

Two factor authentication pada sistem login rekam medis elektronik berbasis web menggunakan metode prototype

Nadia Julian Dewi*, Arizona Firdonsyah, Danur Wijayanto

Program Studi Teknologi Informasi, Fakultas Sains dan Teknologi, Universitas 'Aisyiyah Yogyakarta.

Email: dewi.nadia218@gmail.com, arizona@unisayogya.ac.id, danurwijayanto@unisayogya.ac.id.

Abstrak

Praktek Mandiri Fisioterapi Bio Physio bertempat didaerah Rejowinangun, Yogyakarta, berdiri sejak tahun 2018, memiliki sistem rekam medis elektronik yang belum dilengkapi fitur keamanan yang memadai. Kondisi ini menyebabkan data pasien rentan terhadap ancaman keamanan seperti pencurian identitas dan akses tidak sah. Untuk mengatasi masalah tersebut, diperlukan pembangunan *Two-Factor Authentication* (2FA) pada sistem login rekam medis elektronik berbasis web. Pembangunan sistem ini menggunakan *framework* CodeIgniter dengan metode pengembangan sistem prototype serta memanfaatkan aplikasi Google Authenticator. Pengujian sistem dilakukan dengan metode *Black-box* Testing menggunakan *Ekuivalen Partitioning* untuk memastikan setiap fungsionalitas sistem memenuhi kebutuhan dan spesifikasi Praktek Mandiri Fisioterapi Bio Physio. Berdasarkan hasil pengujian, implementasi *Two-Factor Authentication* pada sistem login rekam medis elektronik berbasis web berhasil dibangun sesuai harapan. Dari total 20 fitur yang diuji, sistem menunjukkan akurasi sistem 100%. Seluruh fitur berfungsi dengan baik dan memenuhi kriteria yang diharapkan. Data rekam medis elektronik pasien bersifat sangat sensitif dan kerahasiaannya harus dijaga dengan ketat. Penyalahgunaan data dapat berdampak serius, terutama informasi yang berkaitan dengan kondisi kesehatan pasien. Keberhasilan pengujian ini mengindikasikan bahwa sistem siap digunakan untuk meningkatkan keamanan data dan kualitas pelayanan di Praktek Mandiri Fisioterapi Bio Physio.

Kata Kunci: codeigneter; *prototype*; rekam medis elektronik; sistem login; *two factor authentication*.

Two factor authentication in web-based electronic medical record login system using prototype method

Abstract

Bio Physio Independent Physiotherapy Practice is in the Rejowinangun area, Yogyakarta, established since 2018, has an electronic medical record system that is not equipped with adequate security features. This condition makes patient data vulnerable to security threats such as identity theft and unauthorized access. To overcome this problem, it is necessary to build Two-Factor Authentication (2FA) on a web-based electronic medical record login system. The development of this system used the CodeIgniter framework with a prototype system development method and utilized the Google Authenticator application. System testing was carried out using the Black-Box Testing method using Equivalent Partitioning to ensure that each system functionality meets the needs and specifications of Bio Physio Independent Physiotherapy Practice. Based on the test results, the implementation of Two-Factor Authentication on the web-based electronic medical record login system was successfully built as expected. Of the total 20 features tested, the system showed 100% system accuracy. All features function properly and meet the expected criteria. Patient electronic medical record data was very sensitive and its confidentiality must be strictly maintained. Misuse of data could have serious consequences, especially information related to the patient's health condition. The success of this test indicated that the system was ready to be used to improve data security and service quality at Bio Physio Physiotherapy Independent Practice.

Keywords: codeigneter; *electronic medical records*; login system; *prototype*; *two factor authentication*

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam sektor kesehatan, termasuk adopsi Rekam Medis Elektronik (RME) yang menggantikan sistem rekam medis manual berbasis kertas (Prawiradirjo et al., 2018). RME menawarkan berbagai manfaat, seperti

efisiensi penyimpanan dan akses data, serta peningkatan akurasi dan kecepatan pengambilan keputusan klinis (Khasanah, 2020). Penggunaan RME berbasis *web* juga memunculkan tantangan baru terkait keamanan data pasien (Sari, 2020) Data rekam medis elektronik pasien sangatlah sensitif dan kerahasiaannya harus dijaga ketat. Penyalahgunaan data tersebut dapat berdampak serius, terutama jika informasi tersebut berkaitan dengan kondisi kesehatan pasien yang seharusnya dirahasiakan (Abduh, 2021).

Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) Pasal 11 mengategorikan rekam medis elektronik sebagai dokumen elektronik yang sah sebagai alat bukti hukum. Oleh karena itu, perlindungan data pasien dalam RME menjadi krusial untuk menjamin kerahasiaan, integritas, dan ketersediaan informasi kesehatan yang sensitif (Rubiyanti, 2023).

Praktek Mandiri Fisioterapi Bio Physio, berlokasi di Rejowinangun, Yogyakarta, berdiri sejak tahun 2018 dan resmi menjadi praktek mandiri pada Juni 2023. Selama ini, Biophysio telah memiliki reputasi yang baik dalam memberikan layanan fisioterapi kepada masyarakat umum, serta menjadi mitra fisioterapi bekerja sama klub sepak bola Persik Kediri dan PSS Sleman, sebagai salah satu penyedia layanan kesehatan, telah mengadopsi Rekam Medis Elektronik berbasis *Web* untuk meningkatkan kualitas pelayanan dan efisiensi operasional.

