EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647 (Online)
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i1.1782

Otentikasi Dua Faktor Menggunakan TOTP dengan SHA-512 untuk Sistem Pemilihan Presiden Mahasiswa

Diki Arisandi[1], Seri Hartati[2*], Givo Vrabora[3]

[1] Program Studi Bisnis Digital, Fakultas Ekonomi dan Bisnis, Universitas Muhammadiyah Riau, Pekanbaru-Indonesia.
[2] Program Studi Pendidikan Informatika, Fakultas Keguruan dan Ilmu Pendidikan, Universitas Muhammadiyah Riau, Pekanbaru-Indonesia.
[3] Program Studi Teknik Informatika, Fakultas Teknik, Universitas Abdurrab, Pekanbaru-Indonesia.
[1]dikiarisandi@umri.ac.id, [2*]serihartati@umri.ac.id, [3]givo.vrabora@student.univrab.ac.id
[*)] serihartati@umri.ac.id

Abstrak−Penelitian ini berawal dari kebutuhan akan sistem pemilihan yang aman di lingkungan akademis, khususnya dalam menghadapi ancaman pencurian kredensial dan serangan siber pada sistem keamanan pemilihan Presiden Mahasiswa. Keamanan pada sistem pemilihan mahasiswa menjadi tantangan utama, mengingat metode autentikasi konvensional rentan terhadap kejadian manipulasi keaslian identitas pemilih. Oleh karena itu, penelitian ini mengusulkan model autentikasi dua faktor menggunakan *Time-Based One-Time Password* (TOTP) berbasis algoritma SHA-512. Model ini menambahkan lapisan keamanan tambahan berupa autentikasi berbasis waktu dan hash yang lebih kuat terhadap serangan. Pengujian dilakukan dengan melibatkan beberapa akun pengguna dari aplikasi Gmail, di mana kode OTP berhasil dikirimkan ke akun email pengguna. Hasil pengujian menunjukkan bahwa waktu pengiriman dan validasi TOTP berkisar antara 150 hingga 300 ms, dengan tingkat kepuasan pengguna lebih dari 80%. Implikasi penelitian ini mencakup peningkatan keamanan pada sistem pemilihan Presiden Mahasiswa di lingkungan akademis serta potensi adopsi yang lebih luas di bidang lainnya yang membutuhkan autentikasi pengguna.

Kata Kunci: Presiden Mahasiswa, TOTP, SHA-512, Otentikasi, Hash

Abstract−This study originated from the need for a secure election system in academic environments, particularly to address credential theft and cyberattack threats in the security of the Student Presidential election system. Ensuring security in student election systems presents a significant challenge, as conventional authentication methods are prone to voter identity authenticity manipulation. Therefore, this research proposes a two-factor authentication model using Time-Based One-Time Password (TOTP) based on the SHA-512 algorithm. This model provides an additional layer of security through time-based authentication and a stronger hash mechanism against attacks. Testing was conducted involving several user accounts from Gmail applications, where OTP codes were successfully sent to the users' email accounts. The results indicated that TOTP delivery and validation times ranged between 150 and 300 ms, with user satisfaction levels exceeding 80%. The implications of this study include enhanced security in the student presidential election system within academic environments and the potential for broader adoption in other fields requiring user authentication.

Keywords: Student Council, TOTP, SHA-512, Authentication, Hash

1. PENDAHULUAN

Pada era digital saat ini, otentikasi secara elektronik sudah menjadi hal yang sangat umum ditemui. Mulai dari penggunaan kata sandi untuk akses media sosial, *e-mail*, dokumen, dan lain sebagainya. Otentikasi elektronik memungkinkan identitas digital pengguna diverifikasi secara akurat dan memberikan jaminan keaslian yang lebih baik [1]. Metode otentikasi elektronik terus berkembang seiring perkembangan teknologi, mulai dari OTP, *captcha*, hingga *blockchain* [2]. Penggunaan otentikasi elektronik di era digital saat ini memiliki banyak manfaat seperti menjaga keamanan data pribadi [3], mencegah pencurian identitas [4], dan memudahkan transaksi daring [5].

Ada banyak implementasi dari otentikasi pengguna secara digital, salah satunya adalah saat pemilihan presiden mahasiswa pada suatu universitas atau institusi pendidikan tinggi. Presiden mahasiswa adalah mahasiswa yang terpilih menjadi pemimpin organisasi kemahasiswaan di suatu perguruan tinggi [6]. Dalam era perkembangan teknologi digital yang terus berlanjut, keamanan sistem pemilihan presiden mahasiswa menjadi aspek yang sangat penting dan membutuhkan perhatian serius. Tantangan utama yang dihadapi adalah bagaimana mengamankan proses otentikasi untuk memastikan bahwa setiap suara yang diberikan berasal dari pemilih yang sah. Dengan meningkatnya ancaman keamanan siber dan potensi serangan terhadap sistem pemilihan, metode otentikasi satu

arah atau konvensional sudah tidak lagi menjamin otentikasi pengguna. Oleh karena itu, pentingnya mengembangkan model otentikasi dua faktor menjadi semakin relevan, karena model ini mampu memberikan lapisan keamanan tambahan dengan memerlukan dua tahap verifikasi yang berbeda untuk memastikan identitas pemilih.

Fokus utama penelitian ini adalah pada pengembangan model otentikasi dua faktor yang memanfaatkan *Time-based One-Time Password* (TOTP) dengan menggunakan algoritma SHA (secure hash algorithm) yaitu SHA-512. TOTP memberikan keamanan tambahan dengan memasukkan unsur waktu dalam proses otentikasi [7], sedangkan penggunaan SHA-512 sebagai algoritma hash menawarkan keamanan tambahan sebagai penguat otentikasi [8]. Beberapa masalah yang ingin diatasi mencakup potensi serangan pencurian kredensial, penggunaan akun palsu, dan keamanan umum dalam sistem pemilihan presiden mahasiswa. Penelitian ini bertujuan untuk memberikan solusi yang efektif dalam memitigasi risiko-risiko tersebut, sehingga dapat menciptakan dasar yang kuat untuk menjaga kontinuitas demokrasi di lingkungan akademis. Pendekatan yang diambil dalam penelitian ini tidak hanya memperhatikan aspek keamanan semata, tetapi juga menekankan pentingnya menjaga integritas dan keaslian setiap suara dalam proses demokratisasi mahasiswa.

