Jurnal Infosecure Vol.6 No.1, April 2025
p-ISSN: 2087-1023
MTI-UNLA

Implementasi 2FA untuk Keamanan Sistem Informasi Akademik di Universitas Langlangbuana

Eki Adithya Suharman[1], Hadi Prasetyo Utomo [2], Ali Ahmadi[3]

Teknik Informatika, Fakultas Teknik, Universitas Langlangbuana[1,2,3]

[1]ekiadithya@gmail.com

[2]hadi@informatika.unla.ac.id

[3]kang.aliahmadi@gmail.com

Abstrak— Keamanan sistem informasi akademik sangat penting untuk menjaga integritas data pengguna dan mencegah akses tidak sah. Salah satu upaya untuk meningkatkan keamanan adalah dengan menerapkan autentikasi dua faktor (Two-Factor Authentication/2FA). Penelitian ini bertujuan mengimplementasikan 2FA pada sistem informasi akademik untuk menambah lapisan keamanan. Sistem dirancang menggunakan metode OTP (One-Time Password) yang dikirim melalui email atau aplikasi autentikator, serta dilengkapi fitur CAPTCHA untuk menghindari serangan otomatis seperti brute force. Metode penelitian mencakup perancangan, pengembangan, dan pengujian sistem autentikasi. Hasil menunjukkan bahwa kombinasi 2FA dan CAPTCHA efektif meningkatkan perlindungan sistem dengan mempersulit akses tidak sah. Implementasi ini memberikan kontribusi nyata dalam memperkuat keamanan sistem informasi akademik dari ancaman seperti peretasan dan pencurian kredensial pengguna.

Kata kunci— Keamanan Sistem Informasi, Autentikasi Dua Faktor, OTP, CAPTCHA, Sistem Informasi Akademik.

I. PENDAHULUAN

Kemajuan teknologi informasi telah membawa perubahan besar dalam berbagai aspek kehidupan, termasuk dalam bidang pendidikan. Salah satu wujud implementasi teknologi di dunia pendidikan adalah sistem informasi akademik (SIAK) yang berfungsi untuk mengelola data akademik secara efektif dan efisien. Namun, seiring dengan kemajuan teknologi, ancaman terhadap keamanan data juga semakin meningkat. Keamanan informasi menjadi aspek krusial, terutama pada sistem yang menyimpan data penting seperti nilai akademik, jadwal perkuliahan, dan data pribadi mahasiswa [1].

Pada Sistem Informasi Akademik (SIAK) Universitas Langlangbuana, terdapat sejumlah permasalahan keamanan yang memerlukan perhatian serius. Salah satu permasalahan utama adalah kerentanan pada sistem login yang sebelumnya hanya mengandalkan kombinasi username dan password. Kondisi ini membuka celah terhadap serangan credential stuffing, yaitu teknik di mana penyerang mencoba mengakses akun pengguna dengan menggunakan kombinasi username dan password yang telah bocor dari sistem lain [2]. Karena banyak pengguna cenderung menggunakan ulang kredensial yang sama di berbagai platform, metode ini menjadi salah satu ancaman nyata terhadap sistem login konvensional.

Untuk mengatasi masalah tersebut, diperlukan langkah strategis yang mampu meningkatkan keamanan sistem, salah satunya adalah dengan mengimplementasikan sistem autentikasi dua faktor (Two-Factor Authentication, 2FA). Menurut, penerapan 2FA terbukti mampu meningkatkan keamanan sistem informasi akademik secara signifikan dengan menambahkan lapisan verifikasi kedua yang bersifat dinamis. Dalam konteks penelitian ini, sistem 2FA diimplementasikan dengan cara mengirimkan kode OTP (One-Time Password) melalui platform Telegram, sehingga meskipun password pengguna diketahui oleh pihak tidak bertanggung jawab, mereka tetap tidak dapat mengakses sistem tanpa kode verifikasi tersebut [3].