Sistem Rekam Medis Elektronik di Praktek Mandiri Fisioterapi Bio Physio yang ada saat ini belum memiliki fitur keamanan yang memadai, sehingga data pasien rentan terhadap ancaman keamanan seperti pencurian identitas dan akses tidak sah oleh karena itu, untuk mengatasi masalah keamanan tersebut, diperlukan penambahan autentikasi menggunakan *Two-Factor Authentication* (2FA) pada sistem rekam medis elektronik. *Two-Factor Authentication* akan memberikan lapisan perlindungan ekstra dengan mewajibkan pengguna untuk memberikan dua bentuk identifikasi sebelum dapat mengakses data sensitif pasien (Sofia et al., 2022).

Two-Factor Authentication (2FA) merupakan solusi untuk meningkatkan keamanan sistem dengan menambahkan lapisan autentikasi tambahan. Metode 2FA tidak hanya diminta memasukkan kata sandi, tetapi juga harus memberikan bukti otentikasi lain, seperti kode TOTP dari aplikasi autentikator (Herdiantoro & Islami, 2023). Cara ini merupakan model perlindungan keamanan berlapis yang dapat meminimalisir akses orang yang tidak memiliki wewenang terhadap akun pengguna sehingga mempersulit langkah pelaku kejahatan untuk masuk ke dalam sistem dan tentunya memberikan keuntungan bagi pengguna dan mengembangkan sistem agar data privasi tidak mudah diakses orang yang tidak berwenang (Heriyanto et al., 2022).

Salah satu metode *Two-Factor Authentication* (2FA) yang digunakan yaitu penggunaan *Password* dan *Time-Based One-Time Password* (TOTP) yang dikirimkan melalui Google Authenticator (Aprilia et al., 2024). Metode *Time-Based One-Time Password* (TOTP) yang mampu menghasilkan kata sandi satu kali pakai. Kata sandi yang dihasilkan oleh TOTP memiliki masa berlaku yang terbatas dan terus berubah dalam waktu tertentu (Sarah Hapsari et al., 2020).

Berdasarkan permasalahan tersebut penulis akan mengembangkan *Two Factor Authentication* pada Sistem *Login* Rekam Medis Elektronik Praktek Mandiri Biophysio Yogyakarta Berbasis *Web*. Sistem ini akan dikembangkan menggunakan *Framework* Codeigniter, karena dalam implementasi dikenal dengan performanya yang cepat dan ringan, terutama untuk aplikasi yang tidak terlalu besar (MASHADOV, 2020). Sistem akan dikembangkan menggunakan metode *prototype* alasan menggunakan Metode *Prototype* memungkinkan adaptasi yang lebih mudah terhadap perubahan kebutuhan fungsionalitas, karena umpan balik pengguna dapat diintegrasikan secara terus-menerus selama proses pengembangan (Taufiq et al., 2023). Penelitian ini diharapkan dapat memberikan dalam meningkatkan keamanan akses data rekam medis pasien di fasilitas kesehatan yang menggunakan RME berbasis *web*, sehingga dapat melindungi privasi dan hak pasien sesuai dengan peraturan perundang-undangan yang berlaku.

2. Metode

Pada bagian metode penelitian, digunakan metode *prototype* yang mencakup penjabarannya dengan menguraikan tinjauan teoritis terkait penelitian ini, seperti konsep dasar *prototype*, tahapan pengembangan sistem, serta relevansi metode ini dalam mencapai tujuan penelitian. Penjelasan ini

melibatkan langkah-langkah spesifik, mulai dari pengumpulan kebutuhan hingga evaluasi prototype untuk memastikan sistem sesuai dengan kebutuhan pengguna.

2.1 Sistem Login

Sistem *Login* adalah proses autentikasi pengguna yang bertujuan untuk memverifikasi identitas seseorang sebelum memberikan akses ke suatu sistem atau sumber daya. Proses ini umumnya melibatkan pemasukan *Email* dan kata sandi yang telah terdaftar dan tersimpan dalam sistem (Azhar et al., 2020).

2.2 Two Factor Authentication

Two-Factor Authentication merupakan sebuah metode otentikasi pengguna di mana dua faktor yang bersifat independen akan digunakan dalam membuktikan adanya klaim bahwa sebuah entitas atau identitas itu asli. Penggunaan *Two-Factor Authentication* akan dapat mengurangi resiko seorang *adversary* dapat masuk ke sebuah sistem dengan menggunakan identitas pribadi individu karena selain harus mengetahui *password* yang kita gunakan, *adversary* juga harus mendapatkan informasi kedua yang bisa dihasilkan dari sumber yang berbeda (Sarah Hapsari et al., 2020).

2.3 Google Authenticator

Google Authenticator menghasilkan kredensial unik menggunakan algoritma kata sandi sekali pakai berbasis waktu (TOTP). Algoritma TOTP berbasis waktu, sehingga kata sandi berubah setiap 30 detik. Hal ini membuat sangat sulit bagi penyerang untuk memecahkan atau memperoleh kata sandi TOTP (Kevin Pitch, 2023).

