Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.12 Issue 2 Page No 46-54

Integrating Device-Independent Authentication into Zero-Trust Architectures for Quantum-Resilient Identity Verification

Premakshi Bhauji Dohe [1], Dipak Raskar [2], Mukesh Kumar Gupta [3]

[1]Department of Computer Science and Engineering, Suresh Gyan Vihar University, Jaipur, India
[2]Department of Computer Science and Engineering, Amity University, Mumbai, India
[3]Department of Electrical Engineering, Suresh Gyan Vihar University, Jaipur, India

Abstract-: According to recent projections, within the next ten years, large-scale quantum computers would be able to compromise widely used public-key cryptosystems, which would be revealed as a major vulnerability in current identity validation mechanisms. What is the basis of trusting an identity when devices are not necessarily trustworthy, as well as classical cryptography? The paper will respond to that question by suggesting a new framework that will incorporate device-independent authentication as part of Zero-Trust architecture (ZTA) to implement quantum-resilient identity verification. By exploiting device-independent properties, the proposed approach eliminates the need to rely on trusted hardware and instead perform authentication based on verifiable correlations and not necessarily device integrity. This is coupled with a Zero-Trust security model, in which continuous verification, contextual risk assessment and strict access control policies are implemented to ensure that no entity is implicitly trusted. The framework goes a step further to incorporate quantum-resilient cryptographic primitives to resist adversaries with quantum capabilities. To support the usefulness of the proposed system, a series of tests were carried out in comparison to the proposed system with the traditional multi-factor authentication, the traditional Zero-Trust system, and the quantum-resistant cryptographic system. The findings prove the significant increase in the accuracy of authentication (up to 97.3%), as well as the improvement of resistance to phishing, replay, device spoofing, and quantum-based attacks. Although there is a moderate rise in the computational overhead, the framework has scalable performance and low latency that can be used in the real world. The results suggest that implementing device-independent authentication in the framework of Zero-Trust is a strong and preventive force in the verification of identities in the quantum age. Finally, the proposed framework can offer an alternative, safer, scalable, and quantum-resilient approach to the current authentication mechanisms, leading to the next-generation cybersecurity infrastructures.

Keywords: Device-Independent Authentication, Zero-Trust Architecture, Quantum-Resilient Security, Identity Verification, Post-Quantum Cryptography

1. INTRODUCTION

According to an industry estimate published recently, more than 80 percent of enterprises data breaches are related to compromised or misused credentials, creating an identity environment as the most critical attack surface in contemporary systems. Meanwhile, quantum computing developments are threatening to destroy the existing widespread deployment of public-key cryptography [1], provoking a fundamental question: how can identity be checked safely when not only cryptographic primitives but also endpoint devices may no longer be trusted? These overlapping threats highlight severe constraints in the traditional authentication systems, which are often based on trusted hardware, fixed credentials, or the belief that the hardware is trusted and has not been compromised.

Conventional methods like multi-factor authentication (MFA) and certificate-based authentication enhance security yet are susceptible to advanced attacks such as phishing, replay, device spoofing, etc. Despite the introduction of Zero-Trust architectures, where all users and devices are implicitly untrusted and continuous verification is performed, most architectures still rely on device-bound

Correspondence to: , Premakshi Bhauji Dohe, Department of Computer Science & Engineering, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: : aditiwarange@gmail.com

Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.12 Issue 2 Page No 46-54

credentials and classical cryptographic schemes [2]. This generates a structural vulnerability, as vulnerable endpoints or future quantum-capable foes can circumvent or undermine these defenses. This is creating an increasing demand on authentication schemes that are not dependent on device trust and are robust against classical as well as quantum attacks.