Beberapa penelitian terkait membahas pemanfaatan metode otentikasi dengan algoritma SHA, termasuk karya dari Semesta dan Amini. Fokus penelitian ini muncul dari masalah dalam sistem otentikasi pada website SMK Karya Bangsa yang saat ini hanya menggunakan password statis, sehingga rentan terhadap serangan *sniffing* yang berpotensi mencuri identitas pengguna. Metode yang digunakan dalam penelitian ini adalah *prototype*, dengan mengimplementasikan sistem otentikasi dua faktor menggunakan OTP (*One-Time Password*) berbasis waktu dengan algoritma SHA-512 yang dikirim melalui SMS. Hasilnya berupa *prototype* sistem otentikasi dua faktor untuk login website SMK Karya Bangsa, yang mengirimkan kode OTP melalui SMS. Pengujian menunjukkan bahwa *prototype* ini dapat meningkatkan keamanan dibandingkan dengan penggunaan hanya password statis, serta efektif dalam mencegah pencurian identitas pengguna melalui serangan *sniffing* [9]. Di sisi lain, penelitian Fitriyansyah dan Hazri juga berfokus pada masalah keamanan *web login* mahasiswa yang mengandalkan *password* statis, memerlukan sistem otentikasi yang lebih aman. Metode penelitian melibatkan analisis kebutuhan, perancangan sistem, dan implementasi otentikasi dua faktor dengan OTP menggunakan algoritma HMAC dan SHA-256. Hasilnya adalah *prototype* sistem otentikasi dua faktor untuk *web login* mahasiswa, menggabungkan password dan TOTP berbasis waktu yang dikirim lewat SMS. *Prototype* ini berhasil meningkatkan keamanan *web login* mahasiswa dibandingkan hanya menggunakan *password* statis [10].

Penelitian oleh Hayat dan rekan-rekannya juga mengulas penggunaan algoritma SHA dalam konteks serupa. Mereka memfokuskan penelitian pada keamanan *login website* yang rentan terhadap serangan *sniffing* dan pencurian identitas pengguna. Metode yang diterapkan dalam penelitian ini mencakup perancangan dan implementasi sistem otentikasi dua faktor dengan TOTP menggunakan algoritma SHA-256. Hasil dari penelitian ini adalah sebuah website untuk top up *voucher game* yang menerapkan otentikasi TOTP. Pengujian menunjukkan bahwa penerapan TOTP pada website dapat meningkatkan keamanan login dengan membatasi waktu validasi kode OTP yang dikirim melalui email dan WhatsApp pengguna [11]. Penelitian oleh Hapsari dan kolega juga menyoroti kepentingan otentikasi dua faktor. Mereka mengatasi masalah keamanan login pada sistem pemesanan *online* yang hanya mengandalkan *password* statis dan rentan terhadap serangan pencurian identitas. Metodenya melibatkan perancangan dan implementasi sistem otentikasi dua faktor dengan TOTP dan SHA-256, menghasilkan sebuah sistem pemesanan online makanan yang menggunakan OTP untuk login. Pengujian menunjukkan bahwa penggunaan OTP yang dikirim melalui email dapat meningkatkan keamanan login dengan membatasi waktu validasi OTP [12]. Di sisi lain, penelitian oleh Sari dan Abdillah juga membicarakan penggunaan TOTP untuk otentikasi. Mereka mengatasi permasalahan pada sistem absensi mahasiswa berbasis QR *code* yang rentan terhadap kecurangan. Untuk mengatasinya, penelitian ini menggunakan metode otentikasi tambahan berupa TOTP yang dikirimkan melalui QR code dan hanya berlaku dalam waktu singkat. Hasilnya menunjukkan bahwa metode ini dapat mengurangi kemungkinan kecurangan karena password selalu berubah setiap waktu tertentu, menghalangi mahasiswa untuk mengirimkan foto QR code yang statis kepada mahasiswa lain [13].

Penelitian sebelumnya telah membuktikan efektivitas autentikasi dua faktor dalam meningkatkan keamanan sistem dibandingkan dengan metode autentikasi satu faktor. Sebagai contoh, penggunaan algoritma SHA-256 dalam kombinasi dengan TOTP mampu menghasilkan kode verifikasi yang unik dan sulit untuk diretas. Selain itu, pendekatan berbasis prototipe yang mengintegrasikan autentikasi dua faktor menunjukkan keandalan dalam berbagai skenario, termasuk pada kondisi jaringan yang tidak stabil. Kelebihan lain dari metode ini adalah fleksibilitasnya dalam mengadopsi teknologi baru untuk mengatasi tantangan keamanan yang terus berkembang.

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647 (Online)
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i1.1782

Penelitian ini memanfaatkan fondasi tersebut dengan meningkatkan algoritma menjadi SHA-512, yang menawarkan hash lebih panjang dan tahan terhadap serangan brute force maupun serangan lainnya.

Penelitian ini berfokus pada pengembangan model otentikasi dua faktor dengan TOTP menggunakan algoritma SHA-512 untuk sistem pemilihan presiden mahasiswa, yang dapat memberikan kontribusi terhadap keamanan pemilihan Presiden Mahasiswa secara demokratis seerta menanggapi permasalahan terkait keamanan di lingkungan akademis. Perbedaan dengan hasil penelitian sebelumnya dapat dilihat pada konteks aplikatif. Pada penelitian sebelumnya lebih menitikberatkan pada pengembangan otentikasi dua faktor untuk website dan pemesanan online, penelitian ini secara spesifik mengadaptasi konsep keamanan ke dalam sistem pemilihan presiden mahasiswa. Selain itu, penggunaan TOTP dan algoritma *hash* SHA-512 memberikan tambahan terhadap keamanan dan otentikasi pengguna yang lebih kuat. Dengan demikian, penelitian ini dapat mengisi *gap* pengetahuan dalam hal keamanan pemilihan mahasiswa yang dilaksanakan secara *online* dengan pendekatan yang berfokus pada kebutuhan khusus lingkungan akademis.

