ABSTRAK

Penggunaan kata sandi tunggal semakin tidak memadai dalam menghadapi ancaman serangan identitas digital, sehingga penerapan *Two-Factor Authentication* (2FA) berbasis *Time-based One Time Password* (TOTP) menjadi standar keamanan yang krusial. Namun, efektivitas sistem TOTP saat ini terhalang oleh penggunaan standar lama HMAC-SHA-2 (seperti HMAC-SHA-256 dan HMAC-SHA-512) yang memanfaatkan arsitektur Merkle-Damgård. Arsitektur ini memerlukan pemrosesan fungsi *hash* secara ganda (*nested double-pass*) untuk mencegah serangan *length-extension*, sehingga menimbulkan beban komputasi yang tinggi dan penggunaan memori yang kurang efisien. Penelitian ini bertujuan untuk menganalisis, membandingkan, serta mengevaluasi performa dan tingkat keamanan algoritma HMAC-SHA-2 dengan algoritma KMAC-SHA-3 (KMACXOF128 dan KMACXOF256 berbasis *Sponge Construction* / KECCAK) dalam implementasi TOTP 2FA. Pengujian dilakukan menggunakan pendekatan eksperimental dan analisis matematis. Aspek performa diuji meliputi kecepatan *generate* dan verifikasi kode TOTP (pada skenario 1.000 *secret key* dan 1.000.000 total eksekusi), penggunaan sumber daya (CPU dan RAM), serta *throughput* dan *multi-thread*. Aspek keamanan dievaluasi melalui uji *avalanche effect*, keacakan (*randomness* menggunakan NIST *Statistical Test Suite*), serta analisis matematis pada *collision resistance, preimage resistance, dan second-preimage resistance*. Hasil analisis dan perbandingan ini diharapkan dapat memberikan referensi akademis serta panduan teknis bagi pengembang sistem keamanan digital dalam melakukan transformasi dan migrasi standar dari HMAC ke KMAC pada skema TOTP masa depan.

Kata Kunci: TOTP, 2FA, HMAC-SHA-2, KMAC-SHA-3, Performa dan Keamanan Kriptografi.

ABSTRACT

The rely on single passwords has become increasingly inadequate in mitigating digital identity threats, making the implementation of Time-based One Time Password (TOTP) within Two-Factor Authentication (2FA) a critical security standard. However, the current effectiveness of TOTP systems is constrained by the legacy standard HMAC-SHA-2 (such as HMAC-SHA-256 and HMAC-SHA-512), which relies on the Merkle-Damgård architecture. This architecture requires a nested double-pass hash execution to prevent length-extension attacks, resulting in high computational overhead and inefficient memory utilization. This study aims to analyze, compare, and evaluate the performance and security strength of HMAC-SHA-2 algorithms against KMAC-SHA-3 algorithms (KMACXOF128 and KMACXOF256 based on Keccak Sponge Construction) in TOTP-2FA implementations. The evaluation was conducted using an experimental approach combined with mathematical analysis. Performance metrics included TOTP code generation and verification latency (tested across 1,000 secret keys and 1,000,000 total executions), resource usage (CPU and RAM), as well as throughput and multi-threading capabilities. Security properties were assessed via avalanche effect testing, bit randomness (using the NIST Statistical Test Suite), and mathematical analysis of collision resistance, preimage resistance, and second-preimage resistance. The comparative findings provide academic reference and technical guidance for digital security developers transitioning from legacy HMAC to modern KMAC standards in future TOTP authentication systems.

Keywords: *TOTP, 2FA, HMAC-SHA-2, KMAC-SHA-3, Cryptographic Performance and Security.*