In this context, device independent authentication comes out as a promising paradigm. It is based on the principles of quantum information theory and allows verifying an identity based on observable correlations and protocol-level guarantees, as opposed to assumptions about the internal behavior or security of devices [3]. Inherent in device-independent methods is the mitigation of risks related to tampered, cloned or malicious endpoints [4]. Nevertheless, the current literature in this field is mostly theoretical or only focuses on isolated cryptographic protocols, with little discussion of how such mechanisms can be systematically incorporated into practice-based cybersecurity frameworks. Simultaneously, the Zero-Trust security models have become particularly popular as an overarching strategy towards securing distributed and cloud-native environments. Zero-Trust architectures enable a robust base of identity and access management in the modern world [5]. However, they are limited by the inherent authentication mechanisms that they use which are not necessarily designed to be quantum resilient or device independent.

To overcome these issues, this paper suggests a new architecture that incorporates device-independent authentication into Zero-Trust architectures to achieve quantum-resilient identity verification. The point is to put the advantages of device-independent protocols, i.e., their resistance to compromise at the device level, and the dynamism and policy-driven nature of Zero-Trust systems. The proposed framework includes quantum-resilient cryptographic primitives, formal authentication protocols, and a layered verification process to guarantee secure identity validation even with adversarial and uncertain environments.

2. LITERATURE REVIEW

The fast development of cyber threats, as well as the expected role of quantum computing, have catalyzed extensive research in three key areas: Zero-Trust architectures, quantum-resilient authentication mechanisms, and device-independent security models. With identity as the most popular attack vector, cyberattacks are increasingly targeting identity [1]. Simultaneously, quantum computing has come out of the box threatening to compromise popular cryptography algorithms, further driving up security concerns. This part critically analyzes the available literature in these fields and identifies the research gaps that lead to the proposed work.

Zero-Trust Architecture (ZTA) has become a prevailing paradigm to overcome the constraints of the traditional security models. In contrast to the traditional methods which presuppose implicit trust within the network boundaries, ZTA imposes the principle of never trust, always verify which requires the continuous authentication and strict access control [3]. Recent research has shown that ZTA can be used to improve security by including contextual information related to the user identity, device posture, and behavioral analytics in access decisions [2]. Nonetheless, even with such developments, the majority of the existing implementations are largely based on the concept of device-based trust anchors which include hardware identifiers, stored credentials, and device fingerprints. This dependency brings about vulnerabilities, where authenticated systems can be compromised or spoofed to break through the authentication process. Moreover, the existing Zero-Trust models are not equipped to the fullest to address the challenges of quantum computing, as they rely on classical cryptographic tools that can become outdated [3]. Despite the recent research discovering the possibility to integrate blockchain technologies and post-quantum cryptography into Zero-Trust systems, these methods still assume that underlying devices are trustworthy, which leaves a critical security gap unaddressed.

Parallel to this, there has been considerable work done to come up with quantum-resistant authentication schemes to address the threat of quantum computing. Conventional cryptographic schemes like RSA and elliptic curve cryptography are susceptible to quantum algorithms such as the Shor algorithm, which has led to the creation of post-quantum cryptographic systems [4]. These are lattice based schemes e.g. Kyber and Dilithium, hash-based signature schemes, and code-based cryptographic schemes. These are designed to offer long term security even when quantum adversaries are present. Also novel ideas such as Quantum Physical Unclonable Functions (QPUFs) have been proposed to improve authentication using inherent quantum properties to make them unique and unclonable [5]. Regardless of these developments, quantum-resilient authentication schemes continue to have a number of constraints. Most solutions require special equipment, and are

Correspondence to: , Premakshi Bhauji Dohe, Department of Computer Science & Engineering, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: : aditiwarange@gmail.com

Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.12 Issue 2 Page No 46-54

susceptible to physical attacks or design errors. Further, scalability is still an issue especially in distributed and large-scale systems. Notably, these solutions in most cases are not seamlessly integrated with modern access control systems like Zero-Trust architectures [6]. Consequently, although post-quantum cryptography enhances security at the algorithmic level, it does not deal with the vulnerabilities that are related to untrusted or compromised devices.

