Penerapan Sistem Keamanan Berlapis untuk Otentikasi Pengguna Website Menggunakan Metode Two-Factor Authentication (2FA) Berlapis Aplikasi Google Authenticator

Abiyyu Rivanza[1], Aswandi [2*], Afla Nevrisa[3]

[1,2,3] *Jurusan Teknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe*
Jln. B.Aceh Medan Km.280 Buketrata 24301 INDONESIA
[2]aswandi@pnl.ac.id

***Abstrak*— Keamanan sistem autentikasi pada website menjadi aspek penting untuk mencegah potensi penyalahgunaan akun akibat pencurian kata sandi. Penelitian ini bertujuan untuk menerapkan metode Two-Factor Authentication (2FA) berbasis Google Authenticator serta menganalisis performa website pada halaman login. Selain itu, penelitian ini juga mengintegrasikan Telegram Bot sebagai media notifikasi untuk memberikan pemberitahuan secara real-time kepada pengguna terkait aktivitas login, sehingga meningkatkan aspek keamanan dan monitoring. Metode penelitian dilakukan dengan mengimplementasikan 2FA menggunakan kode OTP berbasis waktu (Time-Based One Time Password/TOTP) yang terintegrasi dengan Google Authenticator, serta menguji kinerja website melalui pengukuran waktu respon dan throughput. Hasil penelitian menunjukkan bahwa penerapan 2FA berhasil meningkatkan keamanan autentikasi dengan menambahkan lapisan verifikasi tambahan yang hanya dapat diakses pengguna melalui perangkat pribadi, sedangkan integrasi Telegram Bot mampu memberikan notifikasi cepat dan akurat kepada pengguna. Dari sisi performa, pengujian menunjukkan bahwa website mampu memberikan waktu respon rata-rata yang stabil dan throughput yang memadai, sehingga sistem tetap dapat diakses dengan nyaman tanpa mengalami penurunan kinerja.**
Kata Kunci : Google Authenticator, Keamanan Sistem, Telegram Bot, Two-Factor Authentication, Waktu Respon.

Abstract*— *The security of authentication systems on websites is a crucial aspect to prevent potential account misuse due to password theft. This study aims to implement a Two-Factor Authentication (2FA) method based on Google Authenticator and analyze the website's performance on the login page. In addition, this research integrates a Telegram Bot as a notification medium to provide real-time alerts to users regarding login activities, thereby enhancing security and monitoring aspects. The research method involves implementing 2FA using a time-based one-time password (TOTP) integrated with Google Authenticator and testing website performance by measuring response time and throughput. The results show that the implementation of 2FA successfully enhances authentication security by adding an extra verification layer accessible only through the user's personal device, while the integration of the Telegram Bot provides fast and accurate notifications to users. In terms of performance, the tests indicate that the website maintains a stable average response time and adequate throughput, ensuring that the system remains accessible and performs smoothly without degradation.
Keywords **:Google Authenticator, System Security, Telegram Bot, Two-Factor Authentication, Response Time.**

I. Pendahuluan

*E*ra digital yang saat ini disebut dengan era society 5.0 merupakan upaya umat manusia untuk melakukan aktifitas apapun secara mudah secara online. Transformasi layanan yang begitu marak ke ranah online oleh pengguna internet telah meningkatkan kebutuhan akan autentikasi yang lebih baik. Pengguna sekarang perlu mengelola kemampuan mereka dalam mengelola dan mengingat sandi yang digunakan. Perangkat lunak browser khusus yang memiliki kemampuan pengelola kata sandi dapat menjadi solusi, dan pengelola kata sandi dapat memperburuk situasi dalam kasus tertentu. Era sekarang sudah umum bagi pengguna untuk menggunakan kemampuan pengelolaan sandi yang disediakan oleh browser sehingga dapat menimbulkan konsekuensi serius jika aplikasi tersebut tidak berada pada device pribadi pengguna. Metode keamanan two-factor authentication (2FA) diusulkan untuk mengatasi isu penanggulangan sisi server untuk mencegah pencurian kata sandi. (Heriyanto, Y., dkk., 2022). Penelitian sebelumnnya telah mengungkapan bagaimana pemanfaatan metode 2FA terhadap sistem informasi mereka. Model yang pertama adalah physically uncloneable functions (PUFs) yang digunakan untuk ketahanan dan efisiensi sistem terhadap serangan cyber. Model berikutnya penggabungan physically uncloneable functions (PUFs) dan voiceprint yang disebut dengan metode transparent two-factor authentication (T2FA) untuk memberikan pengguna kenyamanan serta rasa aman saat berinteraksi diranah digital. Penelitian berikutnya adalah pengembangan model keamanan dengan mengembangkan sound-proof yang dapat dengan mudah digunakan melalui smartphone dan browser utama tanpa plugin. Masih banyak lagi penelitian yang berkaitan dengan 2FA untuk meningkatkan keamanan penggunaan sistem informasi. Penelitian ini mengusulkan pemanfaatan metode 2FA sebagai solusi tantangan terhadap keamanan sistem website. (Heriyanto, Y., dkk., 2022). Metode 2FA diusulkan sebagai jawaban dari isu keamanan sistem, yang berfokus pada pengamanan sistem website pada bagian awal penggunaan

sistem yang diharapkan dapat mengantisipasi langkah lanjutan kejahatan cyber jika sudah bisa masuk ke dalam dashboard pengguna. Berkolaborasi dengan model one time password (OTP) melalui aplikasi Telegram dan model autentikasi kalkulasi, maka keamanan sistem informasi akademik diharapkan akan lebih baik dan dapat memberikan kenyamanan kepada pengguna kaitan dengan kewajiban untuk menjaga sandi dan akun pengguna. (Heriyanto, Y., dkk., 2022).

II. Metodologi Penelitian

A. *Metode dan Variabel Penelitian*

Penelitian ini menggunakan metode eksperimen dengan pendekatan pengembangan sistem (system development). Metode ini dipilih karena sesuai dengan tujuan penelitian, yaitu merancang dan mengimplementasikan sistem keamanan berlapis Two-Factor Authentication menggunakan Google Authenticator pada sebuah website. Melalui metode eksperimen, sistem yang dibangun diuji secara langsung untuk menilai efektivitas penerapan autentikasi dua faktor dalam meningkatkan keamanan login pengguna. Adapun variabel dalam penelitian ini terdiri dari variabel bebas, yaitu metode autentikasi dua faktor yang diterapkan pada sistem, serta variabel terikat berupa tingkat keamanan otentikasi pengguna yang diukur dari keberhasilan mencegah login tidak sah dan penyalahgunaan akun.

