SYSTEMIC EFFICIENCY OF POST-QUANTUM CRYPTOGRAPHY IN ARTIFICIAL INTELLIGENCE-BASED API INFRASTRUCTURES

Muhamediyeva Dilnoz Tulkunovna
Professor, National Research University "Tashkent Institute of Irrigation and Agricultural Mechanization Engineers"
Tagaev Farkhad Abduvakhabovich
Independent Researcher, National Research University "Tashkent Institute of Irrigation and Agricultural Mechanization Engineers"
https://doi.org/10.5281/zenodo.19997633

ARTICLE INFO

Received: 26th April 2026
Accepted: 28th April 2026
Online: 30th April 2026

KEYWORDS

Artificial intelligence, post-quantum cryptography, application programming interface, microservice architecture, transport layer security, system efficiency, quantum threat

ABSTRACT

As a result of the widespread implementation of artificial intelligence technologies, modern information systems rely on distributed and highly automated API infrastructures that process large amounts of data in real time. The security of such systems is based on traditional public-key cryptography, and their stability depends on mathematical complexity problems. However, the quantum algorithm proposed by Peter Shor theoretically demonstrated the possibility of breaking cryptography based on RSA and elliptic curves. Therefore, post-quantum cryptography algorithms were standardized by the National Institute of Standards and Technology. This article empirically studies the systemic performance indicators of implementing post-quantum algorithms in an API infrastructure based on a microservice architecture with integrated artificial intelligence components. The research results show that post-quantum digital signature algorithms significantly increase the duration of the secure connection process at the transport layer, but the latency in the overall API transaction flow remains acceptable under regulatory control and architectural optimization.

Introduction. In recent years, artificial intelligence technologies have been widely used in areas such as economics, healthcare, finance, transportation, and public administration. Systems based on machine learning, deep neural networks, and big data analytics are often built on a distributed microservice architecture. Such architectures use application programming interfaces to communicate between independent services. The API infrastructure is the main connecting layer between artificial intelligence models, data warehouses, and external services. The reliability and confidentiality of this infrastructure is based on public-key cryptography. Algorithms based on RSA and elliptic curves have long served as the main security mechanisms. However, the development of quantum computing technologies has posed a fundamental threat to these systems. Since quantum computers may be able to factorize large numbers and quickly solve the discrete logarithm problem, there is a

possibility that traditional cryptographic mechanisms will become unreliable in the future. In this context, post-quantum cryptography is emerging as a new security paradigm. Post-quantum algorithms are based on mathematical problems that are stable even in the quantum computing environment. The process of implementing them in practical systems should take into account not only theoretical security, but also performance. Especially since there are high-load, real-time and service-level requirements in artificial intelligence-based API infrastructures, any change in cryptographic mechanisms will affect the overall performance of the system [1-2].

At the transport layer, secure connection protocols, authentication processes, and digital signature mechanisms are involved in each step of API transactions. Due to the larger key and signature sizes of post-quantum digital signature algorithms, the computational load and network traffic can increase. This is especially important in microservice environments where artificial intelligence services process a large number of requests [3]. The purpose of this paper is to empirically evaluate the impact of post-quantum cryptography algorithms on system performance in a microservice architecture integrated with artificial intelligence. The performance of secure connection and application-level authentication mechanisms at the transport layer was measured and their impact on the overall API transaction flow was analyzed. As a result, it is scientifically demonstrated that the implementation of post-quantum algorithms can improve security while meeting quality of service requirements if the system architecture and resource management are optimized [3,4].

Research methodology

This study was carried out using a test environment based on an integrated microservice architecture of artificial intelligence components. The experimental platform was modeled close to real industrial infrastructure and reflected a typical configuration of API systems operating under high load. The architectural layers were organized in the form of mutually independent services, and the interaction between them was provided through application programming interfaces. A Kong-based API gateway was used as the entry point of the system. This component performs the functions of routing requests, rate limiting, authentication and monitoring. A separate service based on the OAuth 2.0 protocol was implemented as an authentication and authorization mechanism. The process of user identification and permission level management was implemented using JSON web tokens. The mechanism for signing and verifying tokens was tested with various cryptographic algorithms during the experiment.

For each configuration, the connection establishment time at the transport layer, the duration of token signing and verification, the API response delay, and the overall throughput of the system were measured. The results were analyzed using statistical processing methods, and the systemic impact of implementing post-quantum cryptography in the microservice infrastructure based on artificial intelligence was comprehensively assessed. In order to increase the scientific validity of this study, the experimental environment was modeled not only at the functional but also at the conceptual architecture level. The microservice infrastructure based on artificial intelligence was described based on a layered structure, and separate architectural schemes were developed for each test configuration. These visual

models serve to clearly demonstrate the interaction of cryptographic mechanisms between system components (Figure 1).