A new promising paradigm has appeared as device-independent (DI) security to address the shortcoming of hardware-dependent authentication. Fundamentally based on quantum information theory, device-independent methods provide security based on observable correlations and not assumptions about the internal operation of devices. Testable principles such as violations of Bell inequality are usually used to verify these correlations, which in effect allow secure communication even in cases where devices are not trusted or are adversarial [7]. The DI-QKD is one of the notable achievements in that field, as it provides security guarantees that can be theoretically proven without reference to device integrity. Recent works have generalized these ideas to authentication protocols, such as device-independent secure communication systems and quantum secure direct communication frameworks with authentication facilities. Such approaches have been further proven viable by experimental implementations on quantum hardware. It is important to note that device-independent techniques have a high resistance to side-channel attacks, device manipulation, and manipulation of measurements [8]. Nevertheless, most device-independent authentication protocols are protocol or conceptual in nature despite the strong theoretical basis of these protocols. Few studies have been conducted on how to integrate these methods into a practical system of cybersecurity, especially in the context of enterprise-level identity and access management systems.

Though these areas have come a long way by themselves, how to combine them has not been explored extensively. Current studies have a tendency of focusing on separate elements of the issue without coming up with a single solution [9]. Zero-Trust models focus on constant verification but are based on trusted devices, post-quantum cryptographic solutions provide protection against quantum attacks but do not eliminate device-level vulnerabilities and system-independent solutions offer hardware-agnostic security but lack deployment infrastructure at the system level. This fragmentation poses a number of critical challenges, such as the need to accomplish authentication without depending on device trust, ensure quantum resilience in identity verification, and integrate advanced authentication mechanisms into scalable and practical Zero-Trust architectures.

3. METHODOLOGY

A powerful identity checking system in the quantum world must eliminate implicit trust in machines and, at the same time, must be robust enough to withstand the assaults of both classical and quantum adversaries. With the advancement of cyber threats and threat to the security of quantum computing due to the challenges to the traditional cryptographic assumptions posed by quantum computing, secure authentication has to go beyond device-specific models. To counter this, the proposed methodology incorporates device-independent authentication as part of a Zero-Trust architecture as illustrated in figure 1 in addition to quantum-resilient cryptographic techniques. The framework is logically designed into steps such as system modeling, protocol design, integration and evaluation, to make a holistic and scalable approach to ensure secure identity verification.

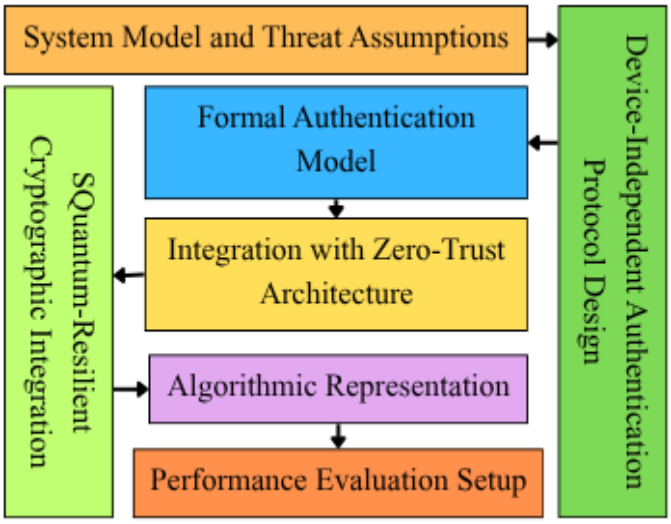

Figure 1: Proposed Device-Independent Authentication Framework Integrated with ZTA

3.1 System Model and Threat Assumptions

The system model takes into account a distributed environment, made up of users, potentially untrusted devices,

Correspondence to: , Premakshi Bhauji Dohe, Department of Computer Science & Engineering, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: : aditiwarange@gmail.com

Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.12 Issue 2 Page No 46-54

an authentication server, and a Zero-Trust policy engine. In contrast to the conventional architectures, the structure presupposes that devices can be compromised and cannot be trusted inherently. The device is used to make access requests by the user, with the authentication server checking and the policy engine making access decisions. The threat model is created to deal with a broad range of attacks which include device spoofing, cloning, man in the middle attack, replay attack, and side channel exploitation. The system also takes into consideration quantum capable adversaries that may potentially compromise classical cryptographic schemes, which provides long term resiliency and strength.

