IMPLEMENTASI TWO-FACTOR AUTHENTICATION (2FA) BERBASIS LINEAR CONGRUENTIAL METHOD DAN SHA-256 SEBAGAI PENGAMAN DATA MEDIS JANTUNGIN

Muhammad Anas Kusuma Amir [1)], M Hadi Prayitno [2)*]

[1,2)] *Informatika, Universitas Bhayangkara Jakarta Raya, Kota Bekasi, Indonesia*

** Correspondency : hadi.prayitno@dsn.ubharajaya.ac.id [1)]*

ABSTRAK

Keamanan sistem informasi medis sangat rentan terhadap serangan siber seperti *brute force* dan praktik *account sharing* jika hanya mengandalkan autentikasi faktor tunggal. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem *Two-Factor Authentication* (2FA) berupa *One-Time Password* (OTP) pada aplikasi JantungIn. Metode pengembangan yang digunakan adalah *Rapid Application Development* (RAD) dengan pola arsitektur *Boundary-Control-Entity* (BCE). Pembangkitan kode OTP 6-digit memanfaatkan *Linear Congruential Method* (LCM) dengan *seed* deterministik yang dihasilkan dari pemotongan nilai *hash* SHA-256 (variabel *username* dan interval waktu 30 detik). Penyimpanan sesi menggunakan *in-memory map* dengan fitur *Auto-Delete* guna mencegah *replay attack*. Sistem diuji menggunakan dua metode: *Black-Box Testing* dan uji *Avalanche Effect*. Hasil *Black-Box Testing* menunjukkan tingkat keberhasilan 100% pada 8 skenario pengujian, termasuk ketahanan saat server di-*restart*. Hasil uji *Avalanche Effect* membuktikan bahwa perubahan satu karakter pada parameter masukan memberikan perubahan (*Hamming Distance*) yang signifikan, mencapai 46,88% pada tahap SHA-256 dan 54,84% pada tahap komputasi LCM, membuktikan ketahanan algoritma terhadap prediksi matematis.

Kata Kunci : *Avalanche Effect, Black-Box, In-Memory, Linear Congruential Method*, OTP

ABSTRACT

The security of medical information systems is highly vulnerable to cyberattacks such as brute-force attacks and account sharing if it relies solely on single-factor authentication. This study aims to design and implement a Two-Factor Authentication (2FA) system using One-Time Passwords (OTP) in the JantungIn application. The development method used is Rapid Application Development (RAD) with a Boundary-Control-Entity (BCE) architectural pattern. The generation of 6-digit OTP codes utilizes the Linear Congruential Method (LCM) with a deterministic seed generated from the hash of SHA-256 (using the username variable and a 30-second time interval). Session storage uses an in-memory map with an Auto-Delete feature to prevent replay attacks. The system was tested using two methods: Black-Box Testing and Avalanche Effect testing. The results of the black-box testing showed a 100% success rate across 8 test scenarios, including resilience when the server was restarted. The Avalanche Effect test results demonstrate that a single-character change in the input parameters results in a significant change (Hamming Distance), reaching 46.88% at the SHA-256 stage and 54.84% at the LCM computation stage, proving the algorithm's resistance to mathematical prediction.

Keywords: Avalanche Effect, Black-Box, In-Memory, Linear Congruential Method, OTP

1. PENDAHULUAN

Perkembangan sistem informasi berbasis jaringan telah mendorong meningkatnya kebutuhan akan mekanisme autentikasi yang tidak hanya bergantung pada kombinasi kata sandi konvensional. Keamanan sistem informasi pada dasarnya dirancang untuk membatasi akses informasi hanya kepada pihak yang berwenang untuk melihatnya (*Need to Know*). Perlindungan informasi harus mencakup tiga aspek utama yang dikenal sebagai *The Information Security Triad* (*CIA Triad*), yaitu *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan) (Pham *et al.*, 2021). Saat ini, model autentikasi faktor tunggal (*single-factor authentication*) terbukti sangat rentan terhadap berbagai serangan siber, sehingga memudahkan penyerang untuk melakukan pencurian identitas apabila kredensial yang digunakan lemah (Setiawan, 2016).

Urgensi penguatan sistem keamanan pada aplikasi penilaian risiko kardiovaskular JantungIn didasarkan pada temuan melalui tahap audit keamanan internal (*vulnerability assessment*). Dalam pengujian tersebut, ditemukan kerentanan serius di mana sistem belum memiliki mekanisme pembatasan *request* (*rate limiting*) atau verifikasi tambahan, sehingga rentan ditembus melalui serangan *brute force*. Serangan *brute force* merupakan teknik intrusi yang bekerja dengan cara mencoba seluruh kemungkinan kombinasi kata sandi secara sistematis dan terus-menerus hingga berhasil menembus sistem (Stallings dan Brown, 2024). Faktanya, arsitektur pertahanan lama cenderung menunjukkan kelemahan ketika dihadapkan pada skema serangan *brute force* modern yang jauh lebih kompleks (Ruambo *et al.*, 2025).