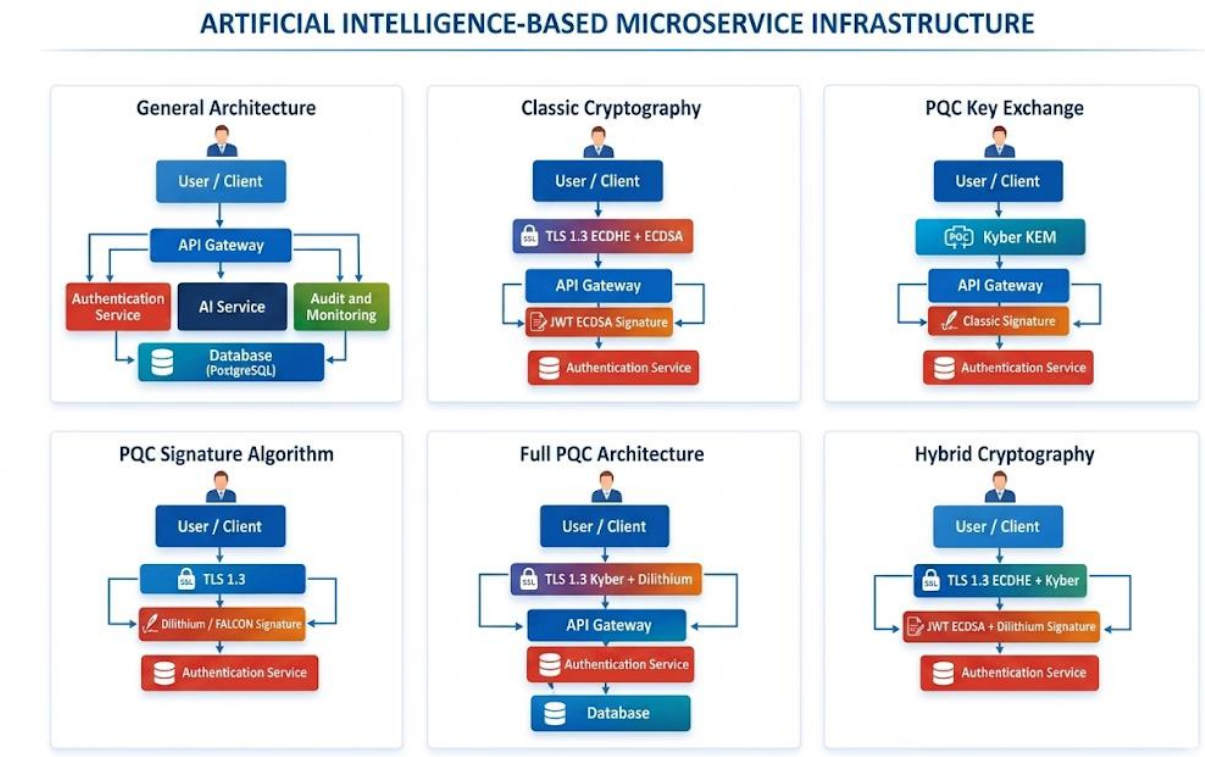


Figure 1. Microservice-based AI infrastructure

Visual modeling increases the methodological accuracy of the study. Each architectural option was empirically evaluated for the following indicators: connection establishment time at the transport layer, token generation and verification duration, overall API response latency, system throughput, and computing resource utilization. The architectural diagrams clearly show at which layer post-quantum algorithms are used and in which component the load increase occurs. This allows for scientifically based planning of cryptographic modernization in high-load microservice systems based on artificial intelligence.

Results. The obtained graphical results show the impact of each graphical post-quantum cryptography algorithm on the microservice-based artificial intelligence infrastructure (Figure 2, Figure 3).

