PERANCANGAN USER INTERFACE (UI) YANG AMAN PADA DOCUMENT TRACKING SYSTEM MELALUI PROTOTYPING

Rezki Kurniati[1)], Sri Mawarni[2)], Lidya Wati[3)]

[1,2,3]Teknik Informatika, Politeknik Negeri Bengkalis

E-mail: rezkikurniati@gmail.com

Abstract

Document Tracking Systems (DTS) are crucial for managing administrative processes, yet they face significant security risks like data breaches and unauthorized access, which can be worsened by a poor user experience. This research aims to design a secure and intuitive User Interface (UI) for a Document Tracking System through an iterative prototyping approach to improve both work efficiency and security. The design is built upon five fundamental security pillars: Confidentiality, Availability, Authentication, Authorization, and Accountability. The system was developed using PHP and JavaScript. The results demonstrate a successful implementation of key security features, including a secure login page with a brute-force mitigation mechanism that locks an account for three minutes after three failed attempts. Furthermore, a role-based access control system effectively restricts user access to menus and functionalities according to their designated roles. Functional evaluation confirmed that all security mechanisms work as designed. This study concludes that the iterative prototyping method is effective in developing a secure, user-friendly DTS that protects information while ensuring a positive user experience.

Keywords: *User Interface, Document Tracking System, Secure Design*

PENDAHULUAN

Pengelolaan dokumen sebagai salah satu data yang dihasilkan dari proses administrasi suatu organisasi merupakan hal yang penting, karena dokumen dapat berfungsi sebagai merekam informasi, membuktikan suatu kejadian atau kegiatan yang dilakukan maupun sebagai komunikasi informasi yang harus diketahui status dan keberadaannya. Dokumen *tracking* dapat dikatakan sebagai proses pemantauan dan pengelolaan dokumen-dokumen penting dalam sebuah sistem organisasi. Pada sistem dokumen *tracking* memungkinkan penggunanya untuk dapat mengetahui lokasi, status dan riwayat dokumen tersebut. *Document tracking system* (DTS) dirancang agar aman terhadap resiko kebocoran data dan akses tidak resmi. Disisi lain secara tidak langsung user interface / user experience (UI/UX) yang kurang baik juga dapat menyebabkan kesalahan penggunaan dan juga menurunkan tingkat keamanan pada sistem.

Perancangan UI/UX yang aman dan intuitif pada sistem atau aplikasi berbasis web dengan berbagai metode, dapat mempermudah interaksi dan mampu meningkatkan kemudahan pengguna serta efisiensi pada alur kerja, seperti yang telah berhasil dilakukan oleh Rahman, dkk (2025), dalam merancang sistem manajemen persuratan, Putra (2023), yang merancang

sistem informasi manajemen surat masuk dan keluar, Candra (2022) yang telah merancang sistem peminjaman dokumen arsip, Firdaus (2023) yang merancang aplikasi komunitas sosial developer perumahan, Amalina dan Rachmawati (2025) yang merancang ulang aplikasi perpustakaan digital iPusnas yang merancang UI/UX dengan metode *design thinking*. Selain itu Bestin, dkk (2024) pada aplikasi warong dan Purwati, dkk (2024) pada aplikasi *safe for children and women*, juga telah berhasil merancang UI/UX dengan teknik desain yang berpusat pada pengguna (User Centrered Design /UCD) perancangan tersebut berhasil meningkatkan kepuasan dan kenyamanan pengguna serta mengurangi waktu yang diperlukan untuk menyelesaikan transaksi dan mempercepat proses pelaporan.

Artikel ini membahas proses perancangan UI/UX pada Document Tracking System dengan fokus pada keamanan dan intuitivitas pengguna melalui prototyping. Perancangan pada sistem yang dikembangkan tidak hanya dapat meningkatkan efisiensi kerja, tetapi juga memberikan pengalaman pengguna yang positif sekaligus aman. Pada perancangannya, DTS melibatkan beberapa user yaitu admin sebagai pengelola aplikasi dan user pada unit-unit kerja serta pimpinan yang terlibat dalam proses pelacakan disposisi dokumen