Tujuan dari penelitian ini adalah mengembangkan model otentikasi dua faktor dengan TOTP menggunakan algoritma SHA-512 untuk sistem pemilihan presiden mahasiswa. Dengan demikian, penelitian ini bertujuan memberikan kontribusi positif terhadap keamanan pemilihan presiden mahasiswa secara demokratis di lingkungan akademis. Harapannya, penelitian ini dapat mengatasi tantangan utama dalam mengamankan proses otentikasi, memastikan setiap suara berasal dari pemilih yang sah, dan merespons ancaman keamanan siber serta potensi serangan terhadap sistem pemilihan. Selain itu, penelitian ini diharapkan dapat memberikan solusi efektif untuk mitigasi risiko seperti serangan pencurian akun, penggunaan akun palsu, dan meningkatkan keamanan dalam sistem pemilihan presiden mahasiswa. Dengan pendekatan yang berfokus pada kebutuhan lingkungan akademis, diharapkan penelitian ini dapat menciptakan dasar untuk menjaga keberlanjutan demokrasi di lingkungan akademis, menekankan pentingnya integritas dan keaslian setiap suara dalam proses demokratisasi mahasiswa.

2. METODE PENELITIAN

2.1 Tahapan Penelitian

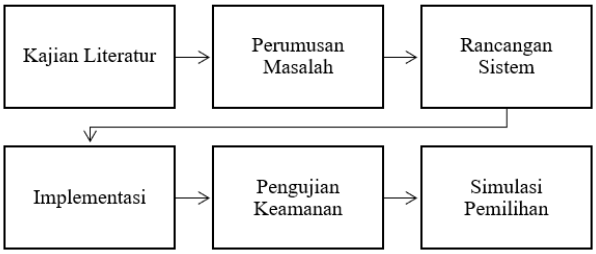
Dalam penelitian ini, digunakan serangkaian langkah penelitian yang secara sistematis menggambarkan, mendeskripsikan, dan menjelaskan penerapan SHA-512 dengan TOTP serta komponen-komponennya. Proses ini difokuskan pada pembangunan suatu sistem yang relevan untuk pemilihan presiden mahasiswa. Berikut adalah tahapan-tahapan yang dilakukan, mengacu pada diagram yang tergambar pada gambar 1.

Berdasarkan gambar 1, berikut uraian dari tahapan kerja yang dilakukan dalam penelitian ini:

1. Kajian Literatur
   Dalam tahap kajian literatur, penelitian ini secara mendalam mengeksplorasi literatur yang terkait dengan otentikasi dua faktor, TOTP, dan algoritma SHA-512. Analisis juga dilakukan terhadap implementasi serupa dan hasil penelitian sebelumnya untuk memahami kerangka kerja dan temuan yang telah ada dalam domain keamanan sistem.
2. Perumusan Masalah
   Perumusan masalah dilakukan dengan mengidentifikasi tantangan dan kekurangan yang ada dalam keamanan sistem pemilihan presiden mahasiswa. Tantangan tersebut menjadi titik fokus untuk dirumuskan dalam bentuk masalah yang dapat diatasi melalui implementasi otentikasi dua faktor menggunakan TOTP dengan menggunakan algoritma SHA-512.
3. Rancangan Sistem
   Tahap rancangan sistem melibatkan perancangan arsitektur sistem pemilihan presiden mahasiswa yang memadukan otentikasi dua faktor. Rincian desain penggunaan TOTP dan penerapan algoritma SHA-512 menjadi elemen kunci dalam menghasilkan solusi keamanan yang kokoh dan efektif.
4. Implementasi
   Dalam implementasi, fokus utama adalah pembuatan prototipe sistem yang telah dirancang, dengan integrasi otentikasi dua faktor menggunakan TOTP. Selain itu, algoritma SHA-512 diimplementasikan untuk menghasilkan dan memverifikasi TOTP, memberikan landasan teknis bagi keamanan sistem secara keseluruhan.
5. Pengujian Keamanan
   Pengujian keamanan menjadi langkah kritis dalam mengevaluasi sistem. Proses ini melibatkan identifikasi potensi celah keamanan, uji ketahanan terhadap serangan otentikasi, dan penilaian keamanan algoritma SHA-512. Hasil pengujian memberikan wawasan yang mendalam terkait kekuatan dan kelemahan sistem.

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647 (Online)
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i1.1782

6. Simulasi Pemilihan
   Simulasi pemilihan presiden mahasiswa menjadi uji coba praktis dari implementasi otentikasi dua faktor menggunakan TOTP. Pengumpulan data hasil pemilihan menjadi dasar evaluasi integritas dan keandalan sistem dalam skenario pemilihan yang sesungguhnya.



Gambar 1. Tahapan Penelitian

2.2 Otentikasi Dua Arah

Otentikasi dua arah (*two-factor authentication* atau 2FA) adalah metode keamanan yang memerlukan dua langkah verifikasi sebelum memberikan akses kepada pengguna [14]. Otentikasi dua arah menambahkan lapisan keamanan ekstra dengan menggabungkan dua elemen berbeda, seperti kombinasi kata sandi dengan token atau kode yang dikirim melalui pesan teks atau aplikasi. Tujuannya adalah untuk meningkatkan tingkat keamanan dengan memastikan identitas pengguna dengan lebih kuat [15]. Contoh penerapan otentikasi dua arah adalah dengan meminta pengguna memasukkan kata sandi sebagai langkah pertama, lalu diikuti dengan memasukkan kode yang dihasilkan oleh aplikasi otentikator atau dikirimkan melalui SMS sebagai langkah kedua. Dengan menggabungkan sesuatu yang diketahui pengguna (contoh: kata sandi) dan sesuatu yang dimiliki pengguna (contoh: token keamanan), otentikasi dua arah membuat akses ke akun atau informasi sensitif menjadi jauh lebih aman [16].

Otentikasi dua arah juga dapat menerapkan penggabungan antara biometrik seperti sidik jari atau pengenalan wajah dengan kata sandi atau PIN (*personal identification number*). Contohnya, untuk membuka kunci ponsel, pengguna diharuskan memindai sidik jari dan memasukkan PIN. Gabungan metode ini sangat efektif karena mengandalkan sesuatu yang melekat pada diri pengguna dan sesuatu yang hanya diketahui pengguna [17]. Dengan otentikasi dua arah, akun dan data pengguna jadi lebih terlindungi dari serangan phishing atau peretasan kata sandi.