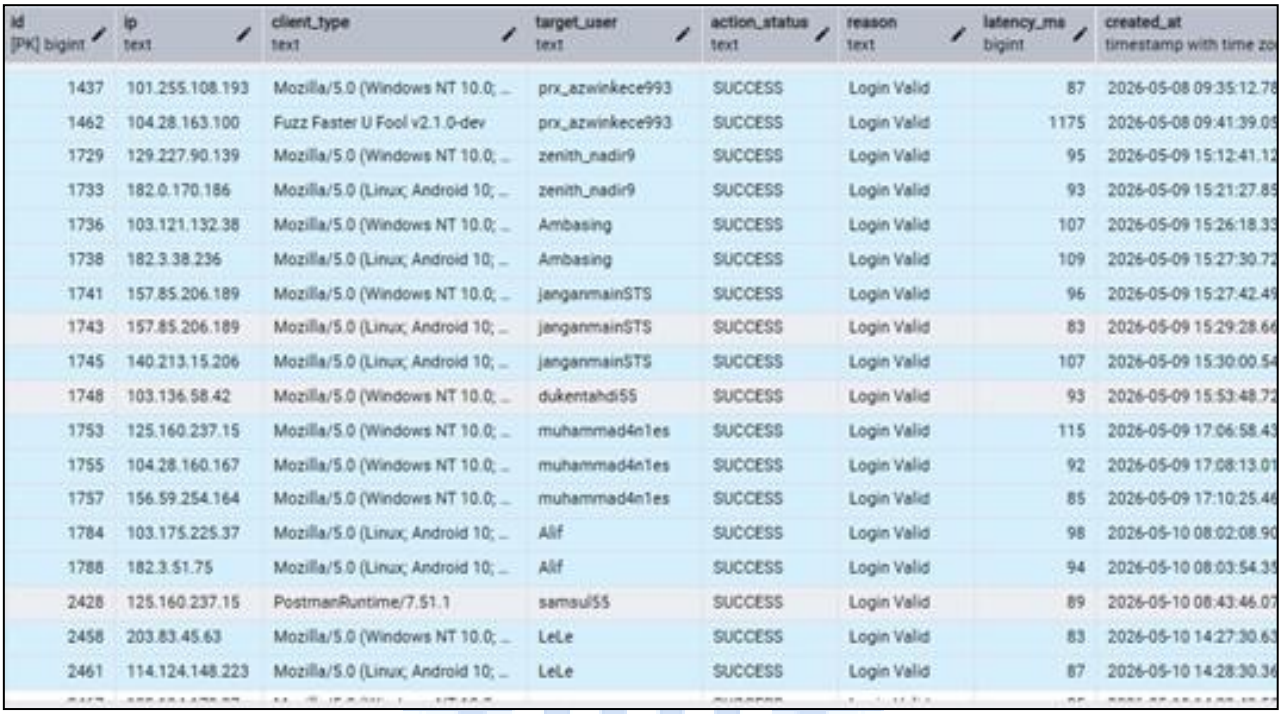
Pada Gambar 1. yang tercatat pada log aktivitas sistem, terdeteksi adanya anomali berupa percobaan akses berulang secara otomatis dalam frekuensi tinggi pada *endpoint* login menggunakan perangkat lunak pihak ketiga, *Fuzz Faster U Fool v2.1.0-dev*.

