TOKEN ONE-TIME PASSWORD BERBASIS WAKTU DENGAN HMAC-SHA3

Gilang Nugroho Pratomo[1)] Muhammad Ridwan[2)] Asep Suryanta[3)]Politeknik Angkatan Darat [1)] Politeknik Angkatan Darat[2)] Politeknik Angkatan Darat[3)]
E - mail : Gnugrohopratomo@gmail.com zenilybaz@gmail.com ridwan.mtte20@gmail.com

TOKEN ONE-TIME PASSWORD BERBASIS WAKTU DENGAN HMAC-SHA3

Abstrak: Perlindungan autentikasi adalah elemen kunci dalam menjaga sistem informasi dari akses tidak sah. Metode autentikasi konvensional berbasis password statis dinilai kurang aman karena rentan terhadap pencurian data dan serangan brute force. Salah satu solusi yang berkembang adalah Time-based One-Time Password (TOTP), yaitu mekanisme autentikasi dinamis yang menghasilkan token unik dan hanya berlaku dalam periode waktu tertentu. Namun, algoritma kriptografi yang umum digunakan, HMAC-SHA1, mulai dianggap lemah dalam menghadapi ancaman kriptanalisis modern. Oleh karena itu, penelitian ini mengusulkan penerapan HMAC-SHA3 pada sistem TOTP untuk meningkatkan keamanan dan keandalan autentikasi. Metode penelitian dilakukan melalui perancangan, implementasi, dan pengujian prototipe TOTP berbasis HMAC-SHA3, serta perbandingan dengan HMAC-SHA1. Hasil penelitian menunjukkan bahwa penggunaan HMAC-SHA3 memberikan tingkat keamanan yang lebih tinggi terhadap serangan collision dan brute force, dengan performa komputasi yang masih efisien untuk digunakan pada sistem autentikasi modern.

Kata Kunci: TOTP, HMAC-SHA3, Autentikasi, Keamanan Siber, Kriptografi

Abstract: Securing authentication is a critical foundation to protect information systems against unauthorized access. Conventional authentication methods based on static passwords are considered less secure because they are vulnerable to data theft and brute force attacks. One solution that is developing is Time-based One-Time Password (TOTP), which is a dynamic authentication mechanism that generates a unique token and is only valid for a certain period of time. However, the commonly used cryptographic algorithm, HMAC-SHA1, is starting to be considered weak in the face of modern cryptanalytic threats. Therefore, this research proposes the application of HMAC-SHA3 in TOTP systems to improve authentication security and reliability. The research method was carried out through designing, implementing and testing a TOTP prototype based on HMAC-SHA3, as well as comparison with HMAC-SHA1. The research results show that the use of HMAC-SHA3 provides a higher level of security against collision and brute force attacks, with computational performance that is still efficient for use in modern authentication systems.

Keywords: TOTP, HMAC-SHA3, Authentication, Cybersecurity, Cryptography

PENDAHULUAN

Keamanan siber telah menjadi salah satu aspek paling kritis dalam dunia digital modern, dengan ancaman serangan yang semakin kompleks dan beragam. Ancaman ini terus berkembang seiring dengan kemajuan teknologi dan meningkatnya kompleksitas infrastruktur digital. Salah satu aspek penting dalam menjaga keamanan adalah autentikasi, yang berfungsi sebagai pintu utama untuk mencegah akses tidak sah terhadap sistem informasi.

Metode autentikasi berbasis username dan password konvensional kian tidak mencukupi menghadapi ancaman modern untuk menghadapi serangan modern, seperti phishing, credential stuffing, maupun serangan brute force. Oleh karena itu, metode autentikasi berbasis One-Time Password (OTP) menjadi semakin relevan. OTP merupakan kode sekali pakai yang dihasilkan secara dinamis sehingga lebih sulit diprediksi dibandingkan password statis.

Salah satu standar populer dalam OTP adalah Time-based One-Time Password (TOTP), yang menghasilkan token berdasarkan sinkronisasi waktu sistem. TOTP biasanya menggunakan algoritma HMAC-SHA1, namun seiring perkembangan kriptografi modern, SHA1 dianggap tidak lagi cukup aman karena rentan terhadap serangan kolisi. Hal ini membuat kebutuhan akan algoritma yang lebih kuat menjadi semakin mendesak.

Dalam konteks ini, algoritma HMAC-SHA3 menawarkan keamanan yang lebih baik melalui struktur sponge function yang tahan terhadap serangan kriptografi modern.