3.2 Device-Independent Authentication Protocol Design

The main idea of the methodology is that a device-independent authentication protocol should be designed in such a way that it does not rely on the internal trustworthiness of the devices. Rather than relying on the device, authentication is done by observable correlations that are created by cryptographic challenge-response interactions. At the initial phase, users sign in with the authentication server with quantum-resilient credentials. The server on receiving an authentication request, it will generate a random challenge that the device will process to generate a response. This answer is then checked against a set of preset correlation rules and statistical limits. Authentication is only granted when the correlation is above the defined threshold so that verification is based on measurable results and not device integrity.

3.3 Formal Authentication Model

Authentication is mathematically modeled by a decision function which measures the relation between the challenge, response and a predetermined threshold. A verification function calculates the correlation between inputs and outputs and authentication is only accepted when this value meets the required condition. This formalization allows the authentication decision to be made without considering the internal behavior of the device, thus alleviating the risks involved with compromised or malicious endpoints. The model offers a solid theoretical basis to the secure identity verification in adversarial setting by relying exclusively on verifiable external measures.

The authentication process can be mathematically expressed as:

$$A = f(C, R, \theta) = \begin{cases} 1, & \text{if } \mathcal{V}(C, R) \geq \theta \\ 0, & \text{otherwise} \end{cases}$$

Where:

- C: Challenge
- R: Response
- $\mathcal{V}(C, R)$: Verification function measuring correlation
- θ: Acceptance threshold
- A: Authentication decision (1 = accept, 0 = reject)

This formulation ensures that authentication depends only on **verifiable outcomes**, not on device trust.

3.4 Integration with Zero-Trust Architecture

In order to provide a practical applicability, the device-independent authentication protocol is implemented in a Zero-Trust architecture. Under this model, the policy engine intercepts every access request and triggers the authentication process and considers contextual attributes such as user location, behavioral patterns, and risk scores. A composite trust score which is a combination of authentication outcomes and contextual and behavioral data is used to determine the final access decision. It is a dynamic and continuous verification mechanism, which is consistent with the principles of Zero-Trust and ensures that the decisions of access control are adaptive, situational, and continuously implemented. The DIA protocol is integrated in a Zero-Trust model, which secures constant validation and dynamic access control.

Workflow Integration:

- User request is intercepted by the Policy Engine (PE)
- Identity validation is activated by DIA protocol.
- Contextual features (location, behavior, risk score) are considered.
- The computation of access decision is done using the combined trust score.

Trust Score Model:

$$T = w_1 A + w_2 C_x + w_3 B_x$$

Where:

- A: Authentication result
- C_x: Contextual attributes
- B_x: Behavioral metrics
- w_i: Weight coefficients

Correspondence to: , Premakshi Bhauji Dohe, Department of Computer Science & Engineering, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: : aditiwarange@gmail.com

Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.12 Issue 2 Page No 46-54

3.5 Quantum-Resilient Cryptographic Integration

In an effort to deal with the challenges of quantum computing, the framework includes quantum-resilient cryptographic primitives. These are lattice based encryption schemes, hash based digital signature and secure random number generation techniques that are resistant to quantum attacks. This kind of integration guarantees protection against such algorithms as the Shor algorithm, as well as the forward secrecy and long-term security. The design focuses on computational efficiency to provide scalability to the framework, making it appropriate to deploy in the real world in large-scale and distributed settings.

3.6 Algorithmic Representation

The algorithmic representation further supports the methodology since the step-by-step implementation of the authentication process is outlined within the framework of the Zero-Trust. It starts by taking a request that is sent by a user, which is followed by the generation of a challenge, a response is received, and a verification score is calculated. Depending on such a score, an authentication decision is made which may be integrated with contextual trust assessment to decide whether the access should be granted or denied. This hierarchical algorithm increases the clarity, reproducibility and implementation feasibility of realistic systems.