id [PK] bigint	ip text	client_type text	target_user text	action_status text	reason text	latency_ms bigint	created_at timestamp with time zone
1452	104.28.163.100	Fuzz Faster U Fool v2.1.0-dev	prx_azwinkece993	FAILED	username atau password tidak valid	1014	2026-05-08 09:41:38.9262...
1453	104.28.163.100	Fuzz Faster U Fool v2.1.0-dev	prx_azwinkece993	FAILED	username atau password tidak valid	1164	2026-05-08 09:41:39.0307...
1454	104.28.163.100	Fuzz Faster U Fool v2.1.0-dev	prx_azwinkece993	FAILED	username atau password tidak valid	976	2026-05-08 09:41:38.9949...
1455	104.28.163.100	Fuzz Faster U Fool v2.1.0-dev	prx_azwinkece993	FAILED	username atau password tidak valid	913	2026-05-08 09:41:38.9947...
1456	104.28.163.100	Fuzz Faster U Fool v2.1.0-dev	prx_azwinkece993	FAILED	username atau password tidak valid	1075	2026-05-08 09:41:39.0198...
1457	104.28.163.100	Fuzz Faster U Fool v2.1.0-dev	prx_azwinkece993	FAILED	username atau password tidak valid	1139	2026-05-08 09:41:39.0423...
1458	104.28.163.100	Fuzz Faster U Fool v2.1.0-dev	prx_azwinkece993	FAILED	username atau password tidak valid	1045	2026-05-08 09:41:39.0524...
1459	104.28.163.100	Fuzz Faster U Fool v2.1.0-dev	prx_azwinkece993	FAILED	username atau password tidak valid	1170	2026-05-08 09:41:39.0538...
1460	104.28.163.100	Fuzz Faster U Fool v2.1.0-dev	prx_azwinkece993	FAILED	username atau password tidak valid	1032	2026-05-08 09:41:39.0422...
1461	104.28.163.100	Fuzz Faster U Fool v2.1.0-dev	prx_azwinkece993	FAILED	username atau password tidak valid	1176	2026-05-08 09:41:39.0479...
1462	104.28.163.100	Fuzz Faster U Fool v2.1.0-dev	prx_azwinkece993	SUCCESS	Login Valid	1175	2026-05-08 09:41:39.0540...
1463	104.28.163.100	Fuzz Faster U Fool v2.1.0-dev	prx_azwinkece993	FAILED	username atau password tidak valid	1177	2026-05-08 09:41:39.0478...
1464	104.28.163.100	Fuzz Faster U Fool v2.1.0-dev	prx_azwinkece993	FAILED	username atau password tidak valid	1014	2026-05-08 09:41:39.0661...
1465	104.28.163.100	Fuzz Faster U Fool v2.1.0-dev	prx_azwinkece993	FAILED	username atau password tidak valid	1166	2026-05-08 09:41:39.0694...
1634	110.138.88.79	Mozilla/5.0 (X11; Linux x86_64; ...	aaaa	FAILED	username atau password tidak valid	4	2026-05-09 08:43:33.1687...
1671	110.138.88.79	PostmanRuntime/7.51.1	anomalimalam12	FAILED	username atau password tidak valid	86	2026-05-09 10:05:37.2265...
1672	110.138.88.79	PostmanRuntime/7.51.1	anomalimalam12	FAILED	username atau password tidak valid	82	2026-05-09 10:11:52.3077...
1673	110.138.88.79	PostmanRuntime/7.51.1	anomalimalam12	FAILED	username atau password tidak valid	82	2026-05-09 10:11:52.6702...
1674	110.138.88.79	PostmanRuntime/7.51.1	anomalimalam12	FAILED	username atau password tidak valid	84	2026-05-09 10:11:53.0442...

Gambar 1. Bukti Serangan Brute Force

Selain ancaman peretasan dari luar, kendala keamanan juga ditemukan pada kebijakan kontrol akses perangkat. Hasil observasi terhadap integritas sesi pengguna menunjukkan bahwa satu kredensial akun medis yang sangat sensitif dapat digunakan secara bersamaan (*simultan*) pada berbagai perangkat dengan identitas digital yang berbeda. Menurut Mayorga dan Yoo (2025), penggunaan kata sandi statis saat ini sudah tidak lagi aman untuk melindungi akun,

sehingga diperlukan mekanisme tambahan untuk memperkuat lapisan autentikasi .



id [PK] bigint	ip text	client_type text	target_user text	action_status text	reason text	latency_ms bigint	created_at timestamp with time zo
1437	101.255.108.193	Mozilla/5.0 (Windows NT 10.0; ...	prx_azwinkece993	SUCCESS	Login Valid	87	2026-05-08 09:35:12.78
1462	104.28.163.100	Fuzz Faster U Fool v2.1.0-dev	prx_azwinkece993	SUCCESS	Login Valid	1175	2026-05-08 09:41:39.05
1729	129.227.90.139	Mozilla/5.0 (Windows NT 10.0; ...	zenith_nadir9	SUCCESS	Login Valid	95	2026-05-09 15:12:41.12
1733	182.0.170.186	Mozilla/5.0 (Linux; Android 10; ...	zenith_nadir9	SUCCESS	Login Valid	93	2026-05-09 15:21:27.85
1736	103.121.132.38	Mozilla/5.0 (Windows NT 10.0; ...	Ambasing	SUCCESS	Login Valid	107	2026-05-09 15:26:18.33
1738	182.3.38.236	Mozilla/5.0 (Linux; Android 10; ...	Ambasing	SUCCESS	Login Valid	109	2026-05-09 15:27:30.72
1741	157.85.206.189	Mozilla/5.0 (Windows NT 10.0; ...	janganmainSTS	SUCCESS	Login Valid	96	2026-05-09 15:27:42.49
1743	157.85.206.189	Mozilla/5.0 (Linux; Android 10; ...	janganmainSTS	SUCCESS	Login Valid	83	2026-05-09 15:29:28.66
1745	140.213.15.206	Mozilla/5.0 (Linux; Android 10; ...	janganmainSTS	SUCCESS	Login Valid	107	2026-05-09 15:30:00.54
1748	103.136.58.42	Mozilla/5.0 (Windows NT 10.0; ...	dukentahdi55	SUCCESS	Login Valid	93	2026-05-09 15:53:48.72
1753	125.160.237.15	Mozilla/5.0 (Windows NT 10.0; ...	muhammad4n1es	SUCCESS	Login Valid	115	2026-05-09 17:06:58.43
1755	104.28.160.167	Mozilla/5.0 (Windows NT 10.0; ...	muhammad4n1es	SUCCESS	Login Valid	92	2026-05-09 17:08:13.01
1757	156.59.254.164	Mozilla/5.0 (Windows NT 10.0; ...	muhammad4n1es	SUCCESS	Login Valid	85	2026-05-09 17:10:25.46
1784	103.175.225.37	Mozilla/5.0 (Linux; Android 10; ...	Alif	SUCCESS	Login Valid	98	2026-05-10 08:02:08.90
1788	182.3.51.75	Mozilla/5.0 (Linux; Android 10; ...	Alif	SUCCESS	Login Valid	94	2026-05-10 08:03:54.35
2428	125.160.237.15	PostmanRuntime/7.51.1	samsul55	SUCCESS	Login Valid	89	2026-05-10 08:43:46.07
2458	203.83.45.63	Mozilla/5.0 (Windows NT 10.0; ...	LeLe	SUCCESS	Login Valid	83	2026-05-10 14:27:30.63
2461	114.124.148.223	Mozilla/5.0 (Linux; Android 10; ...	LeLe	SUCCESS	Login Valid	87	2026-05-10 14:28:30.36