B. *Data dan Pengumpulan Data*

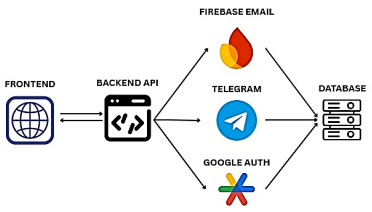
Data yang digunakan dalam penelitian ini berasal dari dua jenis sumber, yaitu data primer dan data sekunder. Data primer diperoleh melalui proses implementasi dan pengujian sistem secara langsung, seperti hasil log aktivitas login, hasil verifikasi OTP, serta hasil pengujian fungsional dan keamanan. Sementara itu, data sekunder diperoleh dari studi literatur berupa jurnal, artikel ilmiah, buku, serta dokumentasi teknis yang berkaitan dengan konsep Two-Factor Authentication, Flask Framework, Firebase, dan Google Authenticator. Teknik pengumpulan data dilakukan melalui beberapa cara, yaitu observasi langsung terhadap hasil implementasi sistem, dokumentasi terhadap rancangan sistem serta hasil pengujian, serta uji coba sistem dengan beberapa skenario untuk mendapatkan data yang objektif.

C. *Rancangan Sistem (Hardware/Software)*

Dalam penelitian yang berjudul "Penerapan Sistem Keamanan Berlapis untuk Otentikasi Pengguna Website Menggunakan Metode Two-Factor Authentication Berbasis Aplikasi Google Authenticator", digunakan beberapa perangkat dan sistem operasi baik secara fisik maupun virtual. Sistem utama yang digunakan untuk pengembangan dan pengujian terdiri dari laptop pribadi, layanan firebase sebagai basis penyimpanan data berbasis cloud, serta integrasi aplikasi autentikasi pihak ketiga seperti Google Authenicator dan Telegram API. Perangkat pertama adalah laptop Lenovo 82LM yang digunakan sebagai komputer utama dalam merancang, mengembangkan, sekaligus menguji sistem. Laptop ini memiliki spesifikasi prosesor AMD Ryzen 5 5500U with Radeon Graphics dengan 6 core dan 12 thread berkecepatan dasar ~2,1 GHz, memori RAM 8 GB DDR4, kartu grafis terintegrasi AMD Radeon Graphics dengan total memory 4 GB, serta media penyimpanan berbasis SSD internal. Sistem operasi yang digunakan adalah Windows 11 Home Single Language 64-bit dengan dukungan DirectX 12. Spesifikasi ini dipilih karena mampu memberikan performa yang stabil dalam pengembangan aplikasi web menggunakan Framework Flask Python, pengolahan data melalui Firebase, serta integrasi dengan layanan keamanan eksternal. Selanjutnya, digunakan Firebase Firestore Database sebagai sistem penyimpanan data utama yang berbasis cloud. Firebase dipilih karena kemampuannya dalam menyimpan, mengelola, dan menyinkronkan data pengguna secara real-time dengan tingkat keamanan yang baik. Selain itu, penelitian ini juga menggunakan integrasi SMTP (Simple Mail Transfer Protocol) untuk mengirimkan kode OTP melalui email, serta Telegram API untuk mengirimkan kode OTP secara instan melalui bot Telegram. Selain layanan tersebut, digunakan pula aplikasi Google Authenticator yang berjalan pada perangkat seluler untuk menghasilkan kode autentikasi berbasis Time-Based One Time Password. Google Authenticator berperan sebagai faktor kedua autentikasi dalam sistem login, sehingga memberikan lapisan keamanan tambahan pada website yang dibangun. Dengan konfigurasi perangkat keras, perangkat lunak, serta layanan eksternal tersebut, penelitian ini mampu menjalankan proses perancangan, implementasi, serta pengujian terhadap efektivitas metode keamanan berlapis berbasis 2FA dalam menjaga keamanan otentikasi pengguna website.

1) *Arsitektur Sistem*

Arsitektur sistem yang dirancang terdiri dari tiga komponen utama, yaitu pengguna (client), server aplikasi, dan layanan eksternal. User melakukan registrasi dan login melalui antarmuka website berbasis Flask Python. Server aplikasi berfungsi sebagai pengolah utama yang menangani proses autentikasi, enkripsi data, dan pengelolaan database. Sistem terintegrasi dengan layanan eksternal seperti Firebase untuk penyimpanan data, layanan SMTP untuk mengirim OTP melalui email, Telegram API untuk mengirimkan OTP melalui pesan instan, serta Google Authenticator untuk menghasilkan kode OTP berbasis Time-Based One Time Password. Dengan arsitektur ini, sistem dapat memberikan fleksibilitas kepada pengguna dalam memilih metode autentikasi yang aman. Gambaran umum arsitektur sistem dapat dilihat pada gambar 1 berikut.



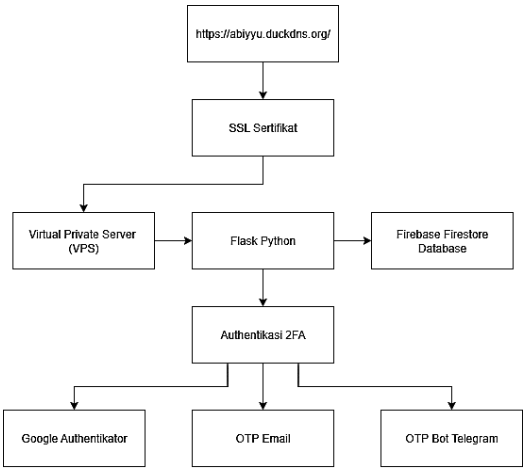
Gambar 1. Gambaran Umum Arsitektur Sistem