2.4 Rekam Medis Elektronik

Rekam medis elektronik adalah Rekaman atau catatan Rekam Medis pasien seumur hidup pasien dalam format elektronik tentang informasi kesehatan seseorang yang dituliskan oleh satu atau lebih petugas kesehatan secara terpadu dalam tiap kali pertemuan antara petugas kesehatan dengan pasien. rekam medis elektronik bisa diakses dengan komputer dari suatu jaringan dengan tujuan utama menyediakan atau meningkatkan perawatan serta pelayanan kesehatan yang efisien dan terpadu (Khasanah, 2020)

2.5 Framework CodeIgniter

CodeIgniter kerangka kerja PHP yang mempercepat pembuatan aplikasi *web* dengan menyediakan kumpulan fungsi siap pakai. Dengan menggunakan pola *Model-View-Controller* (MVC), CodeIgniter membagi aplikasi menjadi tiga komponen terpisah untuk meningkatkan keteraturan kode. Selain itu, kerangka kerja ini menawarkan berbagai alat bantu seperti *helpers* dan *libraries*, yang memungkinkan pengembang untuk fokus pada implementasi tugas utama dan menyelesaikan proyek dengan lebih cepat (Krisna et al., 2022).

2.6 Web

Web adalah layanan internet yang menyediakan informasi bagi pengguna komputer. *Website* merupakan kumpulan halaman yang menampilkan informasi berupa teks, gambar, animasi, suara, atau gabungannya, baik statis maupun dinamis, yang saling terhubung melalui *hyperlink* (Prawiradirjo et al., 2018).

2.7 Prototype

Prototype ini adalah metode dalam rekayasa perangkat lunak yang menunjukkan bagaimana suatu perangkat lunak akan beroperasi. Paradigma atau model *prototype* dimulai dengan berdiskusi dengan pemangku kepentingan untuk menentukan segala kebutuhan dalam pembuatan suatu aplikasi. Data yang telah diidentifikasi kemudian diolah dan dilanjutkan ke tahap perencanaan cepat, yang selanjutnya akan dilanjutkan ke tahap pemodelan desain cepat. Pada tahap ini, *prototype* atau purwarupa aplikasi dibuat, kemudian dilanjutkan ke tahap konstruksi *prototype*, dan tahap terakhir adalah *deployment* serta

evaluasi dari para pemangku kepentingan. berikut ini penjelasan terkait penelitian menggunakan metode *prototype* (Pressman & Maxim, 2020).



Gambar 1. Metode *Prototype*

2.8. Pengumpulan Data

Pengumpulan data merupakan tahap awal untuk mengidentifikasi kebutuhan dalam pengembangan sistem. Penulis melakukan observasi pada sistem rekam medis elektronik yang sudah ada, serta wawancara dengan pemilik dan dokter di Praktek Mandiri Bio Physio Yogyakarta. Sistem sebelumnya belum menerapkan metode keamanan, terutama dengan adanya pergantian dan penambahan dokter. Oleh karena itu, dilakukan analisis kebutuhan untuk mengimplementasikan *Two-Factor Authentication* (2FA) guna meningkatkan keamanan data pasien. Sistem 2FA ini dirancang berdasarkan kebutuhan fungsional dengan fokus pada dokter sebagai pengguna utama.

2.8.1. Kebutuhan Fungsional

Kebutuhan fungsional yang akan dibangun, diantaranya:

- Sistem dapat melakukan Registrasi akun untuk Dokter.
- Sistem dapat mendapatkan pesan Aktivasi melalui *Email*, Registrasi Pendaftaran akun Dokter.
- Sistem dapat melakukan *Login* dan TOTP untuk Dokter.
- Sistem dapat menerima kode TOTP dari Google Authenticator untuk Dokter.
- Sistem dapat melakukan keluar oleh Dokter.
-

2.8.2. Kebutuhan Non-Fungsional

Kebutuhan Non-Fungsional untuk spesifikasi yang akan digunakan untuk membangun *Two-Factor Authentication* pada sistem *login* Rekam Medis Elektronik berbasis *Web*, diantaranya :

Tabel 1 Kebutuhan Non-Fungsional

Sistem Operasi	Perangkat lunak yang digunakan	Perangkat keras yang digunakan
Windows 11 64 Bit	1. <i>Framework</i> Codeigniter 2. Visual Studio Code 3. Laragon 4. <i>Web Browser</i> (Chrome) 5. Google Authenticator	Laptop HP Intel(R) Core(TM) i5-1035G1 CPU @ 1.00GHz 1.19 GHz

2.9. Desain Prototype

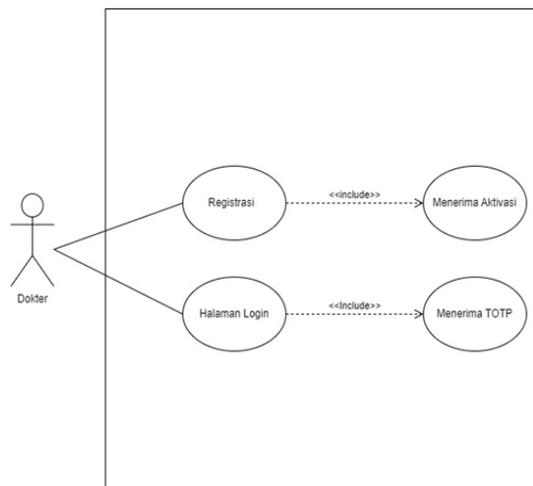
Tahapan ini menjelaskan bagaimana membangun sebuah rancangan desain *prototype* diawali dengan pembuatan Desain Sistem berbasis *Web*.