Gambar 2. Bukti *Account Sharing*

Kondisi pada Gambar 2. mengonfirmasi adanya praktik berbagi akun (*account sharing*) yang secara langsung menegasikan prinsip otoritas akses tunggal, sehingga memicu risiko penyalahgunaan data medis oleh pihak yang tidak berwenang.

Untuk memitigasi risiko tersebut, penerapan *Two-Factor Authentication* (2FA) menjadi pendekatan yang krusial. Salah satu mekanisme 2FA yang efektif adalah *One-Time Password* (OTP), yang memberikan perlindungan ekstra dengan menghasilkan kata sandi berdurasi singkat yang selalu berubah setiap sesi (Qadriah, Achmady dan Husaini, 2023). Namun, implementasi OTP menghadapi tantangan pada sinkronisasi antara pengguna (*client*) dan peladen (*server*), seperti pergeseran waktu perangkat (*clock drift*) atau perbedaan parameter pembangkitan (Anggoro, 2024).

Mengatasi tantangan sinkronisasi tersebut, penelitian ini merumuskan penggunaan pendekatan algoritma matematis *Linear Congruential Method* (LCM). LCM merupakan metode komputasi pembangkit bilangan acak semu (*Pseudo-Random Number Generator*/PRNG) yang efisien (Rosen, 2019). Algoritma LCM bekerja dengan menghasilkan deret angka secara deterministik berdasarkan persamaan rekursif matematis $X_{n+1} = (aX_n + c)(\mathrm{mod}\ m)$. Dengan menggunakan nilai awal (*seed*) yang spesifik dan dikelola di sisi peladen, presisi sinkronisasi tetap terjaga mutlak tanpa bergantung pada waktu perangkat lokal.

Dari segi landasan teori keamanan, arsitektur sistem ini mengadopsi standar *National Institute of Standards and Technology* (NIST SP 800-63B) yang mensyaratkan bahwa OTP minimal terdiri dari 6 digit dan memiliki batas waktu kadaluwarsa yang sangat sempit untuk mencegah penyalahgunaan ulang (*replay attack*) (NIST, 2017). Oleh sebab itu, agar nilai *seed* yang dimasukkan ke dalam algoritma LCM tidak dapat direkayasa atau diprediksi, nilai tersebut diperkuat terlebih dahulu melalui fungsi *hash* kriptografis.

Penelitian ini memadukan fungsi *Secure Hash Algorithm 256* (SHA-256) untuk mengekstraksi nilai *seed* dari penggabungan

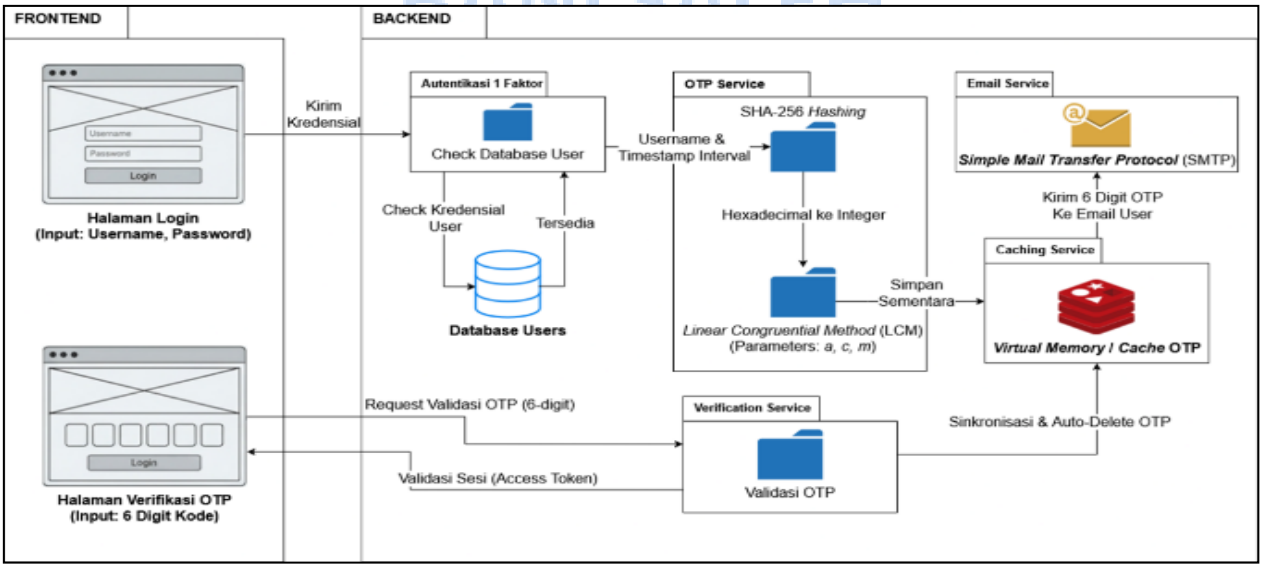
parameter nama pengguna (*username*) dan interval waktu dinamis. SHA-256 dipilih karena karakteristiknya yang *collision resistant* dan *one-way property*, di mana setiap perubahan kecil pada masukan akan menghasilkan nilai yang sama sekali berbeda dan tidak dapat dikembalikan ke teks aslinya (Stallings dan Brown, 2024).