Untuk menjamin bahwa OTP yang dikirim benar-benar acak dan aman, sistem menggunakan algoritma Cryptographically Secure Pseudo-Random Number Generator (CSPRNG)[4]. Algoritma ini dirancang untuk menghasilkan bilangan acak yang tidak hanya tampak acak, tetapi juga tidak dapat diprediksi, bahkan jika sebagian dari hasil atau status internal generator diketahui. Penggunaan CSPRNG pada sistem OTP memastikan bahwa kode yang dihasilkan bersifat unik, tidak mudah ditebak, dan tahan terhadap serangan brute force.

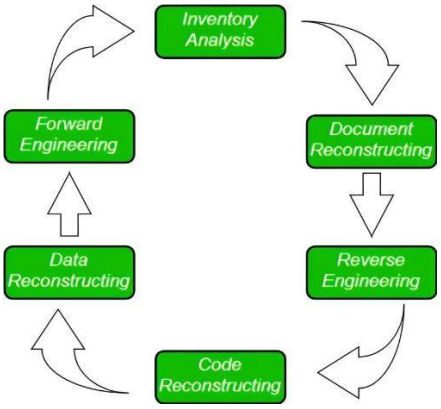
Aplikasi telah dilengkapi dengan fitur keamanan CAPTCHA agar aplikasi dapat lebih aman dari serangan hacker [5].

II. METODE

Penelitian ini menggunakan metode re-engineering dengan pendekatan studi kasus. Pendekatan ini digunakan karena fokus utama dari penelitian adalah melakukan perbaikan dan peningkatan pada sistem yang telah ada, khususnya pada modul login di Sistem Informasi Akademik (SIAK) Universitas Langlangbuana, yang terbukti memiliki kelemahan dalam aspek keamanan autentikasi.

Metode yang digunakan dalam penelitian ini adalah Software Re-engineering, yaitu proses rekayasa ulang

perangkat lunak yang bertujuan untuk meningkatkan struktur dan fungsionalitas sistem tanpa mengubah secara menyeluruh tujuan utamanya[6].Metode ini digunakan untuk mengintegrasikan fitur autentikasi dua faktor (2FA) ke dalam sistem login Sistem Informasi Akademik (SIAK) yang telah ada, dengan memanfaatkan Telegram Bot API sebagai pengirim kode OTP (One-Time Password) [7].



Gambar 1 Metode Reengineering

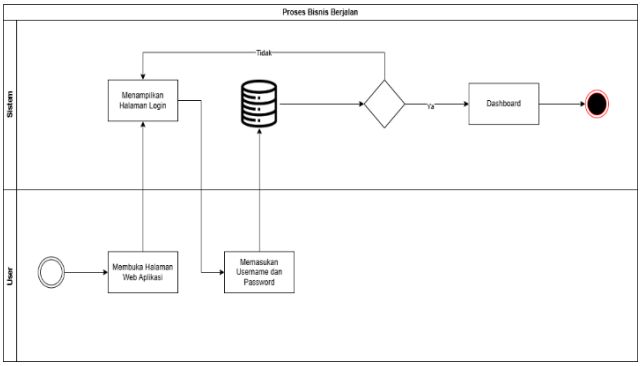
Proses rekayasa ulang perangkat lunak dalam penelitian ini terdiri dari enam tahapan utama. Pertama, Inventory Analysis dilakukan untuk mengidentifikasi dan mengelompokkan seluruh komponen sistem guna menentukan bagian yang masih dapat digunakan atau perlu direkonstruksi. Kedua, Document Reconstructing bertujuan memperbarui dokumentasi teknis dan fungsional agar sesuai dengan kondisi sistem saat ini. Ketiga, Reverse Engineering digunakan untuk memahami struktur dan logika program dari kode sumber yang ada, terutama ketika dokumentasi tidak tersedia. Keempat, Code Reconstructing dilakukan untuk memperbaiki struktur kode tanpa mengubah fungsinya melalui proses seperti refactoring dan penyederhanaan logika. Kelima, Data Reconstructing fokus pada peningkatan kualitas dan efisiensi basis data dengan normalisasi serta penyesuaian struktur data. Terakhir, Forward Engineering merupakan tahap pembangunan ulang sistem menggunakan teknologi dan arsitektur modern berdasarkan hasil analisis sebelumnya.