2.9.1. Desain Sistem

Tahapan Desain Sistem ini menghasilkan gambaran rancangan sistem yang terdiri dari beberapa diagram, seperti *Use Case Diagram* yang menggambarkan interaksi pengguna dengan sistem, *Activity Diagram* yang menunjukkan alur aktivitas dalam sistem, dan *Entity Relationship Diagram* yang memetakan hubungan antar data dalam sistem.

2.9.2. Use Case Diagram

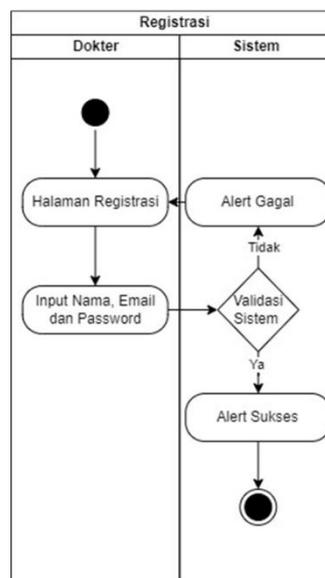
Use case Diagram ini menunjukkan satu aktor yaitu dokter memiliki alur dari penggunaan *Two Factor Authentication* pada sistem *login* rekam medis elektronik berbasis *web*.



Gambar 2. Use Case Diagram

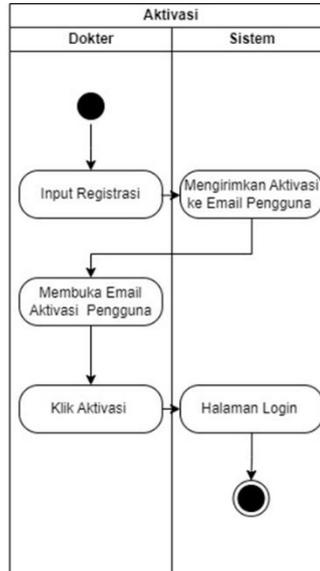
2.9.3. Activity Diagram

Activity Diagram ini menunjukkan alur aktivitas dalam sistem, yaitu alur penggunaan *Two-Factor Authentication* oleh dokter pada sistem *login* rekam medis elektronik berbasis *web*.



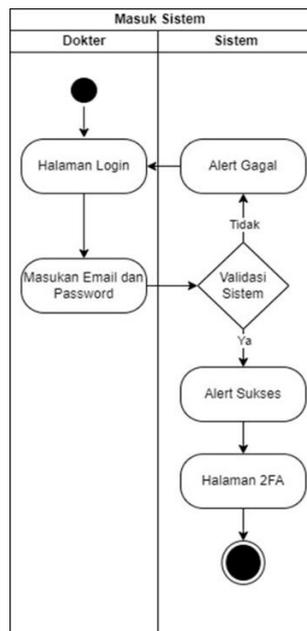
Gambar 3. Activity Diagram Registrasi

Gambar 2.3 menjelaskan Halaman Registrasi menampilkan formulir Registrasi akun untuk dokter. Setelah mengisi Nama, *Email*, dan *Password*, sistem akan melakukan validasi data. Jika data *valid*, pengguna akan diarahkan ke tahap selanjutnya. jika tidak, pengguna akan dikembalikan ke halaman registrasi untuk memperbaiki kesalahan.



Gambar 4. Activity Diagram Aktivasi

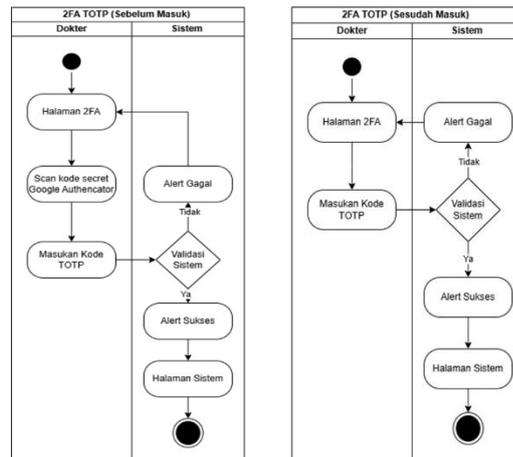
Gambar 2.4 Menjelaskan pada Halaman Aktivasi ini melanjutkan dengan langkah verifikasi *Email*. Sistem akan mengirimkan tautan aktivasi ke alamat *Email* yang didaftarkan sebelumnya. Pengguna perlu mengklik tautan tersebut untuk mengonfirmasi bahwa alamat *Email valid* dan aktif, setelah itu baru dapat diarahkan ke halaman *Login*.



Gambar 5. Activity Diagram Masuk Sistem

Gambar 2.5 Menjelaskan pada Halaman ini menampilkan Halaman Masuk untuk dokter. Setelah memasukkan *Email* dan kata sandi lalu sistem akan melakukan validasi tersebut untuk ke Halaman

Verifikasi 2FA selanjutnya. Jika *password* tidak *valid*, pengguna akan dikembalikan ke halaman *login* untuk mencoba kembali.