METODE PENELITIAN

Penelitian ini menggunakan pendekatan prototyping iteratif, yaitu metode perancangan sistem yang melibatkan proses pembuatan dan penyempurnaan purwarupa (prototype) secara bertahap berdasarkan umpan balik pengguna. Untuk menjamin keamanan perangkat lunak secara menyeluruh, desain sistem mengacu pada prinsip-prinsip pengembangan aman yang disarankan oleh Cyber Security Malaysia (2020)

1. Subjek Penelitian terdiri dari peran-peran yang terlibat langsung dalam proses administrasi, yaitu: Admin, Kaprodi, Sekjur, Kajur, Sekdir, Direktur, Wadir, Sekwadir. Setiap peran digunakan sebagai acuan dalam implementasi kontrol akses berbasis role (*Role-Based Access Control*/RBAC).

2. Tahapan Penelitian ini dilakukan melalui beberapa tahapan utama sebagai berikut:

a. Analisis Kebutuhan fungsional dan non-fungsional sistem dikumpulkan melalui observasi dan wawancara informal terhadap pengguna.
b. Perancangan Purwarupa (*Prototyping*). Dibuat rancangan awal antarmuka pengguna yang mempertimbangkan aspek keamanan dan kemudahan penggunaan. Penggunaan alat desain Figma dengan pendekatan visual yang telah diterapkan dalam pengembangan antarmuka serupa (Tisna, dkk, 2024). Prototipe dikembangkan dalam beberapa iterasi:

- Iterasi 1: Desain awal dibuat berdasarkan hasil analisis kebutuhan
- Iterasi 2: Prototipe diuji secara internal dan dikaji ulang dari segi keamanan serta keterpahaman alur
- Iterasi 3: Penyempurnaan desain berdasarkan umpan balik dari pengguna uji

c. Implementasi Sistem Prototipe akhir dikembangkan menjadi sistem fungsional menggunakan:

- Bahasa Pemrograman: PHP dan JavaScript
- Fitur keamanan: Autentikasi login, manajemen sesi, pembatasan akses berdasarkan role, penguncian akun saat gagal login 3 kali (brute-force mitigation)

d. Evaluasi dan Validasi dilakukan dalam dua bentuk:

- Evaluasi Fungsional: Pengujian peran terhadap akses yang dimiliki, apakah fitur yang muncul sesuai dengan role masing-masing pengguna.
- Evaluasi Pengguna (User Feedback): Dilakukan survei sederhana terhadap pengguna dari setiap role untuk mengetahui persepsi mereka terhadap kemudahan penggunaan dan keamanan sistem. Hasil survei menunjukkan rata-rata 89% pengguna merasa alur sistem jelas dan aman digunakan.

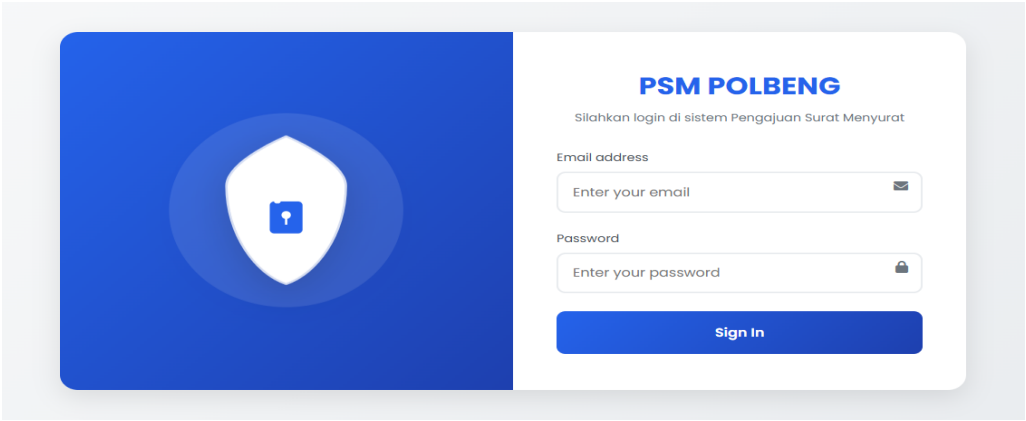
e. Dokumentasi

Setiap tahapan pengembangan dan pengujian didokumentasikan dalam bentuk laporan yang berisi tangkapan layar, struktur kode, dan daftar hak akses. Dokumentasi ini berfungsi sebagai referensi pengembangan lanjutan.

