OpenSSL-Based Hybrid Quantum-Resistant TLS 1.3: Strengthening Cybersecurity Against Quantum Attacks

Suleiman Ahmed Danasabe [1] & Abdulhamid Ibrahim Garba[2]
[1]Department of Computer Engineering, Federal Polytechnic Ilaro, Ogun, Nigeria
[2]Department of Electrical Electronics Engineering, Federal Polytechnic Ilaro, Ogun,
*Corresponding author email:ahmed.suleiman@federalpolyilaro.edu.ng

Introduction
Research analyses cryptography and cybersecurity relationships mainly through the lens of modern cryptographic algorithm changes generated by emerging quantum computing systems. The main framework of cryptography includes complex mathematical models specifically utilizing public-key cryptography (PKC) that needs asymmetric key pairs (public key and private key) for encryption and decryption procedures. The current PKC infrastructure functions on the assumption that large prime number multiplication remains efficient but factorisation steps remain impossible for standard computing machines. Quantum computing poses a challenge to this cryptographic assumption because it executes complex computational operations at considerably accelerated speeds when compared to conventional computers. Quantum computers that achieve maturity will lead to the breach of current PKC encryption methods thus creating severe cybersecurity risks. The current situation demands implementing quantum-resistant cryptography because it ensures protection of sensitive information. The U.S. National Institute of Standards and Technology (NIST) has started its effort to standardize algorithms from the next-generation post-quantum cryptography (PQC). The cryptographic algorithms CRYSTALS-Kyber gained selection as the primary key encapsulation mechanism option alongside CRYSTALS-Dilithium securing the digital signature algorithm position. A complete security solution for communication systems requires the unification of cryptographic techniques that utilize classical as well as PQ along with QKD methods to combat potential security risks.The research analyses key matters about TCP data transmission security which will become more fragile with the growing presence of quantum computing systems. Thisstudy demonstrates how classical cryptographic algorithms become weak against quantum attacks including DNDL. The study evaluates encryption and decryption impact on file size expansion as well as the connection delays necessary for client-server authentication key exchanges.

Methodology
The proposed cryptographic scheme incorporates three sets of algorithms called classical and post-quantum and QKD which work together as a hybrid system. The system uses OpenSSL libraries with TLS 1.3 to provide secure file transfer through sFTP. Security gets boosted through the hybrid key exchange method since it unifies multiple cryptographic secrets into one key that defends against quantum attacks. The model was developed to optimize several elements: agile integration of future encryption advancements and it delivers fast secure server-client data exchange and will preserve confidentiality over time including the possibility of quantum computing breakthroughs.

Results and discussion
Simulation results proved that the hybrid method can successful secure authentication through TLS with an improved file transfer security over encrypted channel. however, it also serves as protection against DNDL attacks and when benchmarked with other techniques such as FTPS (TLS 1.2/1.3), sFTP (SSH-2), HTTPS (TLS 1.3), Post-Quantum FTPS (Kyber +TLS 1.3) over performance its variants relative to security against quantum threats.

Conclusions
Although TLS secures file transfers, it has security flaws such as MTM attacks, quantum threats, and traffic analysis problems. Secure FTP requires hybrid model optimisation and post-quantum cryptography technologies. Future research will concentrate on high-volume systems, and businesses must choose protocols that strike a balance between security and performance.

Keywords: Quantum computers, cryptography, Transport Layer Security (TLS), OpenSSL Library