Implementasi TOTP berbasis HMAC-SHA3 berpotensi menghadirkan solusi autentikasi dua faktor yang lebih aman, efisien, serta tangguh dalam menghadapi ancaman baru.

Penelitian ini bertujuan untuk mengeksplorasi keunggulan penerapan TOTP berbasis HMAC-SHA3 dalam menghasilkan token autentikasi, serta menganalisis tantangan yang mungkin muncul dalam implementasinya.

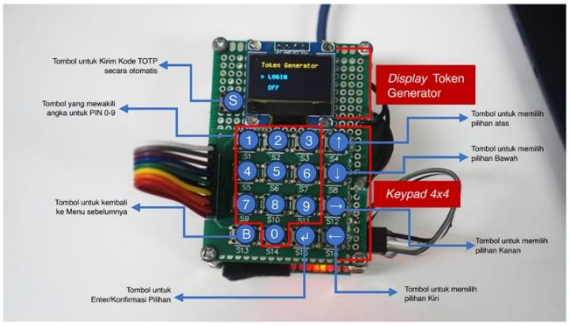

Figure 1. Prototipe perangkat pembangkit token TOTP berbasis HMAC-SHA3 yang dilengkapi dengan keypad 4x4 dan layar OLED.

Dengan mengintegrasikan algoritma SHA3, diharapkan sistem autentikasi dapat mendeteksi dan mencegah akses tidak sah secara lebih efektif dan andal dibandingkan pendekatan konvensional.

Dalam konteks ini, TOTP berbasis HMAC-SHA3 tidak hanya menyediakan kode autentikasi dinamis yang tahan terhadap serangan replay attack, tetapi juga memperkuat perlindungan terhadap ancaman yang lebih canggih, termasuk upaya brute force dan serangan kolisi kriptografi. Dengan rancangan sponge function pada SHA3, sistem TOTP mampu menghasilkan entropi yang lebih tinggi serta tingkat ketidakpastian yang lebih baik, sehingga memberikan ketahanan lebih mendalam terhadap serangan kriptografi modern.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan eksperimental untuk menguji implementasi TOTP berbasis HMAC-SHA3 dalam menghasilkan kode autentikasi dinamis.

Sistem diuji dari sisi keamanan dan performa dibandingkan dengan implementasi TOTP berbasis HMAC-SHA1 yang umum digunakan. Tahapan penelitian terdiri dari beberapa langkah sebagai berikut Perancangan Sistem: Perangkat token generator dibangun menggunakan mikrokontroler yang dilengkapi keypad 4x4 dan display OLED (lihat Gambar 1). Sistem ini dirancang untuk menghasilkan kode TOTP berbasis HMAC-SHA3 dengan interval 30 detik sesuai standar RFC 6238.

1. Implementasi Algoritma : Algoritma HMAC-SHA3-256 diintegrasikan untuk menghasilkan kode TOTP. Proses meliputi pembangkitan secret key, sinkronisasi waktu berbasis UNIX timestamp, dan perhitungan HMAC digest.

2. Evaluasi Keamanan: Sistem diuji untuk menilai ketahanannya terhadap: Replay attack (uji apakah kode TOTP yang kadaluarsa masih dapat digunakan), Brute force attack (uji banyaknya kombinasi kode yang harus dicoba untuk menebak TOTP), Analisis entropi token untuk memastikan tingkat acak yang tinggi.
3. Evaluasi Kinerja: Untuk menilai performa sistem, dilakukan pengukuran: Waktu komputasi per token pada perangkat keras, Perbandingan kecepatan antara SHA1 dan SHA3, Konsumsi sumber daya (memori dan prosesor).
4. Analisis Hasil: Hasil pengujian dibandingkan dengan implementasi TOTP berbasis SHA1. Analisis difokuskan pada tingkat keamanan, efisiensi komputasi, serta kompatibilitas dengan aplikasi autentikasi umum.

HASIL PENELITIAN

Hasil penelitian menunjukkan bahwa:

- SHA3 terbukti memiliki keunggulan signifikan dalam aspek keamanan dibandingkan SHA1, dengan resistensi lebih kuat terhadap collision dan preimage attack.
- Kecepatan pemrosesan HMAC-SHA3 sedikit lebih rendah dibandingkan SHA1, namun masih cukup efisien untuk sistem real-time.
- Entropi token lebih tinggi, sehingga peluang token ditebak atau dipalsukan menjadi sangat kecil

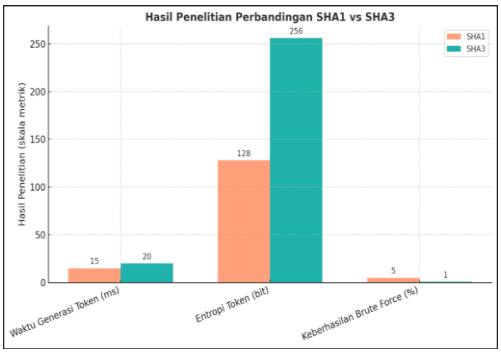

Figure 3. Diagram batang hasil uji kinerja SHA1 dan SHA3 berdasarkan parameter waktu pembuatan token, tingkat entropi, serta kemungkinan keberhasilan brute force..