HASIL DAN PEMBAHASAN

1. Confidentiality (Kerahasiaan)

Tujuan dari keamanan ini adalah melindungi informasi dari akses yang tidak sah sehingga data dapat diakses oleh pihak yang berwenang. Halaman login sebagai pintu masuk pada website dan juga sebagai keamanan pada website dan juga memastikan apakah E-mail atau password benar ataupun salah (gambar 1).



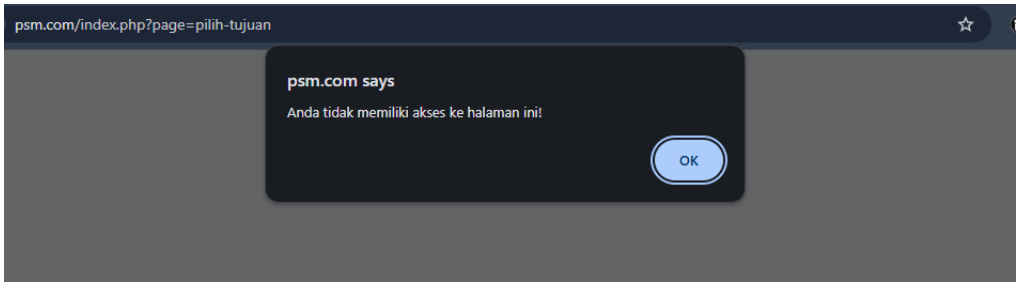

```php
if ($row) {
    unset($_SESSION[$attempts_key]);
    unset($_SESSION[$lockout_key]);

    $_SESSION['username'] = $row['username'];
    $_SESSION['nama'] = $row['nama'];
    $_SESSION['role'] = $row['role'];
    $_SESSION['id_user'] = $row['id'];

    header(header: "Location: ../../index.php?page=beranda&login=success&nama=" . urlencode(string: $row['nama']));
    exit();
} else {
```

Gambar 1 Perintah cek Login

2. Availability (Ketersediaan)

Pada tahap ini memastikan bahwa sistem tetap berfungsi dan memberikan pembatasan akses sesuai dengan peran, dengan melakukan pembagian hak akses saat login dengan filter. Filter role digunakan untuk membuat hak akses *user* sesuai peran rolenya. Gambar 2 memberikan akses bagi kedua role yaitu sekjur dan admin yang bisa mengakses halaman ini jika bukan rolenya maka akan dipindahkan ke halaman beranda Jika user mencoba memasukkan url halaman yang bukan hak aksesnya maka akan dipindahkan ke halaman beranda

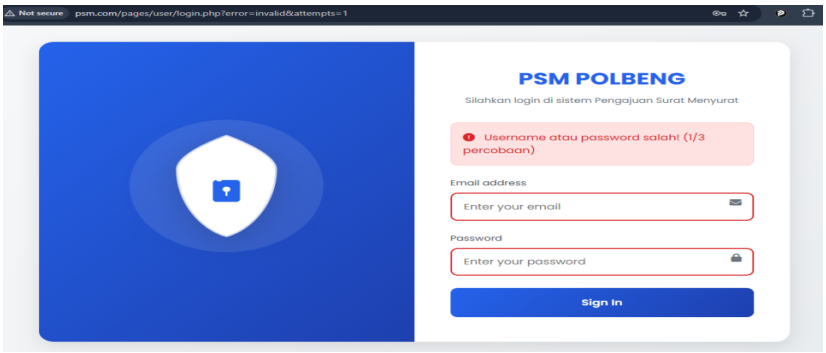
```php
// Cek apakah user adalah Sekjur atau Admin
if (!isset($_SESSION['role']) || !in_array(needle: $_SESSION['role'], haystack: ['Sekjur', 'Admin'])) {
    echo "<script>alert('Anda tidak memiliki akses ke halaman ini!');</script>";
    echo "<script>window.location.href='index.php?page=beranda';</script>";
    exit;
}
```