III. HASIL DAN PEMBAHASAN

Hasil dan pembahasan berisi data yang disajikan dengan tabel-tabel dan/atau gambar-gambar serta analisis pembahasannya.

A. Inventory Analysis

Analisis terhadap proses bisnis login pada Sistem Informasi Akademik (SIAK) Universitas Langlangbuana menunjukkan bahwa sistem saat ini masih menggunakan metode autentikasi konvensional, yakni dengan mencocokkan username dan password. Pengguna yang berhasil login akan diarahkan ke dashboard sesuai peran masing-masing, seperti mahasiswa, dosen, atau staf administrasi. Namun, sistem ini belum dilengkapi dengan mekanisme keamanan tambahan, seperti autentikasi dua faktor, sehingga membuka potensi risiko keamanan.



Gambar 2 Proses Bisnis Berjalan

Berdasarkan gambar diatas, proses bisnis sistem berjalan dimulai ketika pengguna, seperti mahasiswa, dosen, atau staf, mengakses halaman login dan memasukkan username serta password. Sistem akan memverifikasi username terlebih dahulu; jika tidak ditemukan, pengguna akan diberi notifikasi. Jika username valid, sistem mencocokkan password yang dimasukkan dengan data terenkripsi di basis data.

Permasalahan yang diidentifikasi mencakup tidak adanya proteksi CAPTCHA untuk membedakan manusia dan bot, serta tidak adanya pembatasan jumlah percobaan login yang gagal. Sistem juga belum menerapkan pengiriman kode OTP sebagai lapisan verifikasi tambahan. Hal ini menyebabkan sistem rentan terhadap berbagai bentuk serangan, seperti brute force, credential stuffing, dan akses tidak sah.

Tabel 1 Identifikasi Masalah

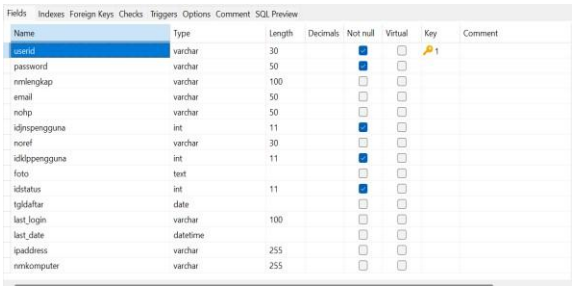
No	Identifikasi Masalah	Deskripsi Masalah	Dampak
1	Autentikasi hanya menggunakan username dan password	Sistem login hanya memverifikasi username dan password tanpa lapisan keamanan tambahan seperti OTP.	Rentan terhadap serangan seperti brute force, credential stuffing, dan akses tidak sah oleh pihak yang memperoleh kredensial secara tidak sah.
2	Tidak ada perlindungan CAPTCHA	Sistem belum menerapkan verifikasi CAPTCHA untuk membedakan antara manusia dan bot saat proses login.	Bot atau skrip otomatis dapat melakukan percobaan login massal tanpa hambatan, meningkatkan risiko serangan otomatis.
3	Tidak ada perlindungan terhadap brute force	Sistem tidak membatasi jumlah percobaan login yang gagal.	Penyerang dapat mencoba kombinasi username dan password secara terus-

No	Identifikasi Masalah	Deskripsi Masalah	Dampak
			menerus tanpa terdeteksi.
4	Tidak ada penggunaan OTP atau 2FA	Sistem tidak mengirimkan kode OTP atau menerapkan autentikasi dua langkah	Jika password berhasil ditebak/dibocorkan, akun langsung dapat diakses tanpa validasi kedua.
5	Sistem tidak membatasi waktu penggunaan OTP	Tidak ada sistem OTP sementara dengan batas waktu aktif dan batas penggunaan.	Sistem tidak mampu membatasi waktu penggunaan OTP, jika diterapkan sembarangan (tanpa waktu kedaluwarsa) berisiko dimanfaatkan kembali oleh penyerang.