Gambar 1 menunjukkan arsitektur sistem yang digunakan dalam penelitian. Sistem terdiri dari beberapa komponen utama yang saling terhubung, yaitu Frontend, Backend API, serta layanan autentikasi eksternal seperti Firebase Email, Telegram API, dan Google Authenticator, yang semuanya terintegrasi dengan Database. Pada sisi Frontend, pengguna melakukan interaksi langsung melalui antarmuka website, baik untuk registrasi, login maupun penggunaan fitur aplikasi. Permintaan dari Frontend kemudian diteruskan ke Backend API yang berfungsi sebagai pengolah utama logika sistem, termasuk validasi data pengguna, pengelolaan autentikasi, serta komunikasi dengan layanan eksternal. Backend API terhubung dengan Firebase Email untuk mengirimkan kode verifikasi OTP melalui email, dengan Telegram API untuk mengirimkan OTP melalui bot Telegram, serta dengan Google Authenticator untuk menghasilkan kode berbasis Time-Based One Time Password. Semua hasil autentikasi, baik dari email, Telegram, maupun Google Authenticator, kemudian dicatat dan diverifikasi melalui Database yang menjadi pusat penyimpanan data pengguna. Adapun integrasi sistem yang mendukung layanan eksternal untuk mendukung fungsionalitas dan keamanan, yaitu:

- Firebase, Digunakan untuk mengelola pengiriman email, termasuk verifikasi email dan notifikasi terkait aktivitas pengguna.
- Email Service, Berperan dalam mengirimkan informasi penting kepada pengguna, seperti konfirmasi pendaftaran dan pemberitahuan keamanan.
- Telegram API, Dimanfaatkan untuk mengirimkan notifikasi melalui bot Telegram, sehingga pengguna mendapatkan informasi secara real-time mengenai aktivitas yang terjadi pada akun pengguna.
- Google Authenticator, Digunakan sebagai metode Two-Factor Authentication. Layanan ini menghasilkan kode OTP (One-Time Password) berbasis waktu yang harus dimasukkan oleh pengguna setelah proses login untuk meningkatkan keamanan akun.

2) Blok Diagram

Pada bagian ini representasi sistem melalui blok diagram yang menggambarkan arsitektur dan hubungan antar komponen dalam sistem yang dikembangkan. Blok diagram dirancang untuk memberikan gambaran jelas tentang bagaimana Frontend berinteraksi dengan Backend API, serta bagaimana Backend API terhubung dengan layanan pendukung seperti Telegram, Google Authenticator, Firebase Email, dan Database. Blok diagram dapat dilihat pada gambar 2 berikut.



Gambar 2. Diagram Blok NAC

Gambar 2 menampilkan blok diagram sistem yang menggunakan domain https://abiyyu.duckdns.org/ sebagai titik akses utama yang dilindungi oleh SSL Certificate. Implementasi SSL/TLS ini berfungsi sebagai protokol keamanan yang mengenkripsi komunikasi antara klien dan server, memastikan bahwa seluruh transaksi data terjadi dalam lingkungan yang aman dan terproteksi. Infrastruktur hosting dibangun di atas Virtual Private Server yang memberikan kontrol penuh terhadap lingkungan server dan memungkinkan kustomisasi konfigurasi keamanan sesuai dengan kebutuhan spesifik aplikasi. Flask Python diimplementasikan sebagai framework web yang menjalankan logika utama aplikasi. Flask dipilih karena sifatnya yang ringan namun powerful, memberikan fleksibilitas tinggi dalam pengembangan aplikasi web. Framework ini bertanggung jawab untuk menangani request HTTP, memproses logika bisnis, dan mengelola komunikasi dengan berbagai komponen sistem lainnya. Untuk penyimpanan dan pengelolaan data, sistem menggunakan Firebase Firestore Database sebagai database NoSQL berbasis cloud. Firestore dipilih karena kemampuannya dalam menyediakan real-time synchronization, scalability yang tinggi, dan integrasi yang seamless dengan berbagai platform. Komponen paling kritis dalam arsitektur ini adalah implementasi Autentikasi 2FA (Two-Factor Authentication) yang dirancang dengan tiga metode verifikasi berbeda untuk memberikan lapisan keamanan:

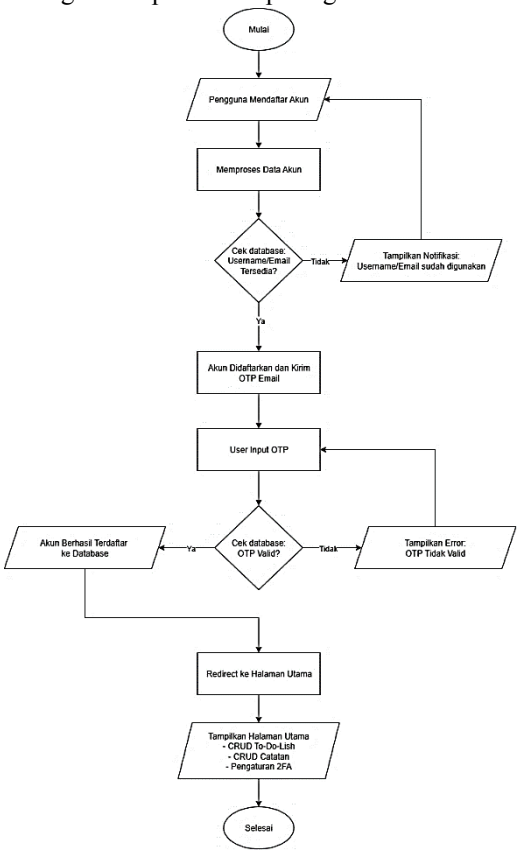
- Google Authenticator: Menggunakan Time-based One-Time Password algorithm yang menghasilkan kode verifikasi berbasis waktu. Metode ini memberikan keamanan tinggi karena kode yang dihasilkan bersifat sementara dan unik untuk setiap sesi autentikasi.
- OTP Email: Sistem mengirimkan One-Time Password melalui email yang telah didaftarkan pengguna. Metode ini memberikan layer verifikasi tambahan melalui saluran komunikasi yang terpisah dari aplikasi utama.
- OTP Bot Telegram: Integrasi dengan Telegram bot memungkinkan pengiriman kode OTP melalui platform messaging yang populer dan aman. Implementasi ini

memberikan alternatif yang user-friendly sekaligus maintating tingkat keamanan yang tinggi.

Arsitektur multi-faktor ini dirancang untuk menerapkan prinsip something you know, something you have, and something you are dalam konteks autentikasi digital, dimana kombinasi metode verifikasi ini secara signifikan mengurangi risiko unauthorized access dan meningkatkan postur keamanan sistem secara keseluruhan. Integrasi seluruh komponen ini menciptakan ekosistem keamanan yang holistik, dimana setiap lapisan saling mendukung untuk memberikan proteksi maksimal terhadap berbagai ancaman keamanan siber yang mungkin dihadapi dalam lingkungan digital kontemporer.