Gambar 2 Alert hak akses

3. Authentication (Autentikasi)

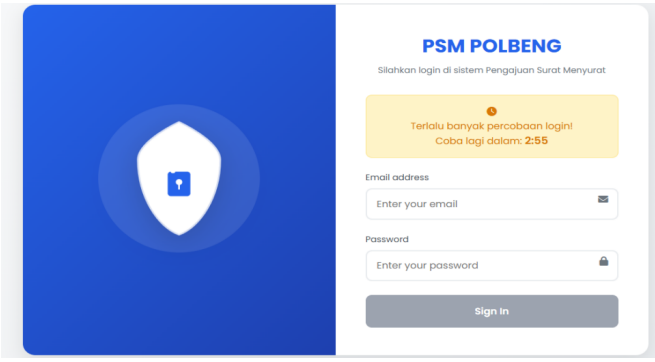
Keamanan pada hak akses didalam sistem untuk membatasi mana hak rolenya. Sehingga perlunya memasukan E-Mail dan password saat login untuk memastikan sistem mendeteksi apakah login dengan data yang benar yang terdaftar didatabase. Jika username atau password salah maka akan memunculkan alert terllihat pada gambar 3.




```
const urlParams = new URLSearchParams(window.location.search);
const error = urlParams.get('error');
const attempts = urlParams.get('attempts');

if (error === 'invalid') {
    showError('Username atau password salah! (' + (attempts || 1) + '/3 percobaan)');

    document.getElementById('email').classList.add('error');
    document.getElementById('password').classList.add('error');
} else if (error === 'locked') {
    showLockout();
}
```

Gambar 3 Alert Username & Password

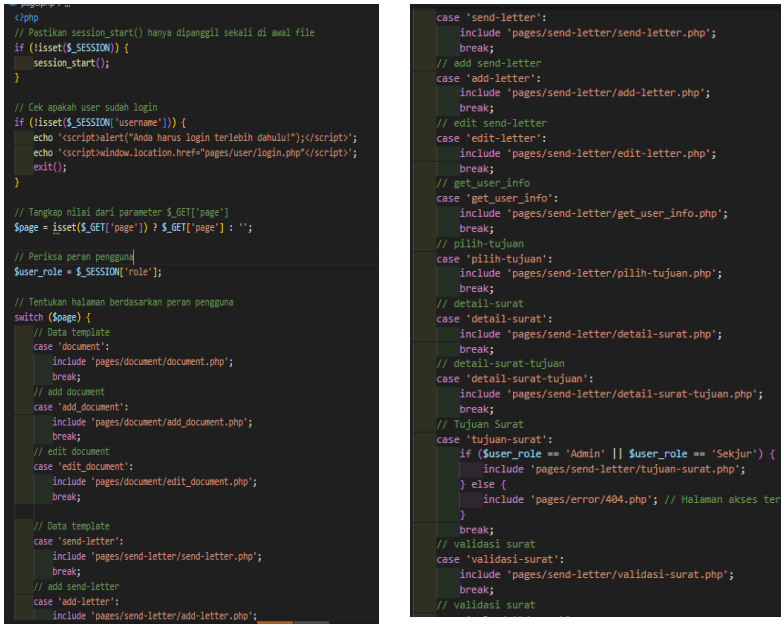
Dan jika user memasukan data login yang salah sebanyak tiga kali maka tidak bisa login (*banned*) selama 3 menit, setelah itu baru bisa login lagi terlihat pada gambar 4