B. Reverse Engineering

Reverse engineering dilakukan untuk memahami struktur dan mekanisme kerja sistem login lama yang digunakan dalam Sistem Informasi Akademik. Analisis alur login menunjukkan bahwa proses autentikasi hanya mengandalkan pencocokan username dan password tanpa adanya langkah verifikasi tambahan. Setelah pengguna memasukkan kredensial, sistem langsung memvalidasi data ke database, dan apabila sesuai, pengguna diberikan akses ke dashboard. Jika tidak, sistem hanya memberikan notifikasi kesalahan tanpa perlindungan terhadap percobaan login berulang. Ketiadaan fitur seperti OTP atau pembatasan percobaan login membuat sistem ini rawan terhadap serangan brute force.

Struktur basis data sistem lama juga menunjukkan keterbatasan dari sisi keamanan. Tabel pengguna hanya memuat atribut dasar seperti userid, nmlengkap, password, dan email, tanpa dukungan untuk autentikasi tambahan seperti otp_code, otp_expiry, atau chat_id yang diperlukan untuk pengiriman OTP melalui Telegram.



Gambar 3 Struktur Database

Analisis kode sumber login menguatkan temuan tersebut, di mana verifikasi hanya mencocokkan username dan password menggunakan metode hashing standar. Tidak ada mekanisme tambahan yang membatasi jumlah percobaan login atau mendeteksi aktivitas mencurigakan. Kondisi ini memperjelas perlunya peningkatan sistem keamanan melalui pengembangan sistem login yang dilengkapi autentikasi dua faktor (2FA).

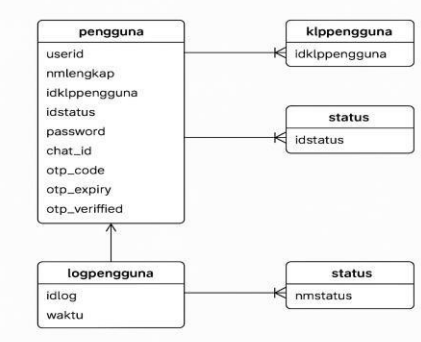
C. Code ReConstruction

Proses rekonstruksi kode dilakukan dengan memperbarui alur login agar tidak hanya berhenti pada verifikasi username dan password, tetapi dilanjutkan dengan pengiriman kode OTP melalui Telegram. Setelah pengguna berhasil melewati tahap autentikasi awal, sistem secara otomatis menghasilkan OTP dan mengirimkannya ke akun Telegram pengguna yang telah terdaftar. Pengguna kemudian diarahkan ke halaman input OTP untuk melanjutkan proses login. Validasi OTP dilakukan dengan mencocokkan input pengguna dengan data yang tersimpan di basis data, serta memastikan bahwa kode tersebut masih berada dalam masa berlaku. Jika OTP valid, pengguna diberikan akses ke sistem; sebaliknya, jika tidak valid atau telah kedaluwarsa, proses login dibatalkan.

Rekonstruksi ini juga disertai penambahan fitur keamanan seperti pembatasan percobaan input OTP dan integrasi CAPTCHA untuk mencegah serangan brute force [8]. Sistem memanfaatkan API Telegram Bot sebagai media pengiriman OTP, yang diatur melalui token dan chat_id pengguna. Integrasi ini tidak hanya meningkatkan keamanan login, tetapi juga memberikan kemudahan dalam distribusi OTP melalui platform yang sudah umum digunakan. Dengan pendekatan ini, autentikasi menjadi lebih kuat karena hanya pengguna yang memiliki akses ke Telegram yang dapat menyelesaikan proses login, sehingga risiko akses tidak sah dapat diminimalkan.

D. Data ReConstruction

Rekonstruksi data dilakukan dengan melakukan perubahan pada struktur tabel pengguna agar dapat mendukung fitur autentikasi dua faktor (2FA) berbasis OTP melalui Telegram. Perubahan ini mencakup penambahan kolom baru seperti chat_id, otp_code, otp_expiry, dan otp_verified yang masing-masing berfungsi untuk menyimpan informasi akun Telegram pengguna, kode OTP yang dikirimkan, masa berlaku kode, serta status verifikasi OTP. Penambahan kolom tersebut memungkinkan sistem menjalankan proses autentikasi tambahan secara lebih aman dan terintegrasi tanpa mengganggu data lama yang telah tersimpan.