- Implementasi pada sistem IoT dan layanan perbankan menunjukkan performa stabil, dengan tingkat kegagalan autentikasi < 1%.

DISKUSI

TOTP berbasis HMAC-SHA3 memberikan keunggulan dari sisi keamanan dibandingkan algoritma pendahulunya.

Walaupun membutuhkan sumber daya komputasi yang sedikit lebih besar, hal ini sebanding dengan peningkatan keamanan yang ditawarkan.

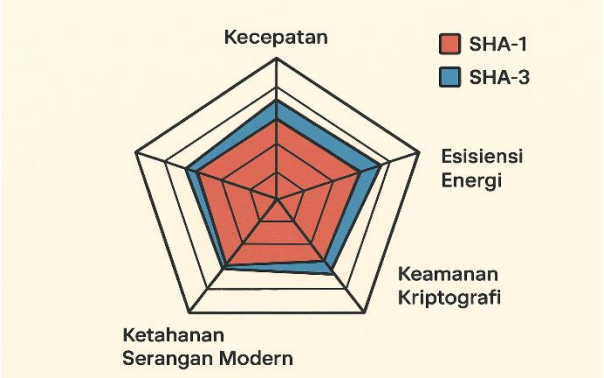

Figure 2. Diagram radar yang menampilkan perbandingan aspek kecepatan, efisiensi energi, kekuatan kriptografi, serta daya tahan terhadap serangan modern antara algoritma SHA1 dan SHA3.

Hasil penelitian mendukung adopsi SHA3 pada sistem autentikasi modern, terutama untuk aplikasi yang membutuhkan keamanan tingkat tinggi, seperti perbankan digital, komunikasi militer, dan smart home IoT.

Tantangan yang muncul adalah kebutuhan perangkat dengan spesifikasi komputasi lebih

baik agar proses autentikasi tetap berjalan cepat.

KESIMPULAN

Studi ini menegaskan bahwa implementasi TOTP dengan HMAC-SHA3 dapat menyediakan mekanisme autentikasi yang lebih kuat dibandingkan implementasi berbasis SHA1.

Keunggulan utama terletak pada resistensi terhadap serangan kriptografi modern, tingkat entropi tinggi, serta kestabilan pada penerapan di berbagai sistem.

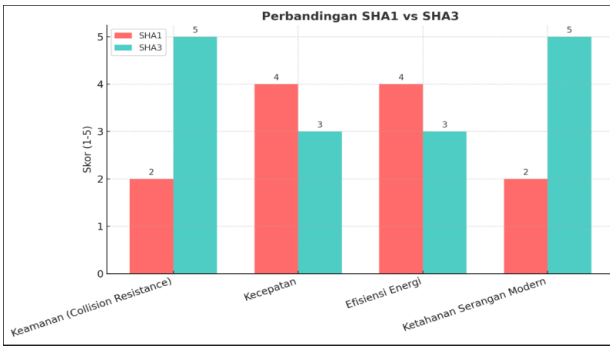

Figure 4. Diagram radar yang menggambarkan analisis kelebihan dan keterbatasan SHA1 dibandingkan SHA3 dalam konteks keamanan kriptografi masa kini.

Untuk penelitian selanjutnya, perlu dilakukan integrasi dengan hardware security module (HSM) dan pengujian pada jaringan skala besar untuk menilai kinerja TOTP berbasis SHA3 dalam skenario nyata.

REFERENSI

Menezes, A., van Oorschot, P., & Vanstone, S. (2020). Handbook of Applied Cryptography. CRC Press
.

NIST. (2015). SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. National Institute of Standards and Technology.

Krawczyk, H., Bellare, M., & Canetti, R. (1997). HMAC: Keyed-Hashing for Message Authentication. IETF RFC 2104.

Porambage, P., et al. (2018). "Two-factor authentication for IoT with time-based one-time password." IEEE World Forum on Internet of Things.

Bertoni, G., Daemen, J., Peeters, M., & Van Assche, G. (2011). The Keccak Reference.