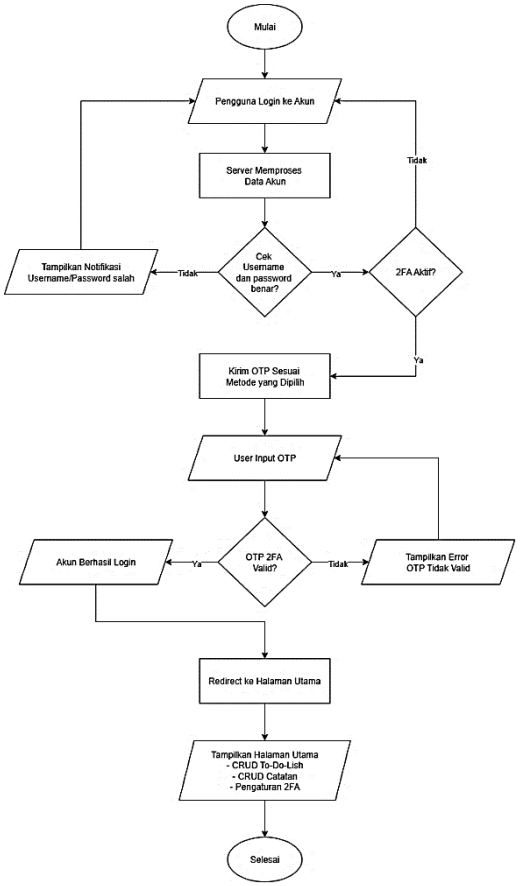
3) Tahapan Penelitian

Alur pelaksanaan penelitian secara sistematis, disusun sebuah flowchart yang menguraikan tahapan-tahapan dari awal hingga akhir penelitian. Flowchart ini menunjukkan urutan proses mulai dari studi literatur, perancangan sistem. Flowchart register dapat dilihat pada gambar 3 berikut.



Gambar 3. Flowchart Register

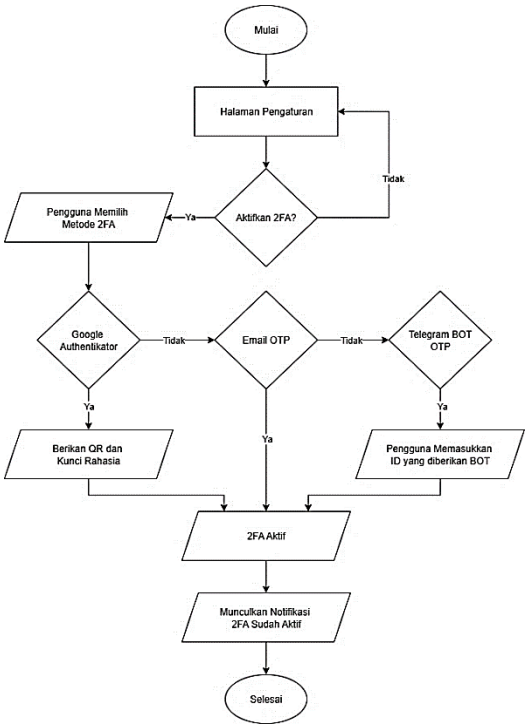
Gambar 3 menampilkan alur proses pendaftaran akun pada sistem. Proses dimulai ketika pengguna melakukan registrasi dengan mengisi data akun. Sistem kemudian memproses data tersebut dan melakukan pengecekan pada database untuk memastikan apakah username atau email yang dimasukkan sudah terdaftar sebelumnya. Jika data sudah ada, maka sistem akan menampilkan notifikasi bahwa username atau email telah digunakan. Namun, apabila data belum terdaftar, sistem akan membuat akun baru sekaligus mengirimkan kode OTP melalui email. Selanjutnya, pengguna diminta memasukkan OTP yang telah diterima. OTP yang diinput akan diverifikasi pada database untuk memastikan validitasnya. Apabila OTP tidak valid, maka sistem akan menyimpan data pengguna ke dalam database. Setelah itu, pengguna akan diarahkan menuju halaman utama yang berisi fitur CRUD To-Do-List, CRUD catatan, serta pengaturan Two-Factor Authentication (2FA). Proses registrasi ini berakhir ketika pengguna berhasil masuk ke halaman utama. Flowchart login menggambarkan alur proses autentikasi pengguna ketika mengakses sistem. Proses ini disusun untuk memastikan bahwa data akun yang dimasukkan telah diverifikasi dengan benar, serta memberikan lapisan keamanan tambahan melalui Two-Factor Authentication apabila fitur tersebut diaktifkan. Flowchart login dapat dilihat pada gambar 4 berikut.



Gambar 4. Flowchart Login

Gambar 4 menampilkan proses yang diawali ketika pengguna memasukkan username dan password. Server kemudian memproses data tersebut dan melakukan pengecekan terhadap kesesuaian data dengan database. Apabila username dan password tidak sesuai, sistem akan menampilkan notifikasi kesalahan. Jika data benar, sistem memeriksa status aktivasi 2FA. Bagi akun yang tidak

mengaktifkan 2FA, pengguna dapat langsung diarahkan ke halaman utama. Namun, jika 2FA aktif, sistem akan mengirimkan kode OTP sesuai metode yang dipilih pengguna, kemudian pengguna diwajibkan memasukkan kode OTP tersebut. Kode OTP yang valid akan memberikan akses login dan mengarahkan pengguna ke halaman utama yang menyediakan fitur CRUD ¬To-Do-List, CRUD catatan, serta pengaturan 2FA. Sebaliknya, jika OTP tidak valid, sistem akan menampilkan pesan kesalahan. Proses aktivasi Two-Factor Authentication pada sistem dilakukan melalui halaman pengaturan akun. Pada tahap ini, pengguna diberikan pilihan untuk mengaktifkan fitur keamanan tambahan dan menentukan metode autentikasi yang akan digunakan sesuai kebutuhan. Flowchart 2FA dapat dilihat pada gambar 5 berikut.