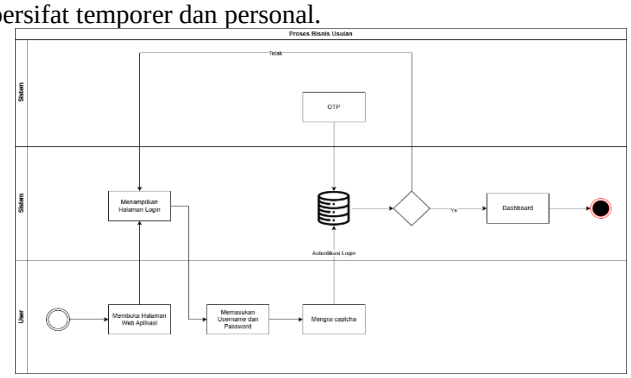


Gambar 4 Perubahan Struktur Database

Selanjutnya dilakukan proses migrasi data dari struktur lama ke struktur baru dengan memastikan bahwa seluruh pengguna memiliki data yang sesuai, terutama pada kolom tambahan untuk kebutuhan 2FA. Proses ini disertai dengan langkah normalisasi untuk menjaga konsistensi dan menghindari duplikasi atau inkonsistensi data. Setelah migrasi selesai, sistem melakukan validasi menyeluruh untuk memastikan integritas data, memastikan bahwa seluruh informasi penting seperti chat_id dan status verifikasi OTP telah terisi dengan benar dan tidak mengalami kerusakan atau kehilangan selama proses migrasi. Validasi ini menjadi tahapan penting agar sistem dapat berjalan dengan baik dan fitur 2FA berfungsi optimal.

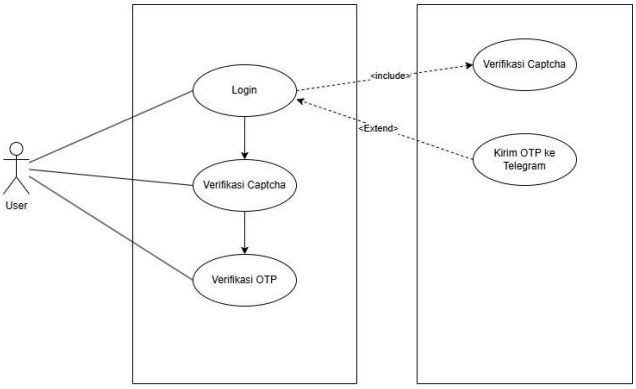
E. Forward Engineering

Proses bisnis usulan dalam sistem login pada Sistem Informasi Akademik Universitas Langlangbuana menerapkan autentikasi dua faktor (2FA) untuk meningkatkan keamanan. Proses dimulai ketika pengguna mengakses halaman login dan memasukkan username serta password. Sebelum proses autentikasi dilakukan, sistem meminta pengguna menyelesaikan tantangan CAPTCHA guna memastikan akses berasal dari manusia, bukan bot. Setelah verifikasi username, password, dan CAPTCHA berhasil, sistem akan mengirimkan kode OTP (One-Time Password) ke akun Telegram pengguna melalui Bot Telegram yang telah terintegrasi. Pengguna kemudian memasukkan kode OTP yang diterima untuk menyelesaikan proses autentikasi. Jika OTP yang dimasukkan valid dan masih berlaku, pengguna diberikan akses ke sistem sesuai perannya. Skema ini dirancang untuk memperkuat keamanan dengan menambahkan lapisan verifikasi yang bersifat temporer dan personal.