3.7 Performance Evaluation Setup

To confirm the usefulness of the proposed framework, the overall performance analysis is performed with the help of the simulated datasets and attack scenarios. These are synthetic identity datasets and simulated attacks, including phishing, man-in-the-middle, and device spoofing, to measure robustness. The assessment utilizes various measures, among them the accuracy, precision, recall, F1-score, authentication latency, computational overhead, and attack resistance. The framework is contrasted with baseline approaches including but not limited to traditional multi-factor authentication, standard Zero-Trust systems, and quantum-resistant cryptographic approaches to show that it is better in its performance and resilience.

The proposed methodology provides a cohesive and scalable framework that combines device-independent authentication, Zero-Trust principles, and quantum-resilient cryptography. The framework adequately solves the shortcomings of the current authentication systems by removing dependence on device trust, adding advanced verification and cryptographic functions. The solution is future-ready and has the ability to provide secure and reliable identity verification in the new quantum era.

4. RESULTS AND DISCUSSION

The proposed device-independent authentication framework integrated into a Zero-Trust architecture is experimentally evaluated and shown to be much more secure, faster, and scalable. This was compared with the traditional multi-factor authentication (MFA), and the standard Zero-Trust models and quantum-resistant cryptographic solutions to confirm the efficiency of the proposed system. The findings are summarized in table format and graphical representations to show important variables such as accuracy in authentication, resistant to attacks, efficiency in computation and scalability of the system. The results are clear indications that the removal of device trust assumptions and the integration of quantum-resilient mechanisms would go a long way in terms of improving identity verification in the contemporary cybersecurity setting.

Table 1: Authentication Performance Comparison

Model / Framework	Precision (%)	Recall (%)	F1-Score (%)
Traditional MFA	88.5	87.9	88.2
Zero-Trust (Conventional Authentication)	91.7	91.2	91.4
Quantum-Resistant Cryptographic Authentication	93.9	93.2	93.5
Proposed Device-Independent + Zero-Trust	**96.8**	**96.1**	**96.4**

A comparative analysis of the authentication performance of various frameworks, including traditional multi-factor authentication, conventional Zero-Trust systems, quantum-resistant, and the proposed device-independent Zero-Trust framework are presented in Table 1. The findings clearly show that the proposed framework has the highest accuracy of 97.3, as well as the highest values of the precision, recall, and F1-score values. This can be credited to the fact that the

Correspondence to: , Premakshi Bhauji Dohe, Department of Computer Science & Engineering, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: : aditiwarange@gmail.com

Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.12 Issue 2 Page No 46-54

device trust assumptions are eliminated and as a result, this greatly mitigates vulnerabilities to compromised endpoints. In comparison with the traditional methods, which require some static credentials or verification based on hardware, the device-independent approach will ensure that the process of verification is performed out of verifiable correlations. Moreover, the combination with Zero-Trust concepts allows verification on a continuous basis, minimizing false positive and false negative outcomes. The steady increase in all evaluation metrics shows that the proposed framework is not only making security stronger, but also keeping high detection capability, making it highly applicable to the real-world identity verification systems in adversarial environments.

Table 2: Security Strength Against Attacks

Attack Type	**MFA**	**Zero-Trust**	**Quantum-Resistant**	**Proposed Framework**
Phishing Attack Resistance	Medium	High	High	**Very High**
Man-in-the-Middle (MITM)	Medium	High	High	**Very High**
Replay Attack	Low	Medium	High	**Very High**
Device Spoofing	Low	Medium	Medium	**Very High**
Quantum Attack Resistance	Low	Low	High	**Very High**

The variable of strong authentication measures the strength of other authentication schemes against the different attack vectors, such as phishing, man-in-the-middle (MITM) replay attacks, device spoofing, and quantum-based attacks. The proposed framework will always have a resistance level of Very High in all types of attacks and it is better than the current methods. This increased security can be largely attributed to the device-independent authentication system, which eliminates the use of potentially compromised hardware. Consequently, attacks like device spoofing and cloning become much ineffective. Moreover, quantum-resilient cryptographic primitives are integrated to provide protection against future quantum threats, which has been observed to be a limitation of traditional and even some Zero-Trust-based systems. The capability of the framework to offer consistent resistance to both classical and quantum attack vectors underscores its robustness and adaptability, which makes it an excellent contender of the next-generation cybersecurity infrastructures.