Gambar 5. Flowchart 2FA

Gambar 5 menampilkan proses diawali dari halaman pengaturan akun. Pengguna dapat memilih untuk mengaktifkan fitur 2FA atau tidak. Jika tidak diaktifkan, sistem akan kembali ke halaman pengaturan. Namun, apabila 2FA diaktifkan, pengguna diminta menentukan metode autentikasi yang akan digunakan. Terdapat tiga pilihan metode, yaitu Google Authenticator, Email OTP, dan Telegram BOT OTP. Jika pengguna memilih Google Authenticator, sistem akan memberikan QR code dan kunci rahasia untuk dihubungkan ke aplikasi Google Authenticator. Apabila memilih Email OTP, sistem akan mengirimkan kode OTP melalui email. Sedangkan jika memilih Telegram BOT, pengguna harus memasukkan ID yang diberikan oleh bot Telegram untuk menerima OTP. Setelah salah satu metode berhasil diaktifkan, sistem akan mencatat bahwa 2FA telah aktif dan menampilkan notifikasi bahwa fitur tersebut sudah digunakan. Dengan demikian, proses aktivasi 2FA selesai dan akun pengguna memperoleh lapisan keamanan tambahan.

4) Teknik Pengujian

Pengujian sistem dilakukan dengan metode Blackbox Testing untuk memverifikasi fungsionalitas utama seperti registrasi, login, aktivasi 2FA, serta penggunaan OTP melalui Google Authenticator, Email, dan Telegram. Selain itu, dilakukan uji keamanan dengan mencoba login tidak sah, penggunaan OTP salah atau kadaluwarsa, dan upaya akses tanpa 2FA. Pengujian ini bertujuan memastikan sistem berjalan sesuai kebutuhan sekaligus mampu mencegah akses ilegal.

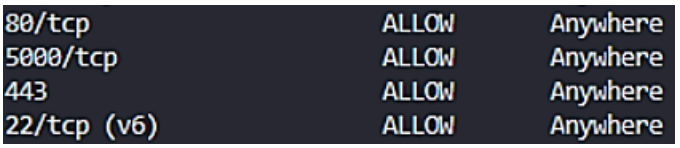
III. Hasil dan Pembahasan

Pada tahap ini, diuraikan tentang hasil dan pembahasan aplikasi yang berupa Hasil Tampilan *User Interfaces*, Hasil Pengujian Sistem dan Hasil Pengujian Akurasi Metode.

A. Hasil Penelitian

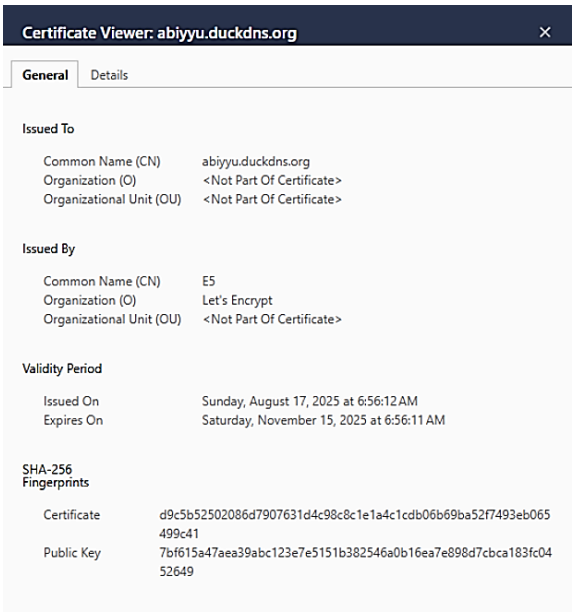
Hasil penelitian menunjukkan bahwa sistem keamanan berlapis berhasil diimplementasikan pada website menggunakan Flask Python dan Firebase. Proses registrasi dilengkapi verifikasi email, sedangkan login ditambahkan autentikasi dua faktor dengan tiga opsi, yaitu Google Authenticator, Telegram OTP, dan email OTP. Selain itu, sistem juga menyediakan dashboard dengan fitur CRUD catatan dan todolist serta pengaturan keamanan 2FA.

Konfigurasi sistem dilakukan pada VPS. Website Flask Python awalnya dijalankan melalui port 5.000 untuk pengujian, kemudian dipindahkan ke port 443 dengan dukungan SSL/HTTPS agar dapat diakses secara aman melalui IP publik. Firewall VPS diatur hanya membuka port yang diperlukan sehingga akses website lebih terkontrol dan aman. Konfigurasi firewall pada VPS untuk mengaktifkan port yang diperlukan dapat dilihat pada gambar 6 berikut.



Gambar 6. Konfigurasi Firewall pada VPS

Gambar 6 menampilkan status firewall dalam kondisi aktif dengan port yang sudah diizinkan, port 5000/tcp dan 443/tcp. Hal ini menunjukkan bahwa VPS telah siap digunakan baik untuk pengujian website maupun untuk akses publik melalui protokol HTTPS dengan sertifikat SSL, sehingga keamanan komunikasi data pengguna dapat terjaga. Sertifikat SSL dapat dilihat pada gambar 7 berikut.



Gambar 7. Sertifikat SSL

Gambar 7 menampilkan domain penelitian abiyyu.duckdns.org telah berhasil terpasang setifikat SSL. Keberhasilan pemasangan sertifikat menunjukkan bahwa konfigurasi pada port 443 telah berjalan dengan baik dan koneksi antara server dan pengguna kini terenkripsi.

B. Pembahasan Penelitian

Pembahasan penelitian ini difokuskan pada efektivitas penerapan autentikasi dua faktor 2FA dalam sistem login website. Implementasi melalui email, Telegram, dan Google Authenticator menunjukkan bahwa mekanisme keamanan tambahan ini mampu memberikan perlindungan lebih baik serta kestabilan akses pengguna.

Pengujian fungsionalitas sistem Two-Factor Authentication dilaksanakan menggunakan metode Black Box Testing untuk mengevaluasi kesesuaian implementasi fitur dengan spesifikasi kebutuhan fungsional yang telah ditetapkan. Pendekatan black box dipilih karena fokus pengujian diarahkan pada validasi input-output sistem tanpa mempertimbangkan struktur kode internal, sehingga dapat memberikan perspektif end-user yang objektif terhadap performa sistem autentikasi. Dataset pengujian terdiri dari sepuluh akun pengguna dengan konfigurasi username dan password yang bervariasi untuk memastikan representativitas skenario penggunaan yang beragam. Setiap akun diuji melalui tiga metode autentikasi sekunder yang berbeda, yaitu One-Time Password melalui email, OTP melalui bot Telegram, dan OTP melalui aplikasi Google Authenticator. Dataset akun dapat dilihat pada tabel 1 berikut.