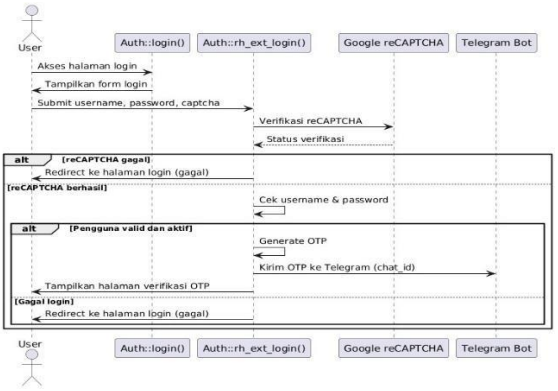
Gambar 4 Proses Bisnis Usulan

Dari sisi pemodelan, use case diagram menggambarkan interaksi antara pengguna dengan sistem melalui tahapan login, verifikasi CAPTCHA, pengiriman OTP, dan verifikasi OTP[9]. Setiap tahapan dijabarkan dalam use case scenario yang mendeskripsikan kondisi awal, interaksi pengguna, serta tanggapan sistem terhadap tindakan pengguna. Diagram sequence menjelaskan urutan proses secara kronologis mulai dari input kredensial, validasi CAPTCHA, verifikasi data login, pengiriman OTP, hingga validasi kode OTP untuk menentukan keberhasilan login.



Gambar 5 *Usecase* Diagram

Diagram sequence menggambarkan alur kerja sistem secara rinci dengan menampilkan interaksi antar komponen berdasarkan urutan waktu. Diagram ini berfungsi untuk membantu perancangan, dokumentasi, dan validasi arsitektur serta logika sistem dengan menunjukkan alur komunikasi antar objek[10]. Dengan visualisasi tersebut, pengembang dapat memahami proses dan hubungan antar bagian sistem secara lebih jelas dari awal hingga akhir dalam satu skenario tertentu.



Gambar 6 Diagram *Sequence*

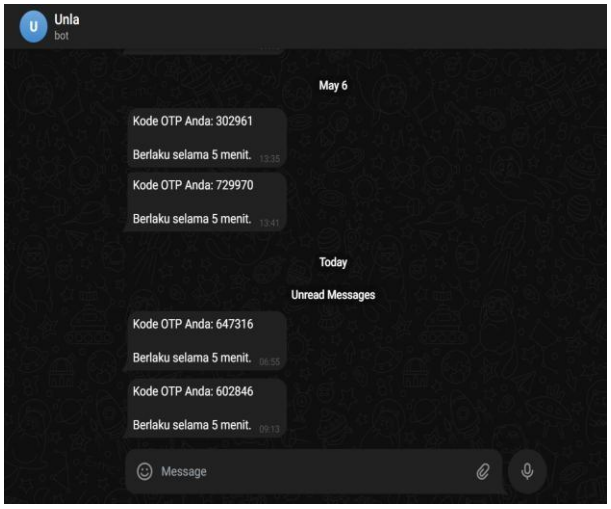
Untuk mendukung struktur sistem, activity diagram digunakan untuk menggambarkan alur kegiatan secara menyeluruh dari awal hingga akhir proses autentikasi. Sedangkan class diagram menunjukkan struktur statis dari sistem dengan menggambarkan relasi antar kelas seperti User, AuthController, dan TelegramBot. Kelas User menangani data pengguna dan status OTP, AuthController mengatur keseluruhan proses autentikasi termasuk validasi CAPTCHA dan OTP, serta TelegramBot bertugas mengirimkan kode OTP melalui API Telegram. Dengan integrasi antar komponen ini, sistem autentikasi dua faktor dapat diterapkan secara efektif dan efisien untuk mencegah akses tidak sah dan meningkatkan perlindungan terhadap data akademik.

Gambar 7 Halaman Login

Validasi CAPTCHA dilakukan melalui API Google reCAPTCHA, dan OTP dikirim secara otomatis menggunakan BotUnla, bot Telegram resmi sistem. OTP bersifat sementara dan hanya berlaku selama beberapa menit. Jika OTP valid, pengguna diarahkan ke dashboard; jika tidak, login ditolak.