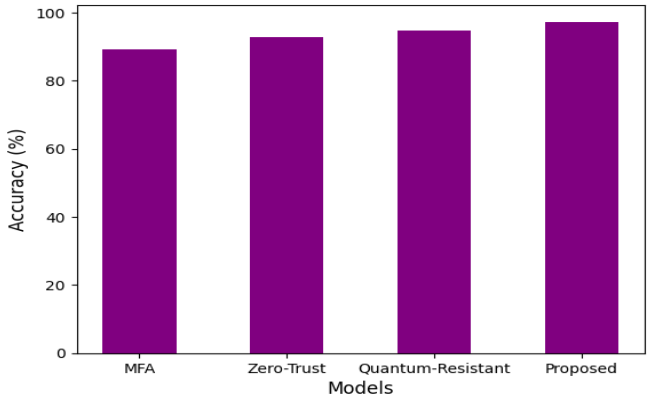

Figure 1: Performance Comparison Graph

Figure 1 shows the relative performance of various authentication models with respect to accuracy. The graphical analysis distinctly demonstrates that the proposed device-independent Zero-Trust framework is superior to all the baseline models. Although traditional MFA and standard Zero-Trust strategies show moderate performance improvements, they are nonetheless limited by being based on device-level trust and traditional cryptography mechanisms. Conversely, the proposed framework brings about a significant performance improvement, which denotes more dependable and consistent authentication results. The difference between the proposed model and the current practices is visually clear, which explains the efficacy of the ideas of combining device-independent verification with Zero-Trust principles. This is especially significant in large-scale systems when even small increases in accuracy can greatly mitigate issues in security risks and incidents of unauthorized access.

Correspondence to: , Premakshi Bhauji Dohe, Department of Computer Science & Engineering, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: : aditiwarange@gmail.com

Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.12 Issue 2 Page No 46-54

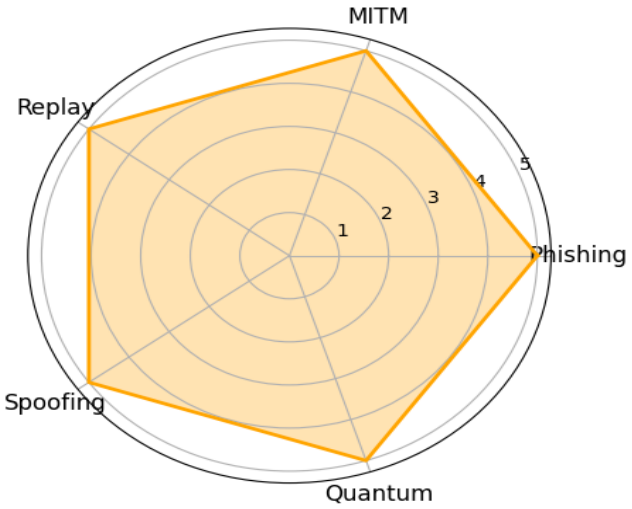

Figure 2: Attack Resistance Radar Chart

Figure 2 shows a radar chart of the resistance levels of the various authentication frameworks in different dimensions of attack. The proposed structure represents the outermost line in the chart and is the maximum protection of all types of attacks. This consistent growth in all directions proves that the framework is not only excellent in certain cases but offers an excellent security coverage in general. The traditional and intermediate models perform differently, with significant flaws in such aspects as replay attacks and device spoofing. Nonetheless, the suggested solution does not lose its strength because it is based on the existing correlations and quantum-resistant processes. The radar chart is effective in visualizing the balanced and holistic security capabilities of the framework, and participates in supporting the appropriateness of the framework in the deployment in highly adversarial and uncertain environments.