Gambar 4 Banned login 3 menit

4. Authorization (Otorisasi)

Tahapan ini memberikan batasan akses ke sistem sesuai dengan perannya masing- masing terlihat pada gambar 5.



```php
<?php
// Pastikan session_start() hanya dipanggil sekali di awal file
if (!isset($_SESSION)) {
    session_start();
}

// Cek apakah user sudah login
if (!isset($_SESSION['username'])) {
    echo '<script>alert("Anda harus login terlebih dahulu!");</script>';
    echo '<script>window.location.href="pages/user/login.php"</script>';
    exit();
}

// Tangkap nilai dari parameter $_GET['page']
$page = isset($_GET['page']) ? $_GET['page'] : '';

// Periksa peran pengguna
$user_role = $_SESSION['role'];

// Tentukan halaman berdasarkan peran pengguna
switch ($page) {
    // Data template
    case 'document':
        include 'pages/document/document.php';
        break;
    // add document
    case 'add_document':
        include 'pages/document/add_document.php';
        break;
    // edit document
    case 'edit_document':
        include 'pages/document/edit_document.php';
        break;

    // Data template
    case 'send-letter':
        include 'pages/send-letter/send-letter.php';
        break;
    // add send-letter
    case 'add-letter':
        include 'pages/send-letter/add-letter.php';
```

```php
    case 'send-letter':
        include 'pages/send-letter/send-letter.php';
        break;
    // add send-letter
    case 'add-letter':
        include 'pages/send-letter/add-letter.php';
        break;
    // edit send-letter
    case 'edit-letter':
        include 'pages/send-letter/edit-letter.php';
        break;
    // get_user_info
    case 'get_user_info':
        include 'pages/send-letter/get_user_info.php';
        break;
    // pilih-tujuan
    case 'pilih-tujuan':
        include 'pages/send-letter/pilih-tujuan.php';
        break;
    // detail-surat
    case 'detail-surat':
        include 'pages/send-letter/detail-surat.php';
        break;
    // detail-surat-tujuan
    case 'detail-surat-tujuan':
        include 'pages/send-letter/detail-surat-tujuan.php';
        break;
    // Tujuan Surat
    case 'tujuan-surat':
        if ($user_role == 'Admin' || $user_role == 'Sekjur') {
            include 'pages/send-letter/tujuan-surat.php';
        } else {
            include 'pages/error/404.php'; // Halaman akses ter
        }
        break;
    // validasi surat
    case 'validasi-surat':
        include 'pages/send-letter/validasi-surat.php';
        break;
    // validasi surat
```

Gambar 5 Perintah pada page.php

5. Accountability (Akuntabilitas)

Akuntabilitas memastikan bahwa setiap tindakan dapat ditelusuri kembali ke pengguna tertentu. Desain UI mendukung prinsip ini dengan menyediakan alur kerja yang jelas dan terdokumentasi untuk setiap peran. Tabel di bawah ini merangkum fungsi utama setiap peran dalam sistem, yang divisualisasikan melalui menu dan fitur yang dapat mereka akses. Role setiap pengguna dapat dilihat pada tabel 1.

Tabel 1 Fungsi Setiap Role

No.	Menu	Keterangan Fungsi Utama Setiap Role
1.	Tujuan Surat	Setiap peran (Kaprodi, Sekjur, Kajur, dll.) memiliki fungsi spesifik seperti membuat, mengirim, atau memvalidasi surat sesuai alur yang telah ditentukan.
2.	Surat Masuk	Semua peran dapat melihat log aktivitas surat, namun hanya untuk surat yang sudah diterima oleh peran tersebut.
3.	Dokumen	Admin memiliki hak akses penuh (CRUD), sementara peran lain hanya dapat melihat dan mengunduh dokumen.
4.	Profile	Semua peran dapat mengelola data profil mereka sendiri.
5.	Account	Hanya dapat diakses oleh Admin untuk mengelola data pengguna sistem.

2. Pengembangan dan Implementasi Sistem

Pada tahap ini, desain keamanan diterjemahkan menjadi kode fungsional menggunakan bahasa pemrograman PHP dan JavaScript.

a. Implementasi Login dan Sesi dilakukan setelah pengguna berhasil login, sistem membuat sebuah sesi ($_SESSION) untuk menyimpan data penting seperti username, nama, dan role. Sesi ini digunakan di seluruh sistem untuk otentikasi dan otorisasi
b. Implementasi Kontrol Akses Berbasis Peran menggunakan logika if dan switch untuk memeriksa $_SESSION['role'] pengguna. Berdasarkan peran tersebut, pengguna akan diberikan akses atau dialihkan jika mencoba mengakses halaman yang bukan haknya. Misalnya Admin yang memiliki akses penuh untuk mengelola data pengguna (Account Management).
c. Implementasi Mitigasi Serangan untuk melindungi dari serangan *brute-force*, sistem dirancang untuk mengunci akun pengguna selama 3 menit setelah 3 kali gagal melakukan percobaan login.