2.3 SHA-512

SHA-512, singkatan dari *Secure Hash Algorithm* dengan panjang bit 512, merupakan algoritma fungsi *hash* kriptografi yang sangat populer dan diakui saat ini. Dikembangkan awalnya oleh Badan Keamanan Nasional Amerika Serikat (NSA), algoritma ini kemudian diresmikan sebagai standar pada tahun 2015. Salah satu ciri khasnya adalah menghasilkan nilai hash sepanjang 512 bit, menawarkan keamanan yang lebih tinggi dibandingkan dengan pendahulunya seperti SHA-1 dan SHA-256 [18]. Cara kerja SHA-512 mirip dengan algoritma hash pada umumnya, mengubah input data menjadi representasi unik berupa *hash value* sepanjang 512 bit. Keunikan representasi ini membuatnya sulit untuk dibalik, menjadikannya pilihan yang aman untuk mengamankan informasi sensitif seperti password pengguna. SHA-512 digunakan luas dalam kriptografi modern untuk penandatanganan digital, verifikasi integritas data, dan otentikasi [19]. Berikut adalah uraian tahapan SHA-512 mulai dari penambahan *bit padding* hingga menghasilkan *output*:

1. Penambahan bit padding
   Misalkan pesan asli M berukuran l bit. Kita tambahkan bit 0 hingga panjang pesan menjadi kongruen dengan 896 modulo 1024.
   $l + 1 + k \equiv 896 \pmod{1024}$
   k adalah banyaknya bit 0 yang ditambahkan.
   Contoh:
   l = 1000 bit
   k = 96 (agar kondisi kongruensi terpenuhi)
   M' (setelah padding) = M || 0..0, panjang M' = l + 1 + k = 1096 bit
2. Panjang *append*
   Panjang pesan dalam bit (N) ditulis dalam 128 bit dan ditambahkan di akhir pesan yang sudah dipadding:
   M'' = M' || N

Panjang M" = l + 1 + k + 128
Contoh:
N = 1096 dalam biner 128 bit = 00000000000010001100000110010
M" = M' || N (panjang 1224 bit)

3. Inisiasi nilai *hash*
   Inisialisasi 8 buah nilai hash awal H0,...,H7 dengan nilai heksadesimal konstan:
   H0 = 6a09e667f3bcc908
   H1 = bb67ae8584caa73b
   H2 = 3c6ef372fe94f82b
   H3 = a54ff53a5f1d36f1
   H4 = 510e527fade682d1
   H5 = 9b05688c2b3e6c1f
   H6 = 1f83d9abfb41bd6b
   H7 = 5be0cd19137e2179
4. Proses penjadwalan pesan
   Pesan M" yang telah dipadding dan append panjang, dibagi menjadi n buah blok B dengan panjang 1024 bit. Jumlah blok n didapat dari membagi panjang M" dengan 1024.
   n = panjang M" / 1024
   Misalkan panjang M" adalah 20000 bit, maka:
   n = 20000/1024 = 20 blok
   Maka M" dibagi menjadi:
   B0 (blok 1) berisi bit 1 s/d 1024
   B1 (blok 2) berisi bit 1025 s/d 2048
   ...
   B19 (blok 20) berisi bit 18433 s/d 20000
   Setiap blok B kemudian diproses dengan fungsi kompresi f yang menggabungkan blok B dengan nilai hash sebelumnya H, menghasilkan nilai hash baru.
   Contoh blok ke-1:
   H0 = H0 + f(H0,B0)
   H1 = H1 + f(H1,B0)
   ...
   H7 = H7 + f(H7,B0)
   Contoh blok ke-2:
   H0 = H0 + f(H0,B1)
   H1 = H1 + f(H1,B1)
   ...
   H7 = H7 + f(H7,B1)
   Seterusnya hingga semua blok diproses.
5. *Output*
   Setelah semua blok diproses, output SHA-512 adalah nilai hash akhir H0 sampai H7 yang digabungkan:
   SHA-512 = H0 || H1 || H2 || H3 || H4 || H5 || H6 || H7
   Dimana || adalah operator penggabungan string biner. Panjang output SHA-512 adalah 512 bit atau 64 byte.

2.4 Time-based One-Time Password (TOTP)

TOTP adalah metode otentikasi dua faktor yang menghasilkan kode pengguna sekali pakai berdasarkan waktu yang telah ditetapkan. Metode ini menggunakan kalkulasi matematis dengan melibatkan waktu saat ini untuk menciptakan kode yang hanya berlaku selama periode tertentu [20]. Pengguna umumnya mengakses aplikasi otentikator seperti *Google Authenticator* atau *Authy* yang menyinkronkan dan menghasilkan kode TOTP secara berkala. Kode ini diperlukan saat pengguna login atau melakukan transaksi yang memerlukan otentikasi, memberikan lapisan keamanan tambahan berdasarkan kombinasi sesuatu yang hanya diketahui oleh pengguna (kata sandi) dan sesuatu yang dihasilkan secara dinamis berdasarkan waktu (kode TOTP) [21]. Keunggulan utama TOTP adalah tingkat keamanan yang tinggi karena sifat kode yang hanya berlaku sesaat. Hal ini membuatnya sulit bagi pihak tak berwenang untuk menggunakan atau mencuri kode otentikasi [22]. TOTP banyak digunakan dalam layanan perbankan, email, dan otentikasi ganda aplikasi. Cara kerja TOTP adalah kode dihasilkan oleh token atau

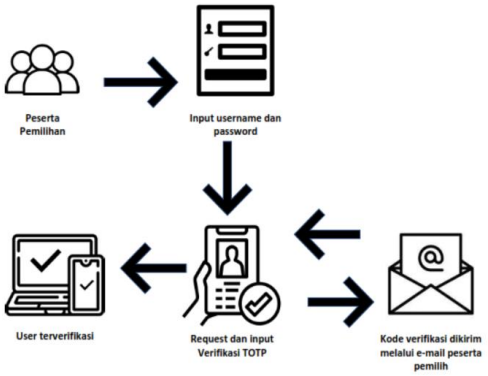
EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647 (Online)
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i1.1782

aplikasi otentikator yang sudah tersinkronisasi dengan *server*. Kode ini selalu berubah berdasarkan waktu saat itu dan hanya valid selama periode tertentu [23].