Berdasarkan perumusan permasalahan di atas, penelitian ini bertujuan untuk merancang dan membangun arsitektur sistem autentikasi dua faktor (2FA) berbasis OTP dengan menerapkan algoritma *Linear Congruential Method* sebagai *seed generator* yang diperkuat dengan SHA-256. Sistem ini secara spesifik dibangun untuk menciptakan mekanisme verifikasi yang dapat memblokir praktik ilegal *account sharing*. Diharapkan sistem ini dapat menghasilkan lapisan keamanan informasi yang tangguh terhadap percobaan serangan eksploitasi *brute force* dengan tetap mempertahankan efisiensi sinkronisasi sistem bagi para pengguna layanan aplikasi medis JantungIn.

2. METODE

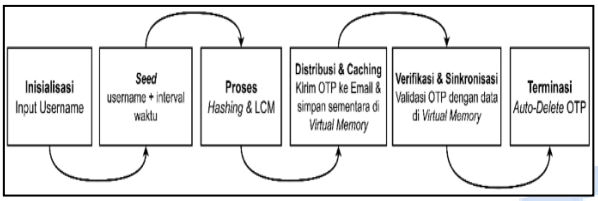
Penelitian implementatif ini berfokus pada pembuatan artefak Teknologi Informasi berupa modul keamanan autentikasi dua faktor (*Two-Factor Authentication/2FA*). Pendekatan yang digunakan dalam pengembangan sistem ini adalah *Rapid Application Development* (RAD). Metode RAD dipilih karena menitikberatkan pada siklus pengembangan yang berkecepatan tinggi dan iteratif, sehingga sangat ideal untuk perancangan dan pengujian algoritma matematis secara langsung melalui pembuatan purwarupa (*prototyping*) yang berkelanjutan. Tahapan pelaksanaannya mencakup *Communication and Planning* (evaluasi log aktivitas peladen dan perumusan kebutuhan), *Modeling* (perancangan logika, matematis, dan antarmuka), serta *Development* (konstruksi kode dan pengujian akhir).

Dalam proses pengembangannya, penelitian ini didukung oleh spesifikasi perangkat keras berupa laptop ASUS ROG Strix G531GD dengan prosesor Intel Core i5-9300H, RAM 16 GB DDR4, dan penyimpanan 512 GB NVMe SSD. Sementara itu, lingkungan perangkat lunak yang digunakan beroperasi pada Windows 11 dan Linux Ubuntu. Logika *backend* sistem dibangun menggunakan bahasa pemrograman Go (Golang) dipadukan dengan *framework* Gin Gonic untuk mempercepat pembuatan RESTful API, sedangkan perancangan model antarmukanya memanfaatkan aplikasi Figma.



Gambar 3. Arsitektur Sistem

Untuk menghindari penulisan data sensitif ke basis data permanen, sistem OTP dikelola murni pada memori internal peladen (*in-memory map* bawaan Go) yang berada di lapisan *Entity*. Penyimpanan memori ini dilengkapi dengan siklus *Auto-Delete*, di mana kode akan otomatis terhapus seketika sesudah verifikasi dinyatakan valid atau durasi masa berlaku 30 detik (*Time to Live*) telah terlampaui.



Gambar 4. Siklus Kerja Sistem

Pada tahap akhir, evaluasi terhadap sistem dilakukan melalui dua teknik pengujian yang komprehensif. Pertama, *Black-Box Testing* digunakan untuk mengevaluasi fungsionalitas antarmuka dan alur autentikasi tanpa meninjau struktur internal kode. Pengujian ini dirancang dalam 8 skenario uji untuk memastikan sistem dapat menolak kode yang kedaluwarsa, menahan percobaan lintas pengguna, serta membuktikan bahwa fungsi *Auto-Delete* mampu mencegah serangan *replay attack*. Kedua, Uji *Avalanche Effect* diterapkan sebagai pengujian *White-Box* untuk membuktikan sensitivitas struktural kriptografi di dalam sistem peladen. Teknik ini mengukur persentase perubahan bit (*Hamming Distance*) pada tahap komputasi SHA-256 dan algoritma LCM ketika diberikan modifikasi parameter yang sangat minor pada identitas pengguna maupun interval waktu.