Gambar 6. Activity Diagram 2fa melakukan TOTP (Sebelum & Sesudah Sistem)

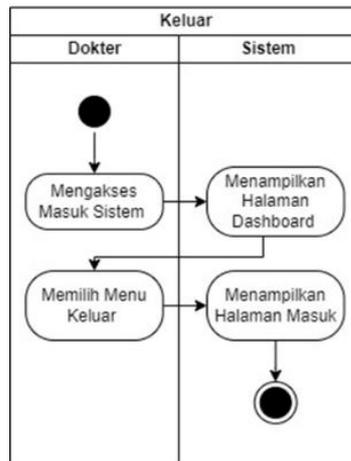
Gambar 2.6 menjelaskan Halaman *Two Factor Authenticator* (2FA) digunakan sebelum dan sesudah *login* untuk memastikan keamanan akses dokter ke sistem rekam medis elektronik berbasis *web*. Pada *login* pertama kali, halaman ini menampilkan *QR code* atau kode *secret* yang harus dipindai menggunakan aplikasi Google Authenticator untuk menghasilkan kode TOTP. Jika kode TOTP pertama kali tidak *valid*, sistem akan mengembalikan pengguna ke halaman 2FA dan mengatur ulang *QR code* atau kode *secret* untuk mencoba kembali. Setelah *login* pertama selesai, halaman ini tetap digunakan sebagai bagian dari proses otentikasi. Dokter harus memasukkan kode TOTP yang dihasilkan oleh aplikasi Google Authenticator untuk dapat mengakses sistem. Jika kode TOTP tidak *valid*, pengguna akan diarahkan kembali ke halaman 2FA untuk memasukkan kode yang benar.



Gambar 7. Activity Diagram TOTP Google Authenticator

Gambar 2.7 menjelaskan pada Halaman ini menunjukkan cara mendapatkan kode TOTP dengan menggunakan Google Authenticator untuk menghasilkan kode TOTP. Sebelum menggunakan Google Authenticator menambahkan akun terlebih dahulu, setelah akun tervalidasi pengguna akan memilih menu pengaturan kunci, lalu mengisi *form* berupa nama, kode kunci Google Authenticator yang ada

di halaman *login* dan pengaturan jenis TOTP jika data sudah benar maka sistem akan mengvalidasi dan menghubungkan ke Google Authenticator. Selanjutnya, aplikasi Google Authenticator akan menghasilkan kode TOTP yang akan digunakan untuk verifikasi tambahan saat masuk ke sistem.

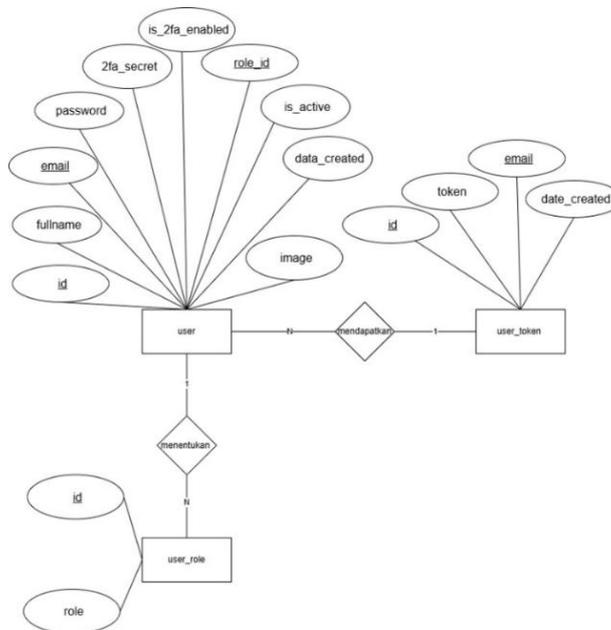


Gambar 8. Activity Diagram Keluar

Gambar 2.8 menjelaskan pada halaman ini menampilkan halaman keluar dari sistem, dokter yang sudah masuk ke dalam sistem kemudian menampilkan menu utama dari sistem. selanjutnya dokter memilih menu keluar dari sistem dan akan menampilkan halaman *login* untuk melakukan *login* kembali.

2.9.4. Entity Relationship Diagram

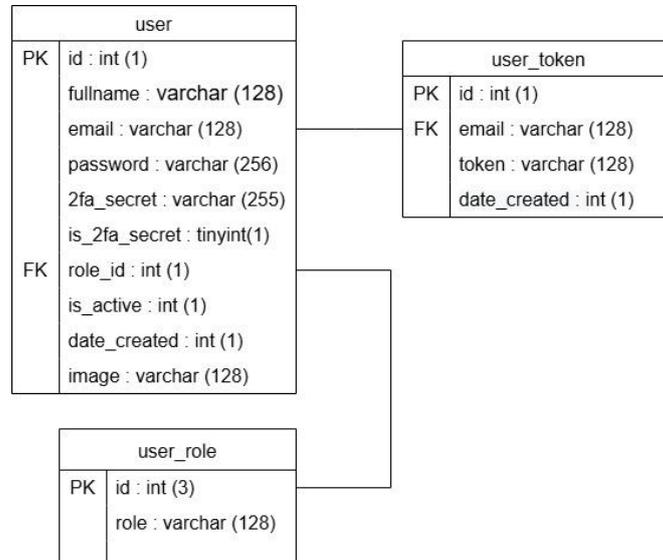
Entity Relationship Diagram ini menggambarkan proses *two-factor authentication* pada sistem *login* rekam medis elektronik, yang melibatkan tiga entitas: *user*, *user_role*, dan *user_token*. Entitas *user* memiliki atribut seperti *id*, *fullname*, *email*, *password*, *2fa_secret*, *is_2fa_enabled*, *role_id*, *is_active*, *date_created*, dan *image*, yang berelasi *one-to-many* dengan entitas *user_role* (atribut: *id* dan *role*). Selain itu, *user_token* (atribut: *id*, *email*, *token*, dan *date_created*) berelasi *many-to-one* dengan tabel *user*.