Tabel 1. Dataset Akun

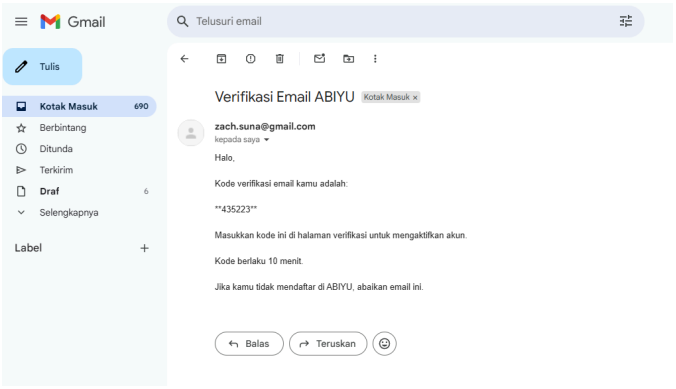
No	*Username*	*Password*
1	Achyar	11223344
2	Zulfikar	11223344
3	Abiyyu	12345
4	Imam	112233
5	Hidayat	112233
6	Fikar	112233
7	Zulfi	112233
8	Zach	112233
9	Zulah	112233
10	Alip	112233

Tabel 1 menampilkan daftar akun uji yang digunakan dalam proses pengujian sistem. Setiap akun memiliki kombinasi username dan password yang berbeda sehingga dapat mempresentasikan berbagai skenario login. Dataset berfungsi sebagai acuan untuk memastikan bahwa mekanisme autentikasi dua faktor dapat diuji secara konsisten pada setiap akun pengguna yang terdaftar. Hasil pengujian OTP melalui email dapat dilihat pada tabel 2 berikut.

Tabel 2. Hasil Pengujian OTP Melalui Email

Kode Uji	**Rincian Pengujian**	**Hasil yang Diharapkan**	**Pengguna**	**Keterangan**
01	Pengguna *login* menggunakan *username* dan *password*, OTP melalui email terkirim	Kode OTP melalui email berhasil terkirim dan pengguna berhasil *login*	1	Berhasil
			2	Berhasil
			3	Berhasil
			4	Berhasil
			5	Berhasil
			6	Berhasil
			7	Berhasil
			8	Berhasil
			9	Berhasil
			10	Berhasil

Tabel 2 menampilkan pengujian kode 01 mengevaluasi fungsionalitas pengiriman dan validasi OTP melalui layanan email. Hasil pengujian menunjukkan tingkat keberhasilan 100% (10/10 akun) dalam proses pengiriman kode OTP ke alamat email yang terdaftar. Tidak ditemukan adanya kegagalan pengiriman email atau error dalam proses validasi kode yang diinputkan oleh pengguna. Adapun tampilan notifikasi OTP terkirim pada email dapat dilihat pada gambar 8 berikut.



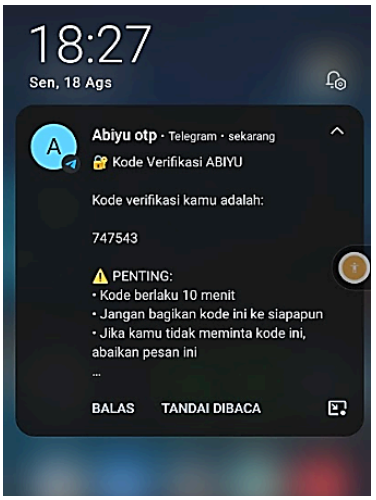
Gambar 8. Tampilan OTP Melalui Email

Gambar 8 menampilkan antarmuka email yang diterima oleh pengguna. Email tersebut berasal dari pengirim zach.suna@gmail.com dengan subjek verifikasi email ABIYU. Di dalam email, terdapat kode verifikasi berjumlah enam digit, yaitu 435223. Teks dalam email juga memberikan instruksi kepada pengguna untuk memasukkan kode tersebut pada halaman verifikasi akun di situs web. Hasil pengujian OTP melalui bot Telegram dapat dilihat pada tabel 3 berikut.

Tabel 3. Hasil Pengujian OTP Melalui Bot Telegram

Kode uji	Rincian Pengujian	Hasil yang Diharapkan	Pengguna	Keterangan
02	Pengguna *login* menggunakan *username* dan *password*, OTP melalui bot telegram terkirim	Kode OTP melalui bot telegram terkirim dan pengguna berhasil *login*	1	Berhasil
			2	Berhasil
			3	Berhasil
			4	Berhasil
			5	Berhasil
			6	Berhasil
			7	Berhasil
			8	Berhasil
			9	Berhasil
			10	Berhasil

Tabel 3 menampilkan evaluasi fungsionalitas OTP melalui bot Telegram (kode pengujian 02) mendemonstrasikan performa yang identik dengan metode email, yakni mencapai success rate 100% untuk seluruh sampel akun pengujian. Setiap pengguna berhasil menerima kode OTP melalui bot Telegram yang telah dikonfigurasi dan dapat menggunakan kode tersebut untuk menyelesaikan proses login. Hasil ini memvalidasi efektivitas implementasi Telegram Bot API dalam arsitektur sistem 2FA. Kestabilan koneksi dengan server Telegram, akurasi pengiriman pesan, dan sinkronisasi waktu kode OTP telah memenuhi standar operasional yang ditetapkan. Tidak terjadi timeout atau failure dalam komunikasi antara sistem dengan Telegram Bot API selama periode pengujian. Adapun tampilan notifikasi OTP terkirim pada Telegram bot dapat dilihat pada gambar 9 berikut.



Gambar 9. Tampilan OTP Melalui Telegram Bot

Gambar 9 menunjukkan notifikasi yang diterima pengguna. Notifikasi tersebut berasal dari akun Telegram bernama ABIYU OTP dan memiliki judul kode verifikasi ABIYU. Di dalam notifikasi, terdapat informasi kode verifikasi yang terdiri dari enam digit, yaitu 747543. Selain itu, notifikasi juga menyertakan peringatan penting yang menggarisbawahi masa berlaku kode 10 menit dan instruksi keamanan untuk tidak membagikan kode tersebut kepada siapa pun. Hasil pengujian Google Authenticator dapat dilihat pada tabel 4 berikut.

