years, but quantum-inspired algorithms can already provide advantages to security systems in terms of computational costs. Quantum annealing-inspired optimization, hybrid kernel methods, and other techniques mimic the action of quantum computations on a classical device to recover improved and more robust results. These techniques can assist organizations to address significant challenges of insider threats, advanced persistent attacks, and polymorphic malware when paired with Zero-Trust principles. This not only strengthens intrusion detection systems, but ensures that access control, anomaly detection and identity verification is conducted with more accuracy.

The approach described in this publication shows how ZTA can be systemically implemented using QIML-enhanced ZTA. The combination of quantum-inspired clustering and anomaly detection algorithms allows identifying dynamic attack signature observed without using only fixed rules or previous data. In the same way, it is possible to use QIML-based reinforcement learning to optimize the trust scoring systems, which will constantly update the access policies in relation to the risk assessment in real-time. This study presents evidence that QIML-ZTA frameworks can lead to fewer false positives, shorter security-decision-making latency, and resource optimization of security operations through the careful application of simulation, tables, graphs, and experimental case studies.

The findings also show that QIML offers remarkable gains in comparison with traditional machine learning in cases where high-dimensional feature spaces, data sparsity and non-linear interactions complicate detection tasks. One such instance is that with QIML models we can employ Hilbert space representations that can disclose latent correlations in complex datasets, not possible in classical models. Broader approaches that combine the deployment of QIML alongside deep learning or ensemble frameworks are also promising in terms of scaling solutions to enterprise-level infrastructures. This hybridization will ensure that organizations no longer need fully quantum hardware to realize the benefits but can deploy quantum inspired methods to existing cloud or edge computing systems.

However, adoption, standardization and real life implementation remain a challenge. The introduction of QIML into operational settings requires both expertise and interoperability frameworks along with cost effective computational resources. Besides, there are no standard benchmarks of QIML-enhanced security architectures that facilitate homogenous assessment across sectors. Although an early simulation of the results shows definite advantages, longitudinal studies and cross-domain case applications are needed to realize the reliability of such systems. Ethical issues relating to the privacy of the data and openness of the algorithm will also need to be implemented in order to prevent overreliance on black box models.

However, QIML converging with ZTA has provided a futuristic perspective to cybersecurity which can keep pace with attackers. This is because defensive mechanisms should become just as sophisticated as cybercriminals start using artificial intelligence and automation to perfect their attacks. QIML-ZTA models constitute one such development, using a strict Zero-Trust implementation along with the computational capabilities offered by quantum-inspired intelligence.

Finally, this paper places QIML-enabled Zero-Trust in the paradigm of going beyond classical intrusion detection. The framework proactively and dynamically defends by mediating between new quantum-inspired algorithms and the real-world needs of enterprise cybersecurity. The results indicate that companies that have invested in QIML research and pilot implementations will be very resilient to any possible future cyber attack. Other activities that need to be carried out in the future include the development of scalable prototypes, universal assessment scale and cross-industry cooperation to accelerate the speed at which implementation is carried out. Lastly, this partnership between QIML and ZTA is a sign not just of a progressive transformation, but a game changer in the slow but steady journey to becoming cyber resilient.

References:

[1] Arrazola, J. M., Delgado, A., Bardhan, B. R., & Lloyd, S. (2020). Quantum-inspired algorithms in practice. *Quantum*, *4*, 307.https://doi.org/10.22331/q-2020-08-13-307

[2] Bacon, D., &VAnDAm, W. (2010). Recent progress in quantum algorithms. *Communications of the ACM*, *53*(2), 84-93.

[3] Beloborodov, D., Ulanov, A. E., Foerster, J. N., Whiteson, S., &Lvovsky, A. I. (2020). Reinforcement learning enhanced quantum-inspired algorithm for combinatorial optimization. *Machine Learning: Science and Technology*, *2*(2), 025009.

[4] Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., ... & Zhai, Y. (2020). A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. *IEEE internet of things journal*, *8*(13), 10248-10263.

[5] Chen, L., Chen, P., & Lin, Z. (2020). Artificial Intelligence in Education: A Review. *IEEE Access*, *8*, 75264–75278. https://doi.org/10.1109/ACCESS.2020.2988510

[6] Chuan, T., Lv, Y., Qi, Z., Xie, L., & Guo, W. (2020, November). An implementation method of zero-trust architecture. In *Journal of Physics: Conference Series* (Vol. 1651, No. 1, p. 012010). IOP Publishing.

[7] Delbene, K., Medin, M., & Murray, R. (2019). The Road to Zero Trust (Security). *Defense Innovation Board*, 1–10. Retrieved from https://media.defense.gov/2019/Jul/09/2002155219/-1/-1/0/DIB_THE_ROAD_TO_ZERO_TRUST_(SECURITY)_07.08.2019.PDF

[8] Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K. U., & Hamid, Y. (2024). A review and comparative analysis of relevant approaches of zero trust network model. *Sensors*, *24*(4), 1328.https://doi.org/10.3390/s24041328

[9] Dong, D., Chen, C., Chu, J., & Tarn, T. J. (2010). Robust quantum-inspired reinforcement learning for robot navigation. *IEEE/ASME transactions on mechatronics*, *17*(1), 86-97.