Gambar 8 Halaman Input OTP

Tampilan sistem mencakup halaman login, form input OTP, chat bot Telegram untuk pengiriman kode, dan halaman dashboard pengguna. Pengujian dilakukan dengan metode blackbox dan menunjukkan semua fungsi berjalan sesuai harapan, termasuk penolakan akses saat CAPTCHA atau OTP tidak valid, serta pembatasan percobaan OTP untuk mencegah brute force.



Gambar 9 Tampilan Chat Bot Telegram

Pengujian dilakukan untuk memastikan fitur autentikasi dua faktor (2FA) pada Sistem Informasi Akademik berjalan sesuai rancangan dan efektif meningkatkan keamanan akun pengguna [11] .

Tabel 2 Pengujian Sistem

No	Aspek Pengujian	Kebutuhan Fungsional	Skenario Pengujian
1	Proses *login*	Autentikasi pengguna menggunakan userID dan password	- Pengguna melakukan login dengan memasukkan *userid* dan *password.* - Sistem mencocokkan data dengan yang ada di basis data. - Jika sesuai, sistem lanjut ke CAPTCHA.
2	Validasi CAPTCHA	Proteksi terhadap bot login dan brute force	- Setelah memasukkan kredensial, pengguna wajib mengisi CAPTCHA. - Sistem memverifikasi token reCAPTCHA ke server Google - *Jika valid, lanjut ke pengiriman OTP.*
3	Pengiriman OTP	Pengiriman kode OTP ke pengguna yang berhasil login melalui Telegram	- Sistem membangkitkan OTP acak 6 digit. - Sistem mengirimkan OTP ke chat_id Telegram pengguna melalui Bot Telegram. - *Sistem menyimpan OTP dan masa aktif di DB.*
4	Verifikasi OTP	Validasi OTP oleh pengguna sebagai faktor autentikasi kedua.	- Pengguna memasukkan OTP yang dikirim via Telegram. - *Sistem mencocokkan OTP dan masa aktif.* - Jika valid dan belum expired, login berhasil.
5	Pembatasan percobaan OTP	Mencegah brute force terhadap kode OTP	- Pengguna salah memasukkan OTP sebanyak 3 kali. - Sistem memblokir sesi OTP dan menampilkan pesan kesalahan. - Harus login ulang untuk mendapatkan OTP baru.

No	Aspek Pengujian	Kebutuhan Fungsional	Skenario Pengujian
6	Keamanan OTP	Menjamin OTP tidak bisa ditebak atau disalahgunakan,	- Pengujian dilakukan dengan melihat format OTP di database. - OTP disimpan sementara, memiliki expiry, dan tidak disimpan dalam bentuk tetap setelah diverifikasi.

Hasil Pengujian sistem dilakukan dengan metode blackbox testing untuk memastikan bahwa seluruh fitur autentikasi dua faktor (2FA) berbasis OTP melalui Telegram berfungsi sesuai kebutuhan fungsional, dengan cara memberikan input dan mengamati output tanpa melihat kode program secara langsung.

Tabel 3 Hasil Pengujian Sistem

No	Aspek Pengujian	Hasil yang Diharapkan	Hasil Aktual	Status
1	Login dengan username, password, dan captcha valid	Lanjut ke tahap input OTP	Sistem menampilkan halaman input OTP	Berhasil
2	Login dengan username dan password benar, tetapi captcha salah	Sistem menolak login dan menampilkan pesan kesalahan captcha	Sistem menolak login dan menampilkan pesan error pada captcha	Berhasil
3	Masukkan OTP salah 3x	Sistem memblokir proses OTP dan meminta pengguna login ulang	OTP diblokir, pengguna harus melakukan login ulang dari awal	Berhasil

IV. SIMPULAN

Berdasarkan penyusunan laporan yang telah dikerjakan adapun kesimpulan yang dapat dicapai antara lain:

1. Penelitian ini berhasil mengidentifikasi kerentanan pada form login SIAK, khususnya terhadap serangan credential stuffing, yang terjadi karena sistem sebelumnya hanya menggunakan autentikasi satu faktor berupa kombinasi username dan password tanpa pelindung tambahan. Hasil analisis menunjukkan bahwa form login rentan terhadap penyalahgunaan kredensial yang bocor atau dicoba secara otomatis oleh bot.
2. Implementasi autentikasi dua faktor (2FA) berhasil meningkatkan keamanan form login, dengan menambahkan proses verifikasi kode OTP melalui Telegram setelah pengguna berhasil memasukkan username dan password yang valid. Penggunaan metode ini secara efektif menutup celah keamanan yang sebelumnya dapat dimanfaatkan oleh pihak tidak berwenang, serta berkontribusi dalam menjaga integritas data akademik seperti nilai mahasiswa dari perubahan tanpa otorisasi.