Gambar 9. Entity Relationship Diagram

2.9.5. Database

Database ini berfungsi sebagai panduan untuk memahami struktur, isi, dan relasi antar tabel, mencakup daftar tabel, kolom, tipe data, serta hubungan antar tabel. Informasi ini mendukung pengelolaan database, optimasi kinerja, menjaga integritas data, dan pengembangan aplikasi yang terhubung. Selain itu, database ini menjadi referensi penting untuk desain, pengembangan, dan pemecahan masalah, serta merupakan implementasi dari ERD yang telah dirancang sebelumnya.



Gambar 10. Database Sistem

3. Hasil dan Pembahasan

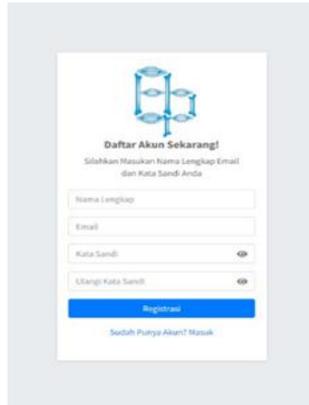
Bagian hasil dan pembahasan ini merupakan kelanjutan dari metode penelitian yang mencakup tahapan implementasi *prototype*, pengujian *prototype*, dan evaluasi *prototype*. Setiap tahapan dijelaskan secara detail untuk menunjukkan bagaimana sistem dikembangkan, diuji, dan dievaluasi hingga memenuhi kebutuhan fungsional dan memperoleh persetujuan dari pihak mitra.

3. Implementasi *Prototype*

Tahapan ini merupakan proses implementasi *Two-Factor Authentication* pada Sistem Login Rekam Medis Elektronik yang telah dirancang pada tahap desain *prototype*. Implementasi mencakup beberapa bagian, yaitu registrasi, login dengan *Two-Factor Authentication* menggunakan Google Authenticator, penambahan kode TOTP, hingga proses keluar dari sistem.

3.1. Implementasi Halaman Registrasi

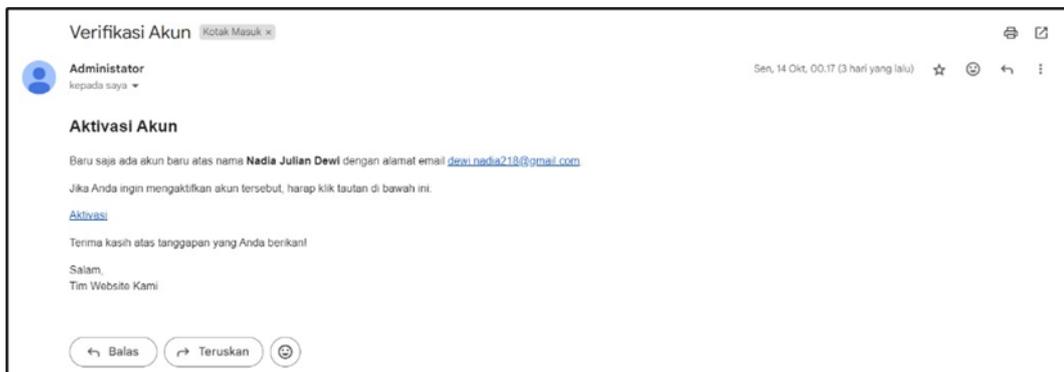
Gambar 3.1 menjelaskan Tahapan ini membuat halaman Aktivasi Registrasi untuk pendaftaran akun fungsi ini berguna saat pertama kali Registrasi akun pada sistem *login* rekam medis elektronik yang dimana sistem ini meminta pengguna yaitu dokter melakukan registrasi memasukan Nama Lengkap, *Email*, Kata sandi akses ke sistem rekam medis elektronik.



Gambar 3.1 Tampilan Halaman Registrasi

3.1.1. Implementasi Halaman Aktivasi

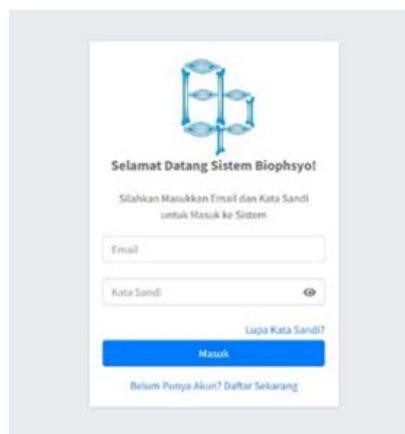
Gambar 3.2 menjelaskan Halaman aktivasi ini menjelaskan bagaimana setelah selesai melakukan registrasi akun dokter akan mengirimkan sebuah *Email* dengan *Email* yang sudah terdaftar pada registrasi akun dan aktif sistem tujuannya agar mengvalidasi apakah *Email* yang digunakan *Email* aktif atau pasif.