3. HASIL DAN PEMBAHASAN

3.1 Skema dan Arsitektur TOTP

Untuk skema dan arsitektur TOTP yang dibangun pada penelitian ini mengikuti pada alur sesuai gambar 2.

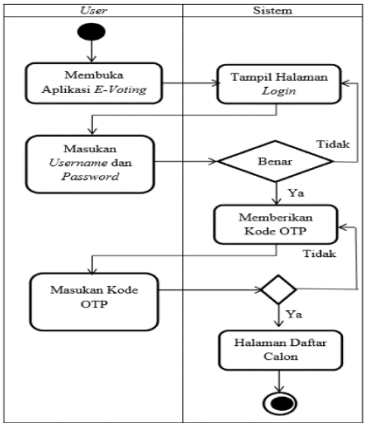


Gambar 2. Tahapan Skema Arsitektur TOTP

Gambar 2 menunjukkan alur verifikasi pengguna pada sistem pemilihan Presiden Mahasiswa yang dibangun. Dimulai dari pengguna atau peserta pemilih memasukkan username dan password untuk login. Setelah itu sistem akan meminta peserta pemilih untuk melakukan verifikasi dua faktor menggunakan kode TOTP. Kode verifikasi TOTP ini dikirimkan melalui email kepada masing-masing peserta pemilih. Jika kode TOTP yang dimasukkan benar, maka pengguna terverifikasi dan dapat mengakses sistem pemilihan. Alur verifikasi dua faktor ini digunakan sebagai lapisan keamanan tambahan untuk memastikan bahwa pengguna yang login adalah pemilik akun yang sah. Dengan otentikasi dua faktor, selain harus memasukkan password, pengguna juga harus memasukkan kode verifikasi yang dikirimkan ke email masing-masing. Hal ini dapat meningkatkan keamanan dan mencegah akses dari pengguna yang tidak berwenang. Secara keseluruhan, gambar ini menjelaskan alur verifikasi pengguna pada sistem pemilihan dengan menggunakan otentikasi dua faktor berbasis TOTP.

3.2 Rancangan Sistem

Sistem yang dirancang pada sistem pemilihan Presiden Mahasiswa melibatkan 2 entitas yaitu user dan sistem seperti pada gambar 3. User atau peserta membuka aplikasi, lalu memasukkan username dan passwordnya. Jika *username* dan *password* benar maka sistem akan mengirimkan kode OTP ke e-mail peserta dengan batas waktu yang ditentukan. Peserta memasukkan kode OTP seperti yang telah dikirimkan sistem, jika peserta memasukkan kode OTP dengan benar maka sistem akan mengarahkan kepada halaman daftar calon Presiden mahasiswa, namun bila salah maka user diminta untuk *request* kode OTP yang baru.



Gambar 3. Tahapan Skema Arsitektur TOTP dengan SHA-512

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647 (Online)
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i1.1782

Gambar 4 adalah interface dari halaman login dan verifikasi pengguna. Sistem dibangun dengan berbasis web, namun demikian tetap dapat diakses dengan menggunakan *smartphone* untuk peserta dengan pengguna *mobile*.

Gambar 4. Halaman Login dan Verifikasi Peserta

User menginputkan *username* dan *password* nya dan menekan tombol login, kemudian sistem akan mengirimkan kode OTP berbasis waktu atau TOTP dan diarahkan kehalaman verifikasi OTP seperti pada gambar 4. Peserta pemilih dapat melihat kode OTP pada email yang telah didaftarkan sebelumnya seperti terlihat pada gambar 5.

Gambar 5. Hasil OTP Dikirimkan Via E-mail

3.3 Pengujian SHA-512

Dari hasil analisis pada fungsi login di dalam mekanisme otentikasi dua faktor, dapat disimpulkan bahwa nilai hash yang dihasilkan dari pesan yang dimasukkan terdiri dari enam digit bilangan. Proses pembentukan hash ini menggunakan algoritma SHA-512, yang memastikan keamanan dalam proses otentikasi. Enam digit tersebut menjadi dasar verifikasi TOTP, meningkatkan keamanan keseluruhan sistem otentikasi. Proses otentikasi ini memberikan lapisan keamanan tambahan dengan memastikan bahwa kode yang dihasilkan bersifat unik dan hanya berlaku dalam jangka waktu tertentu, memperkuat perlindungan terhadap potensi ancaman keamanan. Pengujian SHA-512 yang dilakukan kali ini hanya dilakukan dengan menggunakan e-mail dengan domain Gmail (untuk alamat pengguna disamarkan). Hasil pengujian sebanyak 10 peserta pemilih dapat terlihat pada tabel 1.

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647 (Online)
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i1.1782