3. HASIL DAN PEMBAHASAN

Hasil penelitian ini menyajikan implementasi modul keamanan *One-Time Password* (OTP) pada aplikasi JantungIn beserta hasil evaluasi dari pengujian yang telah dilakukan. Untuk memudahkan pemaparan, bagian ini dibagi ke dalam beberapa sub-pembahasan.

3.1. Implementasi Struktur Data *In-Memory* dan Komputasi Algoritma

Untuk meminimalkan risiko kebocoran data sensitif, sistem penyimpanan sesi OTP dirancang menggunakan struktur data *in-memory map* bawaan (native) Golang tanpa menggunakan basis data eksternal secara persisten. Pendekatan ini dilengkapi dengan mekanisme *Auto-Delete* yang akan menghapus kode secara otomatis dari memori internal server (*virtual memory*) seketika setelah verifikasi berhasil dilakukan atau batas waktu 30 detik (*Time to Live*/TTL) terlampaui. Mekanisme ini dirancang secara khusus untuk mencegah terjadinya celah serangan *replay attack*.

Pada sisi pembangkitan kode, sistem mengombinasikan fungsi *hash* kriptografis SHA-256 dan *Linear Congruential Method* (LCM) untuk menciptakan *seed* yang deterministik namun tidak dapat diprediksi (memiliki sifat *one-way function*). Variabel input (berupa gabungan *username* dan interval waktu Unix yang dibagi 30) diproses menggunakan SHA-256 menjadi 64 karakter heksadesimal.

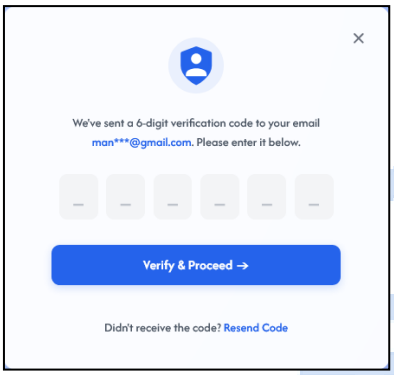
Sistem kemudian memotong 8 karakter pertama dari *hash* tersebut dan mengonversinya menjadi bilangan bulat (*integer*) sebagai nilai awal atau *seed* (X_0). Selanjutnya, nilai X_0 dimasukkan ke dalam persamaan rekursif LCM untuk melakukan komputasi pengacakan dengan standar parameter *ANSI C* (Rosen, 2019), yaitu:

$$X_{n+1} = (aX_n + c)(\text{mod } m) \quad (1)$$

Dengan nilai konstanta $a = 1103515245$, $c = 12345$, dan $m = 2^{31}$. Hasil iterasi pertama (X_1) kemudian dilakukan operasi modulus 1.000.000 untuk mengekstraksi hasil akhirnya menjadi seragam dalam format 6-digit kode OTP.

3.2. Implementasi Antarmuka Verifikasi OTP

Sebagai hasil dari perancangan antarmuka pengguna (*User Interface*), modul autentikasi JantungIn dilengkapi dengan sistem notifikasi dan umpan balik (*feedback*) visual secara *real-time* untuk memudahkan interaksi pengguna. Alur antarmuka verifikasi ini dirancang secara sekuensial mulai dari permintaan kode, penerimaan pesan, hingga validasi akhir.

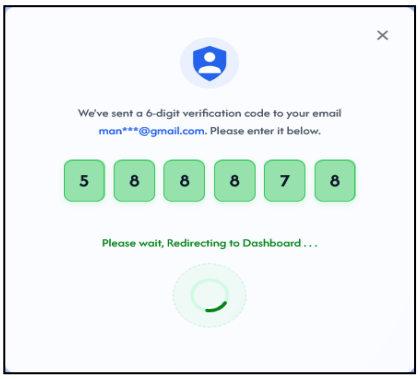


Gambar 5. Tampilan Antarmuka Input OTP

Berdasarkan Gambar 5, setelah pengguna berhasil memasukkan kredensial *username* dan *password* yang sah pada halaman login utama, sistem akan memunculkan jendela *pop-up* verifikasi. Antarmuka ini dirancang dengan menyediakan enam kotak input (*digit field*) kosong dan menampilkan instruksi bahwa kode verifikasi telah dikirimkan ke email terdaftar.