Tabel 4. Hasil Pengujian Google *Authenticator*

Kode uji	Rincian Pengujian	Hasil yang Diharapkan	Pengguna	Keterangan
03	Pengguna *login* menggunakan *username* dan *password*, Aplikasi Google Authentikator memberikan *update* kode OTP	Kode OTP dari Google Authentikator berhasil *update* dan bisa digunakan untuk *login* pengguna	1	Berhasil
			2	Berhasil
			3	Berhasil
			4	Berhasil
			5	Berhasil
			6	Berhasil
			7	Berhasil
			8	Berhasil
			9	Berhasil
			10	Berhasil

Tabel 4 menampilkan pengujian ketiga (kode 03) yang memfokuskan pada kompatibilitas sistem dengan aplikasi Google Authenticator sebagai generator OTP berbasis Time-based One-Time Password (TOTP). Hasil menunjukkan bahwa seluruh akun pengguna (100%) berhasil melakukan sinkronisasi dengan Google Authenticator dan mampu menggunakan kode OTP yang dihasilkan untuk proses autentikasi. Adapun tampilan notifikasi OTP terkirim pada Google Authenticator dapat dilihat pada gambar 10 berikut.

Gambar 10. Tampilan OTP Melalui Google Authenticator

Gambar 4.10 menampilkan tampilan kode verifikasi untuk dua pengguna yang berbeda, yaitu zulfikar dan achyar. Untuk pengguna zulfikar, sistem telah menghasilkan kode verifikasi 667 512, sedangkan untuk pengguna achyar, kode yang dihasilkan adalah 815 772. Tampilan ini memberikan visibilitas kepada administrator mengenai kode OTP yang sedang aktif dan dikirimkan kepada masing-masing pengguna.

Gambar 5 menampilkan proses diawali dari halaman pengaturan akun. Pengguna dapat memilih untuk mengaktifkan fitur 2FA atau tidak. Jika tidak diaktifkan, sistem akan kembali ke halaman pengaturan. Namun, apabila 2FA diaktifkan, pengguna diminta menentukan metode autentikasi yang akan digunakan. Terdapat tiga pilihan metode, yaitu Google Authenticator, Email OTP, dan Telegram BO

C. Pengujian Performa Website

Pengujian waktu respon website dilaksanakan untuk mengevaluasi performa server Flask dalam menangani request HTTP dan mengukur kualitas responsivitas sistem secara keseluruhan. Pengujian menggunakan pendekatan load testing sederhana dengan mengirimkan 25 request GET secara berurutan ke URL utama website (https://abiyyu.duckdns.org). Setiap request dipantau untuk mencatat status code HTTP yang dikembalikan server serta durasi waktu yang diperlukan untuk menyelesaikan setiap transaksi. Metodologi ini dipilih untuk memberikan gambaran objektif mengenai konsistensi performa server dalam kondisi akses normal, sekaligus mengidentifikasi potensi bottleneck atau anomali dalam response time yang dapat mempengaruhi pengalaman pengguna. Pengujian performa website dapat dilihat pada tabel 6 berikut.

Tabel 6. Pengujian Performa *Website*

No	URL	Status Kode	Waktu Respon
1	https://abiyyu.duckdns.org	200 OK	487 ms
2		200 OK	469 ms
3		200 OK	554 ms
4		200 OK	505 ms
5		200 OK	470 ms
6		200 OK	548 ms
7		200 OK	489 ms
8		200 OK	469 ms
9		200 OK	491 ms
10		200 OK	462 ms
11		200 OK	465 ms
12		200 OK	463 ms
13		200 OK	517 ms
14		200 OK	463 ms
15		200 OK	464 ms
16		200 OK	463 ms
17		200 OK	472 ms
18		200 OK	462 ms
19		200 OK	466 ms
20		200 OK	469 ms
21		200 OK	466 ms
22		200 OK	464 ms
23		200 OK	462 ms
24		200 OK	466 ms
25		200 OK	467 ms
Rata-rata = Jumlah Nilai / Jumlah Data			478.92 ms

Tabel 6 menampilkan hasil pengujian menunjukkan bahwa seluruh 25 request yang dikirimkan ke server memperoleh response dengan status code 200 OK (100% success rate). Konsistensi status code ini mengindikasikan bahwa server Flask telah beroperasi dengan stabil dan mampu menangani incoming request tanpa mengalami error server internal (5xx) maupun client error (4xx). Tidak ditemukan adanya request timeout, connection failure, atau response code error selama periode pengujian berlangsung. Hal ini menunjukkan bahwa konfigurasi server, routing URL, dan infrastruktur jaringan telah berfungsi dengan baik dalam melayani akses pengguna terhadap halaman utama website. Analisis waktu respon menunjukkan variasi response time dalam rentang 462 ms hingga 554 ms, dengan rata-rata waktu respon sebesar 478.92 ms. Distribusi waktu respon menunjukkan pola yang relatif konsisten, dengan sebagian besar nilai berkisar antara 460-470 ms, sementara beberapa request mengalami waktu respon yang lebih tinggi pada rentang 500-554 ms. Response time terendah tercatat pada 462 ms (request ke-10, 18, dan 23), sedangkan response time tertinggi mencapai 554 ms (request ke-3). Standar deviasi yang relatif kecil mengindikasikan bahwa performa server cenderung stabil dengan fluktuasi waktu respon yang masih dalam batas toleransi normal.

IV. Kesimpulan

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan, maka dapat disimpulkan sebagai berikut:

Penerapan metode Two-Factor Authentication menggunakan Google Authenticator berhasil meningkatkan keamanan proses autentikasi pengguna website. Dengan adanya lapisan verifikasi tambahan berupa kode OTP berbasis waktu, sistem login menjadi lebih terlindungi dari potensi penyalahgunaan akun akibat pencurian kata sandi.

Hasil Pengukuran dan analisis performa website pada halaman login menunjukkan bahwa sistem mampu memberikan waktu respon rata-rata yang stabil serta throughput yang memadai. Hal ini membuktikan bahwa penerapan 2FA tidak menurunkan kualitas layanan, melainkan tetap menjaga pengalaman pengguna dalam mengakses website.