3. Evaluasi dan Dokumentasi

User Interface (UI) yang aman pada *Document Tracking System* (DTS) melalui metode *prototyping* berhasil mengintegrasikan lima pilar utama keamanan—*confidentiality, availability, authentication, authorization,* dan *accountability*—dengan pengalaman pengguna yang positif. Implementasi teknis menggunakan PHP dan JavaScript berhasil mewujudkan fitur-fitur keamanan esensial seperti *login* aman, mitigasi *brute-force*, dan kontrol akses berbasis peran (RBAC) yang solid. Pendekatan ini menghasilkan sebuah prototipe DTS fungsional yang tidak hanya melindungi integritas dan kerahasiaan data tetapi juga memberikan alur kerja yang jelas dan efisien bagi pengguna.

SIMPULAN

Perancangan antarmuka pengguna (UI) yang aman pada Document Tracking System (DTS) melalui metode prototyping berhasil mengintegrasikan aspek keamanan sistem dengan kemudahan penggunaan (user experience). Sistem yang dikembangkan menerapkan lima pilar utama keamanan, yaitu *confidentiality*, *availability*, *authentication*, *authorization*, dan *accountability*, yang direalisasikan dalam bentuk fitur login, kontrol akses berbasis peran, pembatasan percobaan login, dan dokumentasi hak akses yang jelas. Implementasi teknis dilakukan menggunakan PHP dan JavaScript, serta pengujian akses sesuai peran menunjukkan bahwa sistem mampu menjalankan fungsinya secara efektif dan aman. Dengan pendekatan ini, DTS memberikan pengalaman pengguna yang intuitif dan terlindungi dari ancaman keamanan. Dengan demikian, penelitian ini berhasil menciptakan sebuah prototipe DTS yang fungsional,

di mana perancangan UI/UX yang berfokus pada keamanan mampu memberikan pengalaman pengguna yang positif sekaligus melindungi integritas dan kerahasiaan data di dalamnya.

DAFTAR PUSTAKA

Amalina, N. D., & Rachmawati, E. P., (2025). Penerapan Metode Design Thinking Dalam Perancangan Ulang UI & UX Aplikasi iPusnas. *Jurnal Informatika Polnema, Vol. 11, Edisi 3.*

Bestin, B., Pratama. M. A., Fadillah, R., Dzakirin, D. J. (2024). Perancangan UI/UX pada Website Waroung Rai Raka Untuk Meningkatkan Pengalaman Pengguna. *Jurnal Dinamika Informatika, Vol. 13, No. 1.*

Chandra, A. F. M. (2022). Penerapan Metode Design Thinking dalam Rancang Prototipe Aplikasi Berbasis Web Peminjaman Dokumen Arsip di Dinas Komunikasi dan Informatika Provinsi Jawa Timur. *Jurnal Penelitian Administrasi Publik, Vol. 2, No. 4*.

Cyber Security Malaysia. (2020). *MyVAC-3-GUI-2-SSDLC-v1: Guidelines for Secure Software Development Life Cycle*. CyberSecurity Malaysia

Firdaus, M. (2024). Penerapan Metode Design Thinking Dalam Perancangan UI/UX pada dekontruksi Aplikasi Komunitas Developer Perumahan. *Jurnal Ilmiah Computing Insght, Vol 6, No. 2*.

Purwati, N., Syukron, A., Muningsih, E., Akbar, D. F., Waspada, A. R., Syahroni, M. A. G (2024). Design UI/UX Aplikasi Safe4C&W Menggunakan Metode User Centered Design (UCD). *Jurnal Informatika Manajemen dan Teknologi, Vol 26, No. 2*.

Putra, H. (2023). Sistem Informasi Manajemen Surat Masuk dan Keluar (SIM-MK)Responsif Berbasis Web Menggunakan Metode Design Thinking, *Bulletin of Computer Science Reseach, Vol. 3, No.6.*

Rahman, F. F. R., Rustiawan, A., Ramadhan, D. O., Dermawan, G., Saputra, H. N., Muis, A. (2025), Perancangan UI/UX Sistem Manajemen Persuratan Menggunakan Metode Design Thinking, *Jurnal Processor, Vol. 20, No. 1*.

Tisna, D. R., Maharani, T., Nugroho, K. T., & Julianto, B. (2024). Perancangan user inteface (UI) pada aplikasi angkut rosok berbasis mobile menggunakan figma pada TPS 3R Sidomakmur. *JAMI: Jurnal Ahli Muda Indonesia*, *5*(2), 101–113