INTISARI

Ancaman yang meningkat dari komputer kuantum terhadap keamanan kriptografi klasik mendorong pengembangan algoritma post-quantum untuk melindungi data di masa depan. Penelitian ini bertujuan untuk mengimplementasikan keamanan menggunakan algoritma kriptografi post-quantum Kyber768 pada protokol TLS 1.3. Implementasi dilakukan menggunakan server dan client yang dikonfigurasi di lingkungan AWS dengan memanfaatkan OpenSSL 3.2.3 untuk menghasilkan kunci dan sertifikat hybrid antara kriptografi klasik dan post-quantum. Proses penelitian melibatkan pengumpulan informasi terkait kebutuhan sistem, penyiapan lingkungan OpenSSL, pembuatan kunci dan sertifikat, serta konfigurasi TLS 1.3 pada server Nginx. Namun, hasil implementasi menunjukkan bahwa integrasi algoritma Kyber768 dengan Nginx tidak berhasil. Hambatan teknis ini disebabkan oleh ketidaksesuaian dukungan antara OpenSSL, Nginx, dan algoritma Kyber768 dalam lingkungan server yang digunakan. Penelitian ini memberikan wawasan penting tentang tantangan dan keterbatasan dalam menerapkan algoritma post-quantum pada protokol komunikasi modern. Hal ini diharapkan dapat menjadi dasar untuk pengembangan solusi lebih lanjut dalam menghadapi ancaman keamanan di era komputasi kuantum.

Kata kunci: *Post-Quantum Cryptography* (PQC), *Transport Layer Security* (TLS), *Kyber768*

ABSTRACT

The increasing threat of quantum computers to classical cryptographic security encourages the development of post-quantum algorithms to protect data in the future. This research aims to implement security using the Kyber768 post-quantum cryptography algorithm on the TLS 1.3 protocol. The implementation is done using servers and clients configured in the AWS environment by utilizing OpenSSL 3.2.3 to generate hybrid keys and certificates between classical and post-quantum cryptography. The research process involved gathering information related to system requirements, setting up the OpenSSL environment, generating keys and certificates, and configuring TLS 1.3 on the Nginx server. However, the implementation results showed that the integration of the Kyber768 algorithm with Nginx was not successful. This technical barrier was caused by the incompatibility of support between OpenSSL, Nginx, and the Kyber768 algorithm in the server environment used. This research provides important insights into the challenges and limitations of applying post-quantum algorithms to modern communication protocols. It is expected to serve as a basis for further development of solutions to deal with security threats in the era of quantum computing.

Keywords: Post-Quantum Cryptography (PQC), Transport Layer Security (TLS), Kyber768