Tabel 1. Hasil SHA-512 Terhadap Peserta

Alamat e-mail	Kode TOTP	Hash SHA-512
aaaa@gmail.com	245391	2a83f36b6c45929590b4737fc2c64c568d3317d40d61aac3f30947dffe3674d85e57e8ecdb752c588b08fe558420a2bd3794fae9378d88c4e9c993bbe1ed8cc0
bbb@gmail.com	821093	05abbfcdbc5a1baacbc4abe0f5aac3321644e7fb44b164b773cbfdd138768d4530751fcc595816dd301642b5212c7d7fd3f7c033f5bbfc323874c04aa0757d6
ccc@gmail.com	673241	10ccecffcft417107a5cd4c581f413b129df799198daf83eb5c9e3c8a98e9f1c954250fbd5ca4aa00ccd40e01e302f33823b8b30b7108c0a8042c8d443498ad
ddd@gmail.com	908765	a62fcadaf3e02075965ebfef3234f8b3a29cbaaddc0341bc756554e5eba528b23639cd0ec075822d2795528cbd33d1eee06440f5f376513d65f106f148a04379
eee@gmail.com	124578	3de90237ab5fa1914ccfef338d8f058816b75be916e34dfa8468e0adea933d37677b2da29e9cbe6daece5652efad0162c56b6f71c6560c50c0d3deaafef52a21
fff@gmail.com	564981	441ce6b69d4d6fd9bcc760300f30d1789383cff27cbf523b237e017a97aca1ca3f3a27974ccd3160b2e7d892ce25f10d972837fa695c01e5cbcac856a759e70d
ggg@gmail.com	778621	bb912246607a000681baad7eb3a9050a44aa83b9db8f807a0fe45e7f5121372f409fa16025a1967d532f8a239ed1d6579eba7dacc2a2d0476f1375e649f6de4e
hhh@gmail.com	908833	e829d05b68cd992080af6a06b9835f1a41d6e49ebd7089d2c66c8876acf126aee3470b46ad5a11590b705941cfc5a0b83b58aa0534466ceb51dcdfc2c431ad39
iii@gmail.com	457789	4792d55f4e39378ce185cf8a51df8a1ad9d64e1ca4d18bd310e717426f58417a0a3efdbaeb649fd422e834586cb2593edc89c3096a7ae398dec748fb061e9fca
jjj@gmail.com	013321	39af9bce05c74fd9468db8b6f780bfb98380ac4036455bef9760c13992f3defd71d0726911b2c1e2f8fe9729afdd492320523484e5739b96a5c053811d13f4d6

3.4 Pengujian Sistem

Pemilih dalam sistem pemilihan Presiden Mahasiswa menggunakan aplikasi KPRM yang dirancang khusus untuk memfasilitasi proses pemungutan suara secara online seperti pada gambar 6. Setiap pemilih adalah mahasiswa aktif yang telah terdaftar dan memiliki hak suara dalam pemilihan ini. Untuk mengakses aplikasi, pemilih harus memasukkan akun mereka dengan menggunakan Nomor Induk Mahasiswa (NIM) dan kata sandi pada kolom yang telah disediakan di halaman login. Setelah berhasil masuk, pemilih dapat melanjutkan ke tahap pemilihan dengan memilih salah satu calon Presiden Mahasiswa yang tersedia.

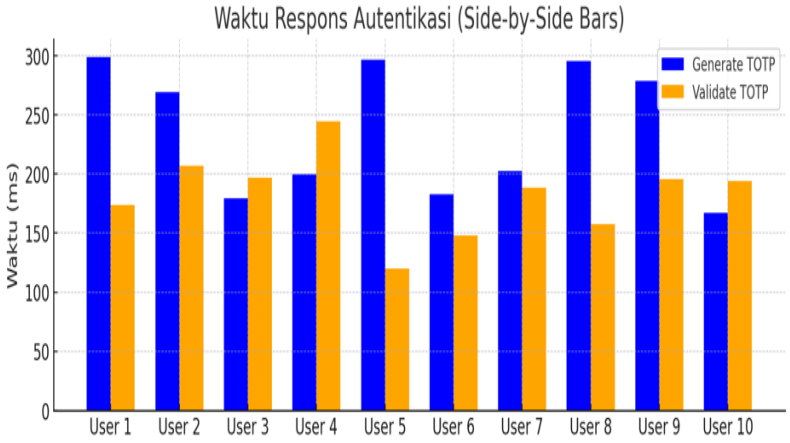
Gambar 6. Tampilan Login

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647 (Online)
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i1.1782

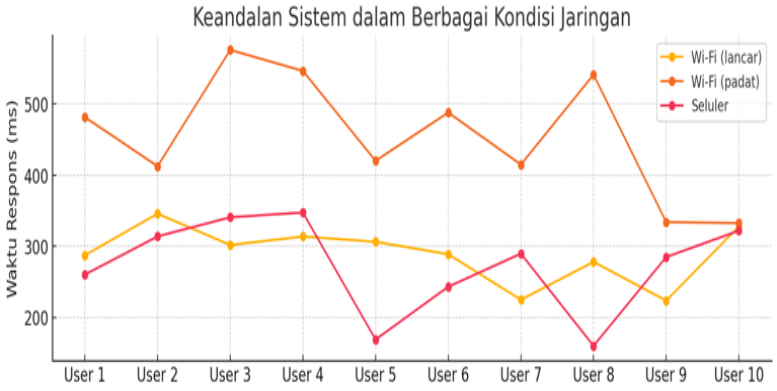
.

Gambar 7. Tampilan Verifikasi TOTP

Selain pengujian pada interface, kami juga melakukan pengujian kehandalan sistem dengan beberapa parameter terhadap 10 pengguna. Parameter tersebut diantaranya waktu respons, kondisi jaringan, dan penerimaan pengguna (*acceptance test*) terhadap keamanan sistem berbasis TOTP dan SHA-512.

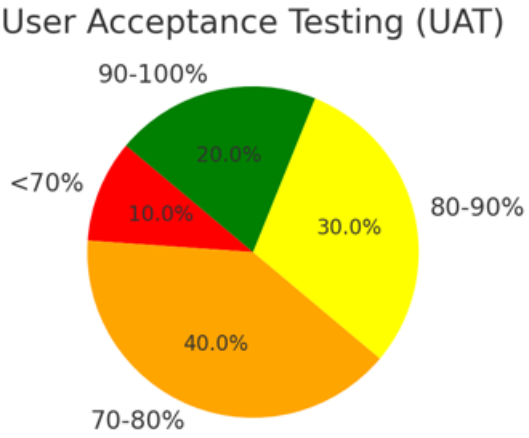


Gambar 8. Pengujian Terhadap Waktu Respons



Gambar 9. Pengujian Terhadap Kondisi Jaringan

EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647 (Online)
Website: https://journal.fkpt.org/index.php/Explorer DOI: https://doi.org/10.47065/explorer.v5i1.1782



Gambar 10. Pengujian Penerimaan Pengguna

Grafik pada gambar 8 menunjukkan waktu rata-rata yang diperlukan untuk menghasilkan dan memvalidasi TOTP menggunakan algoritma SHA-512 untuk 10 pengguna. Secara umum, waktu yang dibutuhkan untuk menghasilkan TOTP berkisar antara 150 hingga 300 ms, sementara waktu untuk memvalidasi TOTP sedikit lebih cepat, berada di rentang 100 hingga 250 ms. Waktu validasi yang lebih cepat ini mencerminkan efisiensi sistem dalam mengecek validitas TOTP dibandingkan dengan proses penghasilannya. Grafik ini juga menunjukkan konsistensi respons sistem antar pengguna, dengan hanya sedikit variasi antara pengguna yang satu dengan lainnya, yang mengindikasikan stabilitas algoritma SHA-512 dalam implementasi otentikasi dua faktor.