Gambar 3.2 Tampilan Halaman Aktivasi *Email*

3.1.2. Implementasi Halaman Login

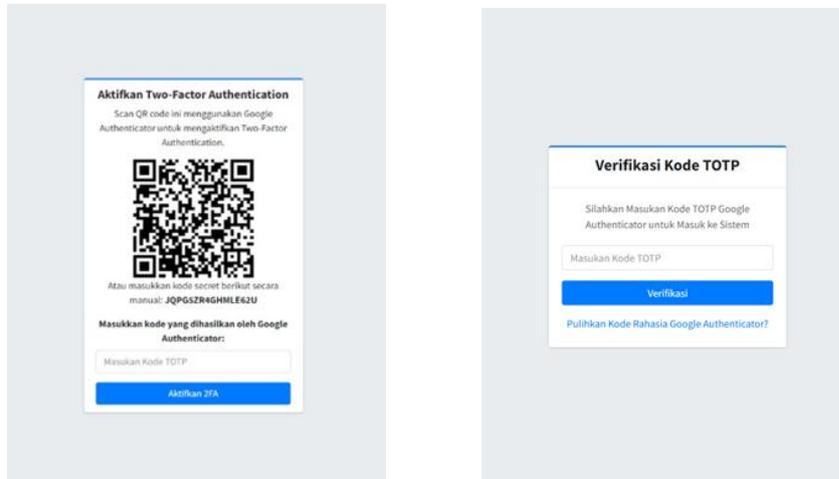
Gambar 3.3 menjelaskan Halaman *Login* memungkinkan dokter mengakses sistem rekam medis elektronik. Tampilan ini dilengkapi tombol "Masuk", pesan kesalahan seperti kata sandi salah atau akun tidak terdaftar, serta fitur ikon untuk menampilkan atau menyembunyikan kata sandi demi kemudahan pengguna.



Gambar 3.3 Tampilan Halaman *Login*

3.1.3. Implementasi Halaman Verifikasi 2FA TOTP (Sebelum & Sesudah Masuk)

Gambar 3.4 menjelaskan Halaman kedua ini berfungsi untuk mengelola proses *Two-Factor Authentication* (2FA) pada sistem. Setelah *login* berhasil dan akun tervalidasi, pengguna (dokter) akan diarahkan untuk mengaktifkan 2FA dengan memindai *QR Code* yang disediakan. Pemindaian ini bertujuan untuk mengintegrasikan akun pengguna dengan aplikasi Google Authenticator, yang kemudian menghasilkan kode TOTP berdasarkan *QR Code* atau kode *secret* yang telah diberikan. Jika pengguna sebelumnya sudah melakukan pemindaian *QR Code*, *login* berikutnya akan langsung menampilkan halaman "Verifikasi Google Authenticator," di mana pengguna diminta memasukkan kode TOTP dari aplikasi Google Authenticator untuk melanjutkan ke sistem.



Gambar 3.4 Tampilan Halaman Verifikasi 2fa TOTP (Sebelum & Sesudah Masuk)

3.1.4. Implementasi Kode TOTP Google Authenticator

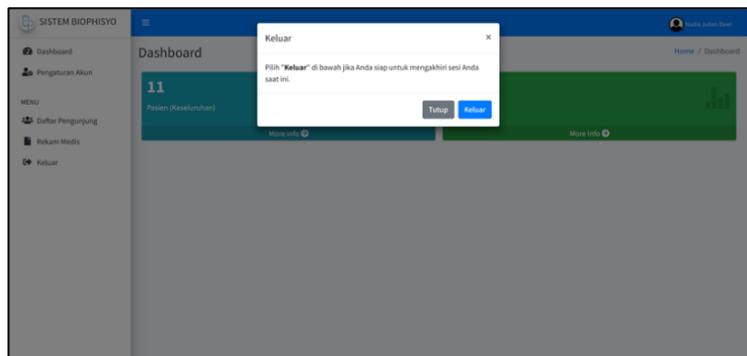
Gambar 3.5 menjelaskan tampilan ini bagaimana cara menghasilkan kode TOTP pada Aplikasi Google Authenticator untuk melakukan 2FA pada sistem *login* rekam medis elektronik.



Gambar 3.5 Tampilan Halaman TOTP Google Authenticator

3.1.5. Implementasi Halaman Keluar Sistem

Gambar 3.6 menjelaskan tampilan ini menampilkan halaman atau proses yang terjadi saat dokter memilih untuk keluar dari sistem rekam medis elektronik setelah menyelesaikan aktivitas pada sistem.



Gambar 3.6 Tampilan Halaman Keluar

3.2. Pengujian Prototype

Pengujian terhadap *Two Factor Authentication* pada Sistem *Login* Rekam Medis Elektronik telah dilakukan menggunakan total 200 data uji. Data tersebut diperoleh melalui partisipasi 10 pengguna, dimana masing-masing pengguna menguji 20 poin fungsionalitas sistem yang terdiri dari beberapa kelompok halaman registrasi dan *login*. Seluruh proses pengujian berhasil diselesaikan dengan hasil yang memuaskan. Berdasarkan hasil tersebut, dapat disimpulkan bahwa *Two Factor Authentication* pada Sistem *Login* Rekam Medis Elektronik telah berhasil memenuhi standar fungsionalitas yang telah ditetapkan.

$$\text{Perhitungan} = \frac{200}{200} \times 100\% = 100\%$$

Hasil perhitungan pengujian fungsionalitas menunjukkan bahwa implementasi fitur *Two-Factor Authentication* pada Sistem *Login* Rekam Medis Elektronik berbasis *Web* mencapai tingkat keberhasilan yang sangat tinggi, dengan persentase kesuksesan mencapai 100% dengan Nilai Akurasi perhitungan Sangat Tinggi. Hal ini mengindikasikan bahwa fitur tersebut dengan fungsionalitas yang sesuai dengan standar perhitungan yang telah ditetapkan.