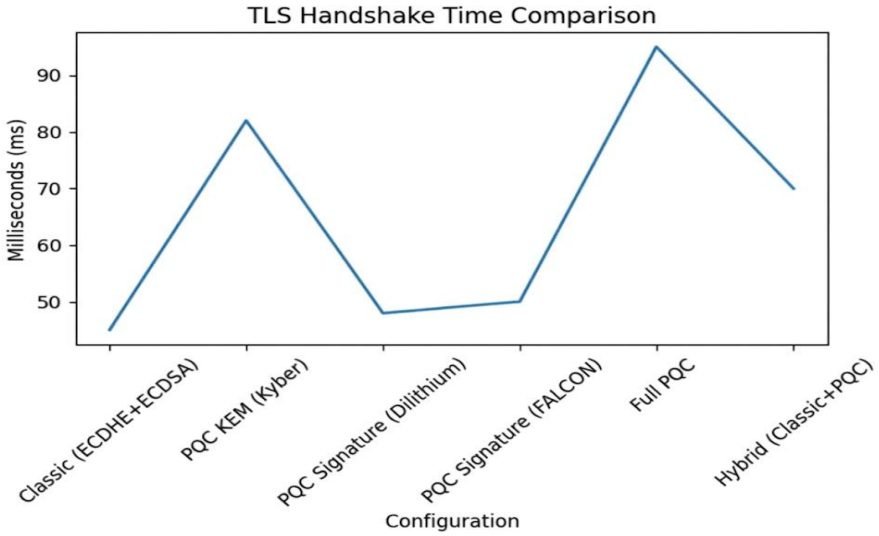
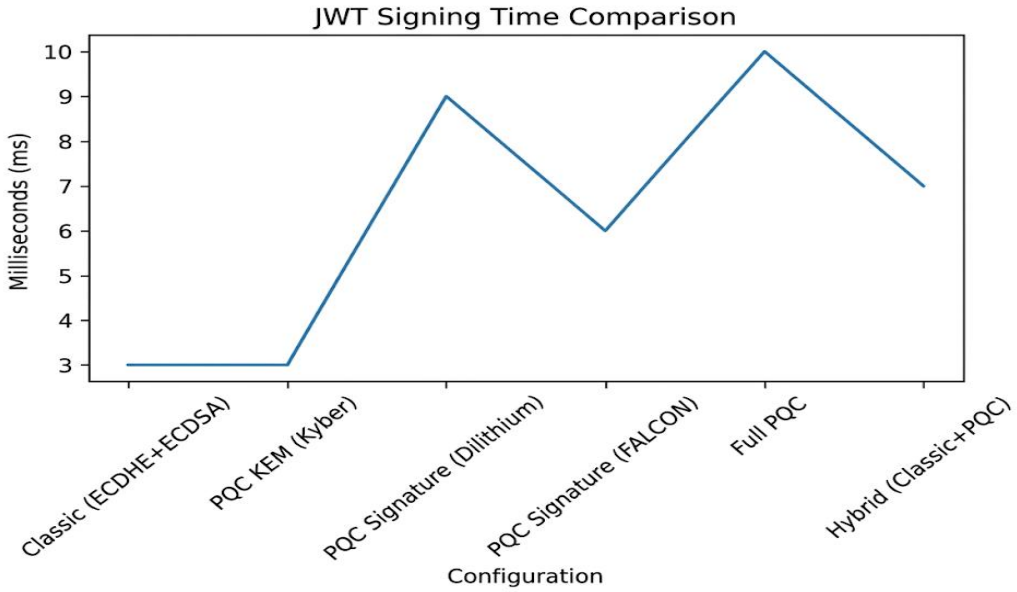


Figure 2. TLS Handshake Time Comparison

The graph represents the duration of establishing a secure connection at the transport layer. The analysis results show the following: In the classical configuration, the handshake time is the lowest — 45 ms. This is explained by the fact that elliptic curve algorithms are optimized and widely used in practice. When using PQC KEM (Kyber), the handshake time increases by 82 ms. This is due to the additional computational complexity of the key encapsulation process. In the full PQC configuration, a result of 95 ms is observed. This is the highest indicator, which is due to the fact that both the key exchange and signature processes are based on post-quantum algorithms. The hybrid model showed a result of 70 ms, i.e., the parallel operation of the classical and PQC mechanisms moderately increased the system load. The scientific conclusion is that post-quantum algorithms require significant computational costs, especially at the connection establishment stage. However, this increase does not have a



critical negative impact on the performance of the system.

Figure 3. JWT signing time

The results show the real-world systemic implications of implementing post-quantum cryptography in modern AI-based microservice infrastructures. First, the handshake phase at the transport layer is found to be the most sensitive point. Since the key exchange at this stage requires mathematically complex operations, post-quantum algorithms take longer than classical options. Second, although the digital signature process has an impact on API response time, it is a small fraction of the total transaction time.

Conclusion.

The results of the study confirm that the implementation of post-quantum cryptography algorithms in the microservice API infrastructure based on artificial intelligence is practically feasible and can be implemented while maintaining system stability. Post-quantum key exchange requires significant additional time at the transport layer, but the overall API response latency remains within the limits consistent with the service level requirements. Post-quantum variants of digital signature mechanisms slow down the authentication process, but this does not have a significant negative impact on the overall performance of the system. A fully post-quantum architecture provides maximum quantum stability, but there is a

decrease in performance. A hybrid model provides the optimal balance between security and performance and is recommended as an acceptable solution for a gradual transition in real infrastructures. Thus, in the context of the development of quantum computing technologies, adapting the API infrastructure to post-quantum algorithms is a strategic necessity, and this process requires systematic optimization and a scientifically sound approach

List of used literature:

1.Nair A., Nicolazzo S., Nocera A., R. R. R. K. A., V. P. Sok: Zero Trust as a Strategy to Address DevSecOps Challenges // Proceedings of the 2025 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). – 2025. – P. 546–554. – DOI: 10.1109/EuroSPW67616.2025.00069.

2.Montenegro J. A., Rios R., Lopez-Cerezo J. A performance evaluation framework for post-quantum TLS // Future Generation Computer Systems. – 2026. – Vol. 175. – Art. 108062. – DOI: 10.1016/j.future.2025.108062.

3.Astrizi T. L., Custódio R. Seamless transition to post-quantum TLS 1.3: A hybrid approach using identity-based encryption // Sensors. – 2024. – Vol. 24, No. 22. – Art. 7300. – DOI: 10.3390/s24227300.

4.Zhang Z., Zhao Y. Enhanced elliptic curve cryptography (EECC) // Procedia Computer Science. – 2024. – Vol. 247. – P. 1324–1330. – DOI: 10.1016/j.procs.2024.10.158.