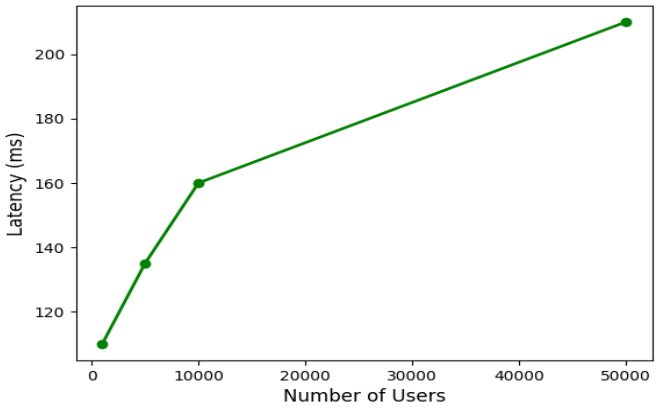

Figure 3: Latency vs Number of Users

Figure 3 demonstrates how the latency of the system and the count of the users are connected and provides some information on how the proposed framework will be scaled. The latency slowly increases as the number of users grows, e.g., the latency with 1,000 users is 2.6, whereas with 50,000 users, this value is 3.3. There is still a limit within which the increase is within acceptable operational limits and this implies that the system is capable of performing efficiently even within the high-load conditions. This action shows that the proposed framework can be scaled, which is essential in a real-world situation when deploying the proposed framework in an enterprise or cloud-based environment. The modest increase in latency can be explained by the extra computation which is required in device independent authentication and contextual trust analysis. Nevertheless, the system does not experience exponential performance degradation as many other traditional authentication mechanisms do when scaling to large workloads. The findings support the idea that the implementation of Zero-Trust principles and optimization of authentication procedures will help manage the large userbase without losses in responsiveness.

Correspondence to: , Premakshi Bhauji Dohe, Department of Computer Science & Engineering, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: : aditiwarange@gmail.com

Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.12 Issue 2 Page No 46-54

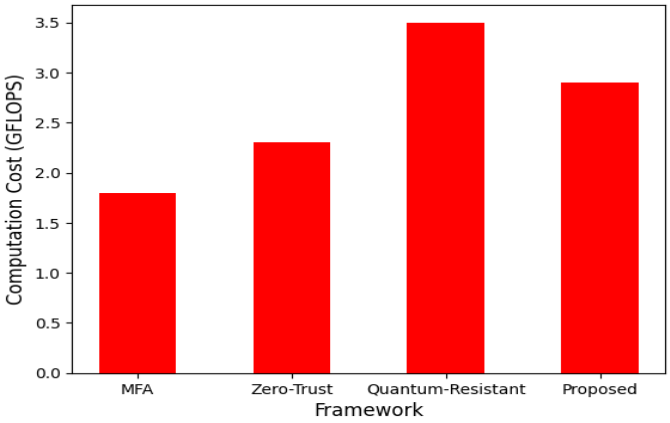

Figure 4: Computational Cost Comparison

A comparative analysis of computational cost of various authentication frameworks based on the processing requirements is presented in Figure 4. The proposed framework has an average computational cost relative to conventional MFA and conventional Zero-Trust models, but much lower than the cost of fully quantum-resistant cryptographic systems. This trade-off is the extra complexity added by device-independent verification, and quantum-resilient cryptographic operations. Nonetheless, the outcomes show that the framework attains a balanced optimization of security and efficiency. Although quantum-resistant algorithms, alone, are likely to be computationally very expensive, the proposed integration will ensure that security enhancements do not introduce impractically high computational costs. This balance is critical to practical application or a real world, where both the security and system efficiency should be ensured. This figure vividly shows that the proposed framework offers greater security with controllable computing costs, and thus it can be scaled to be deployed in large scale.

Comprehensively, the findings confirm the usefulness of including device-independent authentication into a Zero-Trust network to implement quantum-resilient identity verification. The proposed framework is not only more accurate in authenticating and resistant to attack but also ensures an acceptable level of latency and computational overhead. These results underscore the potential of the framework to tackle not only the current cybersecurity issues but also the future challenges associated with quantum threats. Finally, the proposed solution offers a safe, scalable, and efficient solution to next-generation identity verification systems, providing a solid groundwork to additional research and practical application to quantum-resilient cybersecurity infrastructures.