3.3. Evaluasi Prototype

Evaluasi ini bertujuan menilai efektivitas, fungsionalitas, dan kemudahan penggunaan *Two-Factor Authentication* pada Sistem *Login* Rekam Medis Elektronik berbasis *web*. Proses ini melibatkan Bapak Muhamad Ali Jafar, S.Fis., Ftr., M.Fis., pemilik Praktek Fisioterapi Mandiri BioPhisyio. Berdasarkan evaluasi yang didokumentasikan, mitra tidak memberikan umpan balik tambahan dan menyatakan fungsionalitas sistem sudah memadai.

4. Kesimpulan

Two-Factor Authentication pada Sistem *Login* Rekam Medis Elektronik di Praktek Fisioterapi Mandiri BioPhisyio, Rejowinangun, Yogyakarta, berhasil dikembangkan menggunakan metode *Prototype* dan *framework* CodeIgniter. Tahapannya meliputi Pengumpulan data, Desain, Implementasi, Pengujian, dan Evaluasi *Prototype*. Evaluasi dilakukan sekali dengan umpan balik dari mitra, yang menyetujui hasilnya. Pengujian menggunakan metode *Black-box Testing* dengan *Equivalence Partitioning* menunjukkan seluruh fitur berfungsi dengan baik dan sistem memiliki akurasi tinggi sesuai dengan fungsionalitas yang diimplementasikan.

Daftar Pustaka

- Abduh, R. (2021). Kajian Hukum Rekam Medis Sebagai Alat Bukti Malapraktik Medis. *DE LEGA LATA: Jurnal Ilmu Hukum*, 6(1), 221–233.
- Aprilia, T., Pitoyo, B. S., Fauzi, A., Ramadhanti, R. G., & Dwi, R. (2024). 2024 Madani : Jurnal Ilmiah Multidisiplin Pengaruh Keamanan Two Factor Authentication Terhadap Pencurian Data (Cyber Crime) Pada Media Sosial 2024 Madani : Jurnal Ilmiah Multidisiplin. 2(5), 449–458.
- Azhar, Arkarni Wais, & Atthariq. (2020). Sistem Keamanan Pada Halaman Login Menggunakan One Time Password. *Journal of Embedded System, Security, and Intelligent System*, 01(2), 106–113.
- Dewa Made Andika Dwi Prawiradirjo, Kartiko, B. H., & Feoh, G. (2018). Elektronik Rawat Jalan Berbasis Web. *Elektronik Rawat Jalan Berbasis Web*, 4(1), 31–41.
- Herdiantoro, H. R., & Islami, M. R. R. (2023). IMPLEMENTASI TWO-FACTOR AUTHENTICATION (2FA) DAN FIREWALL POLICIES DALAM MENGAMANKAN WEBSITE. 4(1).
- Heriyanto, Y., Qalban, A. A., & Mukaromah, I. A. (2022). Pengembangan Metode Login Two Factor Authentication (2FA) untuk Keamanan Sistem Informasi Akademik. 142–150.
- Kevin Pitch. (2023). *Google Workspace Guide Unlock Every Google App – Elevate Efficiency with Exclusive Tips, Time-Savers & Step-by-Step Screenshots for Quick Mastery.*
- Khasanah, M. (2020). TANTANGAN PENERAPAN REKAM MEDIS ELEKTRONIK UNTUK. *Urnal Sainstech Politeknik Indonusa Surakarta*, 7.
- Krisna, W., Muhammad, H. J., & Ambadar, N. (2022). Rancang Bangun Sistem Informasi Akademik Menggunakan Framework Codeigniter Pada universitas Muhammadiyah Purworejo. *Jurnal Sistem Cerdas*, 5(2), 107–116. <https://doi.org/10.37396/jsc.v5i2.187>
- MASHADOV, M. B. (2020). SISTEM INVENTORI GUDANG PADA TOKO JB DISTRO MENGGUNAKAN FRAMEWORK CODEIGNITER.
- Neng Sari Rubiyanti. (2023). Penerapan Rekam Medis Elektronik di Rumah Sakit di Indonesia: Kajian Yuridis. *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora*, 1(1), 179–187. <https://doi.org/10.59246/aladalah.v1i1.163>
- Pressman, R. S., & Maxim, B. R. (2020). *Software Engineering*.
- Sarah Hapsari, N., Fatman, Y., & Penulis Korespondensi, E. (2020). JURNAL MEDIA INFORMATIKA BUDIDARMA Implementasi Metode One Time Password pada Sistem Pemesanan Online. *Jurnal Media Informatika Budidarma*, 4, 930–939. <https://doi.org/10.30865/mib.v4i4.2195>
- Sari, O. M. (2020). Sistem informasi rekam medis pada dinas kesehatan kabupaten musirawas berbasis web mobile. 05(02), 141–156.
- Sofia, S., Ardianto, E. T., Muna, N., & Sabran, S. (2022). Analisis Aspek Keamanan Informasi Data Pasien Pada Penerapan RME di Fasilitas Kesehatan. *Jurnal Rekam Medik & Manajemen Informasi Kesehatan*, 1(2), 94–103. <https://doi.org/10.47134/rmik.v1i2.29>
- Taufiq, R., Prianggodo, D. Y., Sugiani, Y., Andini, N., Informatika, T., Teknik, F., Tangerang, U. M., & Tangerang, C. (2023). PENGGUNAAN METODE PROTOTYPE PADA PENGEMBANGAN SISTEM. 7(4), 431–439.