Gambar 9 memvisualisasikan waktu respons otentikasi sistem dalam tiga kondisi jaringan: Wi-Fi saat lalu lintas jaringan lancar, Wi-Fi saat lalu lintas padat, dan jaringan seluler. Hasil menunjukkan bahwa waktu respons pada jaringan Wi-Fi dengan lalu lintas lancar berada di kisaran 200 hingga 400 ms, sementara pada Wi-Fi dengan lalu lintas padat, waktu respons meningkat secara signifikan, mencapai 300 hingga 600 ms. Sebaliknya, jaringan seluler memberikan waktu respons yang lebih konsisten dan lebih cepat dibandingkan Wi-Fi pada kondisi padat, berkisar antara 150 hingga 350 ms. Perbedaan ini menunjukkan bahwa kondisi jaringan sangat memengaruhi kinerja sistem, dengan lalu lintas padat pada Wi-Fi menjadi faktor yang memperlambat waktu otentikasi.

Sedangkan gambar 10 menampilkan hasil survei terhadap 10 pengguna mengenai tingkat kepuasan mereka dalam menggunakan sistem otentikasi dua faktor berbasis TOTP. Responden dibagi menjadi empat kategori tingkat kepuasan: <70%, 70-80%, 80-90%, dan 90-100%. Hasilnya menunjukkan bahwa mayoritas pengguna memberikan tingkat kepuasan yang tinggi, dengan proporsi terbesar berada pada kategori 80-90% dan 90-100%, yang masing-masing mencerminkan tingkat kepercayaan dan kenyamanan pengguna terhadap sistem. Hanya sebagian kecil responden yang memberikan skor di bawah 80%, yang menunjukkan bahwa sebagian besar pengguna menilai sistem ini mudah digunakan, aman, dan memberikan respons yang cepat dalam proses otentikasi.

Berdasarkan hasil pengujian, sistem otentikasi dua faktor berbasis TOTP dengan algoritma SHA-512 menunjukkan kehandalan yang tinggi dalam menghasilkan dan memvalidasi kode otentikasi secara efisien. Waktu respons rata-rata untuk menghasilkan TOTP berkisar antara 150 hingga 300 ms, sementara validasi membutuhkan waktu yang lebih singkat, yaitu 100 hingga 250 ms. Hal ini mengindikasikan bahwa algoritma SHA-512 mampu menangani proses hash dengan cepat meskipun memiliki tingkat keamanan yang sangat tinggi. Selain itu, waktu respons yang konsisten di antara 10 pengguna menggarisbawahi stabilitas sistem dalam skenario yang beragam.

Keandalan TOTP dengan SHA-512 juga terlihat dalam pengujian pada berbagai kondisi jaringan. Meskipun performa sedikit menurun saat lalu lintas jaringan Wi-Fi padat, sistem tetap memberikan waktu respons yang dapat diterima, dengan peningkatan waktu respons yang tidak terlalu ekstrem. Lebih penting lagi, dalam jaringan seluler yang sering kali memiliki latensi tinggi, sistem tetap mampu memberikan waktu respons yang cepat dan konsisten. Ini menunjukkan bahwa TOTP dengan SHA-512 memiliki ketahanan terhadap fluktuasi kondisi jaringan. Tingkat kepuasan pengguna yang tinggi (80-100%) menunjukkan bahwa sistem yang dibangun layak digunakan dan handal.

4. KESIMPULAN

Implementasi autentikasi dua faktor berbasis TOTP dengan algoritma hash SHA-512 pada sistem pemilihan Presiden Mahasiswa terbukti handal, aman, dan responsif. Hasil pengujian menunjukkan bahwa waktu pengiriman kode OTP rata-rata berkisar antara 150 hingga 300 ms, sementara waktu validasi berada dalam rentang 100 hingga 250 ms. Ini menunjukkan efisiensi sistem, bahkan di bawah kondisi jaringan padat. Sistem ini efektif dalam mencegah akses tidak sah dan memberikan pengalaman pengguna yang optimal. Dengan tingkat kepuasan lebih dari 80%, sistem ini menegaskan kemudahan penggunaan dan keandalannya. Lapisan keamanan tambahan yang diterapkan, berupa autentikasi berbasis waktu dan algoritma hash SHA-512, mampu mengurangi risiko serangan siber seperti *brute force* dan sejenisnya, serta memastikan integritas proses pemilihan. Untuk penelitian selanjutnya, ada beberapa area yang dapat ditingkatkan. Efisiensi pengiriman kode TOTP dalam kondisi jaringan tidak stabil perlu diperbaiki. Selain itu, eksplorasi penggunaan algoritma hash yang lebih ringan, seperti SHA-256, atau integrasi teknologi *blockchain* dapat meningkatkan efisiensi, transparansi, dan integritas data dalam proses pemilihan.

REFERENSI

[1] D. Arisandi, S. Sukri, and M. B. Yusuf, "PEMERIKSAAN INTEGRITAS DOKUMEN DENGAN DIGITAL SIGNATURE ALGORITHM," *JOISIE J. Inf. Syst. Informatics Eng.*, vol. 4, no. 1, pp. 1–6, 2020, doi: 10.55601/jsm.v16i1.180.

[2] F. Basya, M. Hardjanto, and I. Permana Putra, "SHA512 and MD5 Algorithm Vulnerability Testing Using Common Vulnerability Scoring System (CVSS)," *Buana Inf. Technol. Comput. Sci. (BIT CS)*, vol. 3, no. 1, pp. 1–4, 2022, doi: 10.36805/bit-cs.v3i1.2046.