Gambar 6. Tampilan Pesan Email OTP

Secara bersamaan di latar belakang, peladen mengeksekusi komputasi algoritma *Linear Congruential Method* (LCM) dan langsung mendistribusikannya melalui layanan *Electronic Mail* (Email) pengguna. Seperti yang ditunjukkan pada Gambar 6, pesan email tersebut memuat 6-digit kode OTP beserta keterangan tegas mengenai batas waktu kedaluwarsa selama 30 detik untuk memberikan kesadaran keamanan bagi pengguna.



Gambar 7. Tampilan Umpan Balik Sukses Verifikasi OTP

Pada tahap akhir yang ditunjukkan pada Gambar 7, apabila 6-digit kode OTP yang diinputkan oleh pengguna terdeteksi valid dan cocok dengan data sesi yang tersimpan di dalam *Virtual Memory* peladen, sistem akan memberikan umpan balik visual berupa perubahan warna pada kotak input menjadi hijau. Sebagai tanda konfirmasi keberhasilan, antarmuka akan langsung menampilkan pesan "*Please wait, Redirecting to Dashboard...*". Pesan ini mengonfirmasi bahwa sesi autentikasi dua faktor telah sah, dan pengguna sedang dialihkan (*redirect*) secara otomatis untuk masuk ke halaman beranda utama aplikasi.

3.3. Hasil Pengujian *Black-Box*

Pengujian *Black-Box* dilakukan untuk memvalidasi pemenuhan persyaratan fungsionalitas antarmuka sistem dan efektivitas alur autentikasi, serta memastikan mekanisme keamanan berjalan sesuai dengan parameter perlindungan.

Tabel 1. Hasil Pengujian *Blackbox*

Skenario Uji	Input	Ekspektasi Output	Hasil
Login dengan identitas valid	*Username* & *password* benar	OTP terkirim ke email User	Pass
Login dengan kredensial tidak valid	*Username*/*password* salah	Pesan *error*	Pass
Verifikasi OTP valid	*UserId* & Kode OTP	Pesan *error* "OTP tidak	Pass

Skenario Uji	Input	Ekspektasi Output	Hasil
	benar	valid"	
Verifikasi OTP kadaluwarsa	*UserId* & Kode OTP > 30 detik	Pesan *error* "OTP tidak valid"	Pass
Verifikasi OTP lintas pengguna	*UserId* & OTP *User* berbeda	Pesan *error* "OTP tidak valid"	Pass
Replay attack	*UserId* & OTP yang sudah dipakai	Pesan *error* "OTP tidak valid"	Pass
Verifikasi OTP saat *Server Restart*	*UserId* & Kode OTP benar	Pesan *error* "OTP tidak valid"	Pass

Berdasarkan Tabel 1, sistem lulus 100% pada 8 skenario pengujian fungsional dan keamanan. Analisis dari temuan tersebut membuktikan bahwa mekanisme penghapusan otomatis berfungsi dengan sempurna dalam menggagalkan penggunaan kode bekas (*replay attack*) dan menolak akses kode yang telah melewati batas 30 detik. Sistem juga terbukti mampu memblokir praktik penggunaan kredensial menyilang (*cross-user*). Secara spesifik pada skenario *restart* peladen, penyimpanan sesi berbasis *in-memory* menunjukkan keandalannya dengan cara menggugurkan seluruh status OTP aktif secara otomatis (mencegah *dangling session*), sehingga memaksa pengguna untuk inisialisasi ulang demi menjaga integritas keamanan.

3.4. Hasil Pengujian *Avalanche Effects*

Pengujian struktur internal (*White-Box*) dilakukan untuk mengukur sensitivitas dan persentase perubahan bit (*Hamming Distance*) secara berlapis pada komputasi sistem. Pengujian dilakukan dengan memberikan modifikasi input yang sangat minor (satu karakter) untuk mengamati reaksi *avalanche effect*.

Tabel 2. Hasil Pengujian *Avalanche Effect*

Skenario	SHA-256 Hamming (%)	Trunc32 Hamming (%)	LCM X_1 Hamming (%)	OTP 6-digit Hamming (%)
Ubah 1 karakter *username*	46,88%	59,38%	54,84%	45,00%
Ubah interval waktu (+30s)	48,05%	46,88%	48,39%	35,00%

Berdasarkan Tabel 2, modifikasi minor pada input terbukti memberikan efek berantai yang sangat signifikan pada setiap lapis algoritma. Mengacu pada standar *Strict Avalanche Criterion* (SAC), pencapaian persentase yang mendekati nilai 50% pada tahapan *hashing* SHA-256 (46,88% dan 48,05%) dan tahapan LCM (54,84% dan 48,39%) membuktikan bahwa struktur algoritma sistem memiliki keacakan yang sempurna. Penurunan entropi pada luaran akhir OTP 6-digit menjadi 45,00% dan 35,00% adalah hal matematis yang wajar akibat adanya penyempitan ruang lingkup digit pada proses pemotongan modulus basis desimal terakhir. Secara keseluruhan, temuan ini mengonfirmasi bahwa 6-digit kode OTP yang dihasilkan oleh sistem memiliki tingkat dinamika yang sangat tinggi dan kebal terhadap upaya manipulasi rekayasa matematis (*seed guessing*) oleh peretas.