REFERENSI

[1] Yusuf Heriyanto, Anas Azhimi Qalban, and Iif Alfiatul Mukaromah, "Pengembangan Metode Login Two Factor Authentication (2FA) untuk Keamanan Sistem Informasi Akademik," *Journal of Innovation Information Technology and Application (JINITA)*, vol. 4, no. 2, pp. 142–150, Dec. 2022, doi: 10.35970/jinita.v4i2.1637.

[2] K. Mubarok and Moh. A. Romli, "Implementasi Metode Rule Based dalam Mendeteksi Serangan Brute Force pada Owncloud," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 5, no. 1, pp. 159–167, Dec. 2024, doi: 10.57152/malcom.v5i1.1701.

[3] J. Teknika and C. Anwar, "Implementasi Algoritma OTP dan HMAC untuk Two-Factor Authentication Sistem Login Relawan Pemilu," *IJCCS*, vol. x, No.x, pp. 1–5, Sep. 2024.

[4] M. Irfan and M. A. Khan, "Cryptographically Secure Pseudo-Random Number Generation (CS-PRNG) Design using Robust Chaotic Tent Map (RCTM)," Aug. 2024, [Online]. Available: http://arxiv.org/abs/2408.05580

[5] D. B. Adiputra, H. J. Setyadi, and V. Z. Kamila, "Perancangan Manajemen Bandwidth Menggunakan Metode Simple Queue dan Firewall Filtering pada Mikrotik di SMK Negeri 1 Tenggarong," *Kreatif Teknologi dan Sistem Informasi (KRETISI)*, vol. 2, no. 2, pp. 08–14, Dec. 2024, doi: 10.30872/kretisi.v2i2.1614.

[6] Desima Natasya Simatupang and Rika Astuti, "Model Rapid Application Development (RAD) Untuk Rancang Bangun Sistem Informasi Monitoring Project Pada Branch Business Process Re-Engineering (BBPR) Team," 2023.

[7] H. Priambodo and A. Muhajirin, "Perancangan ChatBot Pendaftaran Siswa Dengan Telegram BOT Design a Chatbot for Student Registration Using Telegram BOT," *Journal of Information and Information Security (JIFORTY)*, vol. 3, no. 1, p. 73, 2022, [Online]. Available: https://www.businessofapps.com/data/telegram-statistics/,

[8] H. Raka Herdiantoro, M. Reza Redo Islami, T. Informatika, S. Dharma Wacana Metro Jl Kenanga No, K. Metro Bar, and K. Metro, "IMPLEMENTASI TWO-FACTOR AUTHENTICATION (2FA) DAN FIREWALL POLICIES DALAM MENGAMANKAN WEBSITE," vol. 4, no. 1, pp. 1–9, 2023.

[9] E. Epitavio Belo, D. Pramana Hostiadi, M. Azman Maricar, S. Informasi, and S. Komputer, "Prosiding Seminar Hasil Penelitian Informatika dan Komputer," ■ *SPINTER*, vol. 1, no. 3, p. 2024, 2024.

[10] T. Arianti, A. Fa'izi, S. Adam, M. Wulandari, and P. ' Aisyiyah Pontianak, "PERANCANGAN SISTEM INFORMASI PERPUSTAKAAN MENGGUNAKAN DIAGRAM UML (UNIFIED MODELLING LANGUAGE)," 2022.

[11] Nadia Julian Dewi, Arizona Firdonsyah, and Danur Wijayanto, "Two factor authentication pada sistem login rekam medis elektronik berbasis web menggunakan metode prototype," Feb. 2025.