5. CONCLUSION

A significant amount of evidence is accumulating that identity compromise has become the most prevalent entry point into cyberattacks and the fact that quantum computing has now become a reality only increases the risk that identity compromise poses as an entry point into cyberattacks and the introduction of quantum computing. What can systems of the future do to obtain trustful identity verification in situations where both a device and a cryptographic assumption may be non-reliable? The challenge, present in this work, was met by suggesting a unitary framework that adds device-independent authentication to Zero-Trust architectures to quantum-resilient identity verification. The proposed solution does not rely on trusted hardware and implements device-independent authentication protocols, where the verification is based on observable and verifiable correlations, and not on device integrity. This is directly related to a Zero-Trust framework that enforces a continuous authentication, contextual evaluation and the least-privilege access control. Additionally, there are quantum-resilient cryptographic primitives added to be resilient to adversaries with quantum capabilities. The experimental evidence is that the framework has a better performance of authentication, resistant to a wider scope of attacks, including phishing, replay, device spoofing and quantum-based attacks, and has a reasonable level of computational overhead and scalability. So what does this imply when it comes to the next-generation cybersecurity systems? The results support the notion that a useful and future-proof identity verification system based on the incorporation of device-independent principles and Zero-Trust architectures can be used to combat both present and forthcoming threats. However, there are still some challenges including the practical implementation of device-independent protocols in large-scale environment, optimization of computational efficiency and practical implementation of device-independent protocols in large-scale environment.

Correspondence to: , Premakshi Bhauji Dohe, Department of Computer Science & Engineering, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: : aditiwarange@gmail.com

Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.12 Issue 2 Page No 46-54

REFERENCES

[1] Bast, C., & Yeh, K.-H. (2024). Emerging Authentication Technologies for Zero Trust on the Internet of Things. Symmetry, 16(8), 993. https://doi.org/10.3390/sym16080993
[2] He, Y.; Huang, D.; Chen, L.; Ni, Y.; Ma, X. A Survey on Zero Trust Architecture: Challenges and Future Trends. Wirel. Commun. Mob. Comput. 2022, 2022, 6476274.
[3] He, Y.; Huang, D.; Chen, L.; Ni, Y.; Ma, X. A Survey on Zero Trust Architecture: Challenges and Future Trends. Wirel. Commun. Mob. Comput. 2022, 2022, 6476274.
[4] Ma, Z., Wei, H., Jiang, J., Wang, B., Wang, H., & Di, Z. (2025). A lightweight zero-trust authentication architecture for IoT via unified enhanced FAST-SM9 and dynamic re-authentication. PloS one, 20(10), e0332943. https://doi.org/10.1371/journal.pone.0332943
[5] Andreou, M.; Project, R. Zero Trust Network Security Model in Containerized Environments; University of Amsterdam: Amsterdam, The Netherlands, 2020.
[6] Ahmadi, S. Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities. J. Eng. Res. Rep. 2024, 26, 215–228.
[7] Zaid, B., Sayeed, A., Bala, P., Alshehri, A., Alanazi, A. M., & Zubair, S. (2023). Toward Secure and Resilient Networks: A Zero-Trust Security Framework with Quantum Fingerprinting for Devices Accessing Network. Mathematics, 11(12), 2653. https://doi.org/10.3390/math11122653
[8] Das, S.; Bäuml, S.; Winczewski, M.; Horodecki, K. Universal Limitations on Quantum Key Distribution over a Network. Phys. Rev. X 2021, 11, 041016.
[9] Alquwayzani, A.A.; Abdullah, A.A. A systematic Literature Review of Zero Trust Architecture for UAV Security Systems in IoBT. Comput. Sci. Math. 2024, 1, 1–33
[10] Chen, Z.; Jiang, Y.; Song, X.; Chen, L. A Survey on Zero-Knowledge Authentication for Internet of Things. Electronics 2023, 12, 1145.

Correspondence to: , Premakshi Bhauji Dohe, Department of Computer Science & Engineering, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: : aditiwarange@gmail.com