3.5. Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya, atas dukungan fasilitas selama pelaksanaan penelitian ini. Penghargaan juga disampaikan secara khusus kepada Bapak M. Hadi Prayitno, S.Kom, M.Kom. selaku dosen pembimbing yang telah memberikan arahan dan evaluasi teknis, serta seluruh pihak yang berkontribusi hingga penelitian ini dapat diselesaikan.

4. PENUTUP

4.1. Kesimpulan

Penelitian ini berhasil merancang dan mengimplementasikan sistem *Two-Factor Authentication* (2FA) berbasis *One-Time Password* (OTP) pada aplikasi JantungIn menggunakan kombinasi *Secure Hash*

Algorithm 256 (SHA-256) dan algoritma *Linear Congruential Method* (LCM). Penggunaan arsitektur penyimpanan *in-memory* yang dilengkapi mekanisme *Auto-Delete* 30 detik terbukti sangat tangguh dalam mencegah serangan *replay attack* serta menghindari *dangling session* apabila terjadi *restart* pada peladen. Berdasarkan pengujian *Black-Box* pada 8 skenario uji, sistem mencatatkan tingkat keberhasilan 100%, termasuk kemampuannya dalam memblokir praktik akses ilegal dan *account sharing* antar identitas perangkat yang berbeda. Lebih lanjut, pengujian *Avalanche Effect* membuktikan bahwa algoritma sistem memiliki tingkat entropi struktural yang sangat tinggi, dengan persentase perubahan bit mencapai 54,84% pada tahap komputasi LCM. Hal ini menegaskan bahwa 6-digit kode OTP yang dibangkitkan sangat dinamis, stabil, dan kebal terhadap upaya manipulasi serta prediksi matematis (*seed guessing*) oleh pihak peretas.

4.2. Saran

Berdasarkan keterbatasan dan temuan dalam penelitian ini, terdapat beberapa saran untuk pengembangan sistem selanjutnya:

1. Pengembangan mekanisme *Linear Congruential Method* (LCM) dapat diujicobakan dengan iterasi yang lebih kompleks, atau dipadukan dengan algoritma kriptografi asimetris untuk memastikan keamanan transmisi data secara *end-to-end* yang lebih mutlak.
2. Memperluas saluran distribusi pengiriman kode OTP. Selain menggunakan *Electronic Mail* (Email), sistem dapat diintegrasikan dengan API pihak ketiga seperti WhatsApp atau *SMS Gateway* guna mempercepat waktu penerimaan kode di sisi pengguna.
3. Melakukan pengujian keamanan (*security stress test*) dengan vektor serangan yang lebih beragam dan ekstrim, seperti *Distributed Denial of Service* (DDoS) atau *Man-in-the-Middle* (MitM) *attack*, guna mengukur ketahanan infrastruktur peladen secara lebih komprehensif.

5. DAFTAR PUSTAKA

Anggoro, H.T. (2024) *Implementasi Two Factor Authentication (2FA) Berdasarkan Protokol RFC 3548 Menggunakan Google Authenticator*.

Grassi, P.A. *et al.* (2017) *Digital identity guidelines: authentication and lifecycle management*. Gaithersburg, MD. Available at: https://doi.org/10.6028/NIST.SP.800-63b.

Mayorga, O.E.A. and Yoo, S.G. (2025) "One Time Password (OTP) Solution for Two Factor Authentication: A Practical Case Study," *Journal of Computer Science*, 21(5), pp. 1099–1112. Available at: https://doi.org/10.3844/jcssp.2025.1099.1112.

Pham, L.-H.T. *et al.* (2021) "The Information Security Triad: Confidentiality, Integrity, and Availability," *Information Systems for Business and Beyond*. Sacramento, CA: LibreTexts. Available at: https://workforce.libretexts.org/@go/page/9781.

Qadriah, L., Achmady, S. and Husaini (2023) "Sistem Pengamanan Dokumen dengan Algoritma Time-Based One Time Password (TOTP) pada Two-Factor Authentation (2FA)," *Jurnal Sains dan Informatika*, pp. 29–35. Available at: https://doi.org/10.34128/jsi.v9i1.519.

Rosen, K.H.. (2019) *Discrete Mathematics and Its Applications*. 8th Edition. New York: McGraw-Hill Education. Available at: https://books.google.co.id/books?id=ZO8iMAEACAAJ (Accessed: March 21, 2026).

Ruambo, F.A. *et al.* (2025) "Brute-force attack mitigation on remote access services via software-defined perimeter," *Scientific Reports*, 15(1), p. 18599. Available at:

https://doi.org/10.1038/s41598-025-01080-5.

Setiawan, T. (2016) *PENGEMBANGAN SISTEM TWO FACTOR AUTHENTICATION MENGGUNAKAN PROTOKOL TIME-BASED ONE TIME PASSWORD*.

Stallings, William. and Brown, Lawrie. (2024) *Computer security : principles and practice*. Pearson Education Limited.

UNIVERSITAS
BANI SALEH