[3] I. Rahmatsyah, Y. Sari Siregar, and Khairunnisa, "Proteksi Keamanan Data dengan Menerapkan Algoritma Bacon Cipher dan ROT128," *J. Comput. Sci. Inf. Technol.*, vol. 4, no. 1, pp. 34–41, 2024, [Online]. Available: https://journal.fkpt.org/index.php/Explorer/article/view/1099

[4] D. Setiawan, M. Charlie Pratama, and D. Arisandi, "Implementasi Sistem Keamanan Jaringan Menggunakan Rule-Based Ids Pada Pt Netkrida Tuah Cakrawala," *JOISIE J. Inf. Syst. Informatics Eng.*, vol. 7, no. 2, pp. 381–389, 2023.

[5] M. U. Noor, "Tanda tangan digital: otoritas pada arsip elektronik," *JIPI (Jurnal Ilmu Perpust. dan Informasi)*, vol. 6, no. 1, pp. 17–26, 2021.

[6] M. M. Purba, "Perancangan E-Voting Untuk Pemilihan Bem Berbasis Web," *J. Sist. Inf. Univ. Suryadarma*, vol. 5, no. 2, pp. 160–170, 2014, doi: 10.35968/jsi.v5i2.245.

[7] L. Qadriah, S. Achmady, and Husaini, "Sistem Pengamanan Dokumen dengan Algoritma Time-Based One Time Password (TOTP) pada Two-Factor Authentation (2FA)," *J. Sains dan Inform.*, vol. 9, no. November 2022, pp. 29–35, 2023, doi: 10.34128/jsi.v9i1.519.

[8] A. Setiawan and A. I. Purnamasari, "Implementasi JSON Web Token Berbasis Algoritma SHA-512 untuk," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 1, no. 10, pp. 4–10, 2021.

[9] L. G. R. Semesta and S. Amini, "Implementasi One Time Password Dengan Algoritma Secure Hash Algorithm 512 (SHA-512)," *Skanika*, vol. 1, no. 3, pp. 1206–1211, 2018.

[10] A. Y. Fitriyansyah and M. Hazri, "Analisis Security Web Login Mahasiswa Menggunakan Algoritma Two-Factor Time-Based One Time Password," *Sainstech J. Penelit. dan Pengkaj. Sains dan Teknol.*, vol. 30, no. 1, pp. 1–14, 2020, doi: 10.37277/stch.v30i1.725.

[11] M. A. M. Hayat, Abbas Reski, and Bakti Rizki Yusliana, "Desain Dan Implementasi Time Based One Time Password," *Muhyiddin*, vol. 4, no. 1, pp. 16–23, 2022.

[12] N. Sarah Hapsari, Y. Fatman, and E. Penulis Korespondensi, "Implementasi Metode One Time Password pada Sistem Pemesanan Online," *J. Media Inform. Budidarma*, vol. 4, no. 4, pp. 930–939, 2020, doi: 10.30865/mib.v4i4.2195.

[13] A. N. Sari and T. G. Abdillah, "Metode Absensi Mahasiswa berbasis QR Code dan Time-Based One-Time Password," *J. Inform. Polinema*, vol. 7, no. 2, pp. 29–34, 2021, doi: 10.33795/jip.v7i2.492.

[14] D. Tirfe and V. K. Anand, "A Survey on Trends of Two-Factor Authentication BT - Contemporary Issues in Communication, Cloud and Big Data Analytics," in *Contemporary Issues in Communication, Cloud and Big Data Analytics*, H. K. D. Sarma, V. E. Balas, B. Bhuyan, and N. Dutta, Eds., Singapore: Springer Singapore, 2022, pp. 285–296.

[15] G. Ali, M. A. Dida, and A. E. Sam, "Two-factor authentication scheme for mobile money: A review of threat models and countermeasures," *Futur. Internet*, vol. 12, no. 10, pp. 1–27, 2020, doi:

10.3390/fi12100160.

[16] M. A. Al Hilmi, A. Sumarudin, and W. P. Putra, "One-Time-Password (Otp) Dengan Modifikasi Vigenere Chiper Dan Perangkat Usb Berbasis Microcontroller, Sensor Fingerprint, Dan Real Time Clock (Rtc) Untuk Autentikasi Pengguna Pada Akses Aplikasi Web," *Cyber Secur. dan Forensik Digit.*, vol. 3, no. 2, pp. 6–11, 2020, doi: 10.14421/csecurity.2020.3.2.2082.

[17] N. W. K. Syah, M. I. Sani, and S. J. I. Ismail, "Alat Bantu E-voting Dengan Sensor Sidik Jari," in *eProceedings of Applied Science*, 2021, pp. 2726–2744.

[18] P. J. F. Bemida, A. M. Sison, and R. P. Medina, "Modified SHA-512 Algorithm for Secured Password Hashing," in *2021 Innovations in Power and Advanced Computing Technologies (i-PACT)*, IEEE, 2021, pp. 1–9.

[19] T. Velmurugan and S. Karthiga, "Security based Approach of SHA 384 and SHA 512 Algorithms in Cloud Environment," *J. Comput. Sci.*, vol. 16, no. 10, pp. 1439–1450, 2020, doi: 10.3844/jcssp.2020.1439.1450.

[20] L. Adelson *et al.*, "Smart Login Pada Website Dengan Menggunakan Qr Code Dan Otentikasi One Time Password," in *SNASTIKOM 2020*, 2020, pp. 425–430. [Online]. Available: www.snastikom.com

[21] C. Ozkan and K. Bicakci, "Security Analysis of Mobile Authenticator Applications," *2020 Int. Conf. Inf. Secur. Cryptology, ISCTURKEY 2020 - Proc.*, pp. 18–30, 2020, doi: 10.1109/ISCTURKEY51113.2020.9308020.

[22] I. Gordin, A. Graur, and A. Potorac, "Two-factor authentication framework for private cloud," in *2019 23rd International Conference on System Theory, Control and Computing, ICSTCC 2019 - Proceedings*, IEEE, 2019, pp. 255–259. doi: 10.1109/ICSTCC.2019.8885460.

[23] I. T. Plata and J. L. Calpito, "Application Of Time-Based One Time Password (TOTP) Algorithm For Human Resource E-Leave Tracking Web App," *Int. J. Sci. Technol. Res.*, vol. 9, no. 03, pp. 4070–4077, 2020.