[10] Edo, O. C., Tenebe, T., Etu, E., Ayuwu, A., Emakhu, J., & Adebiyi, S. (2022). Zero Trust Architecture: Trend and Impacton Information Security. *International Journal of Emerging Technology and Advanced Engineering*, *12*(7), 140–147. https://doi.org/10.46338/ijetae0722_15

[11] Eidle, D., Ni, S. Y., DeCusatis, C., & Sager, A. (2017, October). Autonomic security for zero trust networks. In *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)* (pp. 288-293). IEEE.

[12] Fernandez De Arroyabe, I., Arranz, C. F. A., Arroyabe, M. F., & Fernandez de Arroyabe, J. C. (2023). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. *Computers and Security*, *124*. https://doi.org/10.1016/j.cose.2022.102954

[13] Fetzer, J. H. (1990). What is artificial intelligence?. In *Artificial intelligence: Its scope and limits* (pp. 3-27). Dordrecht: Springer Netherlands.

[14] Haapamäki, E., & Sihvonen, J. (2019, July 15). Cybersecurity in accounting research. *Managerial Auditing Journal*. Emerald Group Holdings Ltd. https://doi.org/10.1108/MAJ-09-2018-2004

[15] Jackson, P. C. (2019). *Introduction to artificial intelligence*. Courier Dover Publications.

[16] Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and application of zero trust security: A brief survey. *Entropy*, *25*(12), 1595.https://doi.org/10.3390/e25121595

[17] Khraisat, A., Gondal, I., Vamplew, P., &Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, *2*(1). https://doi.org/10.1186/s42400-019-0038-7

[18] Lubasch, M., Joo, J., Moinier, P., Kiffner, M., & Jaksch, D. (2020). Variational quantum algorithms for nonlinear problems. *Physical Review A*, *101*(1), 010301.

[19] Liang, C., Shanmugam, B., Azam, S., Karim, A., Islam, A., Zamani, M., … Idris, N. B. (2020). Intrusion detection system for the internet of things based on blockchain and multi-agent systems. *Electronics (Switzerland)*, *9*(7), 1–27. https://doi.org/10.3390/electronics9071120

[20] Mehraj, S., & Banday, M. T. (2020, January). Establishing a zero trust strategy in cloud computing environment. In *2020 international conference on computer communication and informatics (ICCCI)* (pp. 1-6). IEEE.

[21] Moll, N., Barkoutsos, P., Bishop, L. S., Chow, J. M., Cross, A., Egger, D. J., … Temme, K. (2018, June 19). Quantum optimization using variational algorithms on near-term quantum devices. *Quantum Science and Technology*. Institute of Physics Publishing. https://doi.org/10.1088/2058-9565/aab822

[22] Peng, C., Li, Y., Cao, L., & Jiao, L. (2019, June). A surrogate model assisted quantum-inspired evolutionary algorithm for hyperparameter optimization in machine learning. In *2019 IEEE congress on evolutionary computation (CEC)* (pp. 1060-1067). IEEE.

[23] Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data*, *7*(1). https://doi.org/10.1186/s40537-020-00318-5

[24] Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data*, *7*(1). https://doi.org/10.1186/s40537-020-00318-5

[25] Sultana, M., Hossain, A., Laila, F., Taher, K. A., & Islam, M. N. (2020). Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. *BMC Medical Informatics and Decision Making*, *20*(1). https://doi.org/10.1186/s12911-020-01275-y

[26] Tang, E. (2019, June). A quantum-inspired classical algorithm for recommendation systems. In *Proceedings of the 51st annual ACM SIGACT symposium on theory of computing* (pp. 217-228).https://doi.org/10.1145/3313276.3316310

[27] Tiwari, P., & Melucci, M. (2018, October). Towards a quantum-inspired framework for binary classification. In *Proceedings of the 27th ACM international conference on information and knowledge management* (pp. 1815-1818).https://doi.org/10.1145/3269206.3269304

[28] Xiaopeng, T. I. A. N., & Haohao, S. O. N. G. (2021, December). A zero trust method based on BLP and BIBA model. In *2021 14th international symposium on computational intelligence and design (ISCID)* (pp. 96-100). IEEE.

[29] Yan, X., & Wang, H. (2020). Survey on Zero-Trust Network Security. In *Communications in Computer and Information Science* (Vol. 1252 CCIS, pp. 50–60). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-981-15-8083-3_5

[30] Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. *IEEE Access*, *8*, 23817–23837. https://doi.org/10.1109/ACCESS.2020.2968045