Referensi

[1] W. L. Aji, Y. Riady, and B. L. Qasthari, "Pengelolaan Pemesanan Menu Makanan Menggunakan Framework Flask Python," JATISI (Jurnal Teknik Informatika dan Sistem Informasi), vol. 9, no. 2, pp. 916–929, 2022, doi: 10.35957/jatisi.v9i2.1459.

[2] T. Aprilia, B. S. Pitoyo, A. Fauzi, R. G. Ramadhanti, R. D. Nurazizah, E. T. Wanti, and A. R. Prasetyo, "Pengaruh Keamanan Two Factor Authentication Terhadap Pencurian Data (Cyber Crime) Pada Media Sosial," Madani: Jurnal Ilmiah Multidisiplin, vol. 2, no. 5, 2024.

[3] A. D. Djayali, M. Muzammil, and A. Samad, "Implementasi Aplikasi Meeting Online Pada Virtual Private Server di Masa Pandemi," Simkom, vol. 6, no. 1, pp. 23–33, 2021, doi: 10.51717/simkom.v6i1.52.

[4] Y. Fatman and R. Oktaviawati, "Implementasi Metode Open Authorization (OAUTH2) Untuk Pengelolaan Data Dosen di Universitas Islam Nusantara," Ainet: Jurnal Informatika, vol. 2, no. 1, pp. 10–18, 2020, doi: 10.26618/ainet.v2i1.3212.

[5] N. M. D. Febriyanti, A. K. O. Sudana, and I. N. Piarsa, "Implementasi Black Box Testing pada Sistem Informasi Manajemen Dosen," JITTER: Jurnal Ilmiah Teknologi dan Komputer, vol. 2, no. 3, p. 535, 2021, doi: 10.24843/jtrti.2021.v02.i03.p12.

[6] E. D. Handoyo, S. Santoso, and D. J. Surjawan, "Pengembangan Aplikasi Mobile Pemesanan dan Pembayaran Makanan Berbasis Cloud Storage," Jurnal Teknik Informatika dan Sistem Informasi, vol. 8, no. 1, pp. 161–174, 2022, doi: 10.28932/jutisi.v8i1.4393.

[7] Y. Heriyanto, A. A. Qalban, and I. A. Mukaromah, "Pengembangan Metode Login Two Factor Authentication (2FA) untuk Keamanan Sistem Informasi Akademik," 2022, pp. 142–150.

[8] J. S. P. Kase and P. O. N. Saian, "Pengembangan aplikasi," vol. 8, no. 4, pp. 1288–1299, 2023.

[9] D. M. Kusumawardani, S. Astiti, M. Y. Fathoni, D. Sunardi, and S. Fernandez, *Web Dasar Menggunakan HTML, CSS, JS, PHP dan Studi Kasus*. PT. Sonpedia Publishing Indonesia, 2023.

[10] F. M. Lanang Adi Saputra, "Ancaman Keamanan Pada Sistem Informasi Manajemen Perusahaan," Jurnal Pendidikan Siber Nusantara, vol. 1, no. 2, pp. 58–66, 2024.

[11] I. Muhammad and M. Masnur, "Aplikasi QR Code Sebagai Sarana Penyampaian Informasi Pohon di Kebun Raya Jompie," vol. 1, no. 1, pp. 33–41, 2021.

[12] R. Parlika, D. C. M. Wijaya, and A. Pratama, "Bot Penyimpan Data Pengumpulan Tugas Peserta Elearning Berbasis Telegram [Er-Bot Pdpt]," XVI, 2021.

[13] L. Qadriah and S. Achmady, "Sistem Pengamanan Dokumen dengan Algoritma Time-Based One Time Password (TOTP) pada Two-Factor Authentication (2FA)," Jurnal Sains dan Informatika, pp. 29–35, 2023.

[14] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron, and K. Seamons, "A usability study of five two-factor authentication methods," in *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, 2020, pp. 357–370.

[15] R. A. Sasono, S. P. Kristanto, L. Hakim, and D. Yusuf, "Optimasi Web Service REST Pada Backend Aplikasi Prospect Menggunakan Metode Extreme Programming," Journal Zetroem, vol. 7, no. 1, pp. 96–103, 2025, doi: 10.36526/ztr.v7i1.4202.

[16] J. N. Semendawai, I. Febiola, B. Pamungkas, and M. D. Ruliansyah, "Perancangan Aplikasi Otomatisasi Menggunakan Bahasa Pemrograman Python Pada Aktivitas Monitoring Pemakaian Data Harian Kartu Internet of Things," Jurnal Rekayasa Elektro Sriwijaya, vol. 3, no. 1, 2021.

[17] A. Syahputra and R. Supardi, "Rancang Bangun Monitoring Jaringan dengan Metode Simple Mail Transfer Protocol," Jurnal Teknik Informatika UNIKA Santo Thomas, vol. 7, no. 2, pp. 152–159, 2022.

[18] A. N. Syahrudin and T. Kurniawan, "Input dan Output pada Bahasa Pemrograman Python," *Jurnal Dasar Pemrograman Python STMIK*, Jun. 2018. [Online]. Available: https://www.researchgate.net/publication/338385483

[19] M. L. Syam, "Sistem Informasi Stok Barang Menggunakan QR-Code Berbasis Android," Jurnal Informatika Ekonomi Bisnis, vol. 4, 2022, doi: 10.37034/infeb.v4i1.108.

[20] M. Syani, "Implementasi Intrusion Detection System (IDS) Menggunakan Suricata Pada Linux Debian 9 Berbasis Cloud Virtual Private Servers (VPS)," *Jurnal Pengembangan Teknologi Informasi*, vol. 1, no. 1, pp. 13–20, 2020.

[21] A. Tedyyana, "Implementasi Secure Socket Layer Pada Aplikasi Computer Assisted Test Komisi Pemilihan Umum Bengkalis," Digital Zone: Jurnal Teknologi Informasi dan Komunikasi, vol. 11, no. 1, pp. 71–80, 2020, doi: 10.31849/digitalzone.v11i1.3859.

[22] S. M. Ulfa, F. Santoso, and N. Azize, "Rancangan Bangun Sistem Informasi," Eka Wida Fridayanthie, vol. 9, no. 2, pp. 31–48, 2024.

[23] D. W. Musu, "Analisis Pola Penggunaan Fitur Autentikasi Dua Faktor Oleh Para Remaja," E-Jurnal JUSITI: Jurnal Sistem Informasi dan Teknologi Informasi, vol. 11, no. 2, pp. 212–222, 2022.