Implementasi Zero Trust Access Control pada Aplikasi Sederhana

kelompok 4
Luthfi Kurniawan (2201020013)
M. Afief Anugrah (2201020015)
Aditya Firmansyah (2201020018)
Halta Putra Ash Sidiq (2201020092)

Laporan Mingguan 1: Perancangan Role & Use Case

1. Deskripsi Proyek Singkat

Proyek ini bertujuan mengimplementasikan **Zero Trust Access Control** pada **Aplikasi Sederhana Manajemen Dokumen**. Aplikasi ini memungkinkan pengguna dengan peran yang berbeda untuk mengelola dan mengakses dokumen sesuai dengan hak istimewa terkecil yang diberikan.

2. Konsep Zero Trust dalam Perancangan

Perancangan ini mengintegrasikan tiga prinsip inti Zero Trust:

- **Verify Explicitly (Verifikasi Secara Eksplisit):** Semua user harus melalui proses verifikasi identitas (Login) sebelum akses diberikan ke sumber daya apa pun.
- **Least Privilege Access (Akses Hak Istimewa Paling Kecil):** Hak akses terhadap fungsionalitas kritis (seperti **Mengunggah, Mengedit, dan Menghapus Dokumen**) dibatasi ketat melalui RBAC.
- **Assume Breach (Anggap Sudah Terbobol):** Desain mencakup fitur mitigasi seperti **Melihat Log Audit** dan penerapan **Session Timeout** untuk membatasi dampak jika terjadi pelanggaran keamanan.

3. Perancangan Role-Based Access Control (RBAC)

3.1. Definisi Peran (Roles)

Role (Peran)	user	Deskripsi Singkat
Admin	Manajer Sistem	Memiliki hak akses tertinggi. Bertanggung jawab mengelola pengguna dan semua dokumen, serta melihat log audit.
Editor	Kontributor Data	Bertanggung jawab mengunggah, melihat, dan mengedit dokumen. Tidak dapat menghapus dokumen atau mengelola pengguna.
Viewer	Pengguna Biasa	Memiliki hak istimewa paling kecil. Hanya dapat melihat dokumen.

3.2. Perancangan Izin (Permissions)

Permission (Izin)	Aksi yang Diizinkan	Resource (Sumber Daya)
upload_doc	Mengunggah Dokumen baru.	Modul Dokumen
view_doc	Melihat/membaca Dokumen.	Modul Dokumen

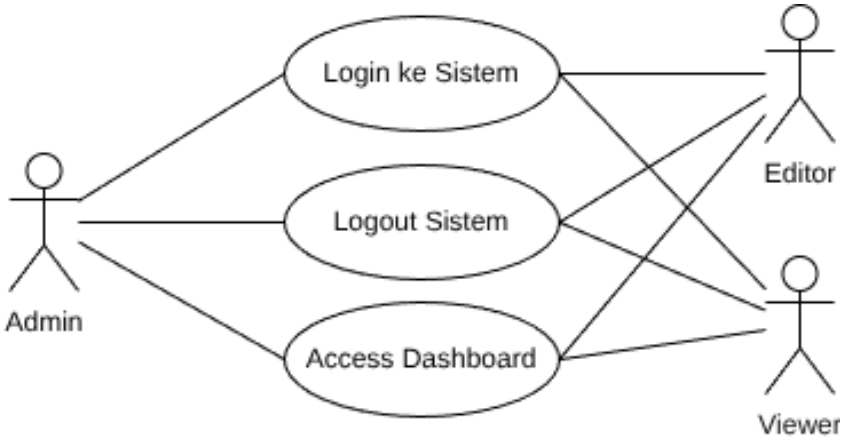
edit_doc	Mengedit Dokumen yang sudah ada.	Modul Dokumen
delete_doc	Menghapus Dokumen.	Modul Dokumen
manage_users	Mengelola (membuat, mengubah, menghapus) akun pengguna.	Modul Pengguna
view_audit	Melihat Log Audit sistem.	Modul Keamanan

3.3. Pemetaan Peran & Izin

Peran	Izin yang Dimiliki
Admin	upload_doc, view_doc, edit_doc, **delete_doc**, **manage_users**, **view_audit**
Editor	upload_doc, view_doc, edit_doc
Viewer	view_doc

4. Perancangan Use Case Kritis

4.1. Visualisasi Use Case 1



4.1.1 Diagram Use Case Dasar Sistem

1. User

User adalah pengguna yang berinteraksi dengan sistem. Terdapat tiga (3) jenis user dalam diagram ini, masing-masing dengan peran dan hak akses yang berbeda:

- **Admin:** Memiliki hak akses tertinggi.
- **Editor:** Memiliki hak akses untuk mengedit, tetapi lebih terbatas dari Admin.
- **Viewer:** Memiliki hak akses paling dasar, biasanya hanya untuk melihat.

2. Use Case (Fungsi Sistem)

Use Case adalah fungsi atau aktivitas yang disediakan oleh sistem:

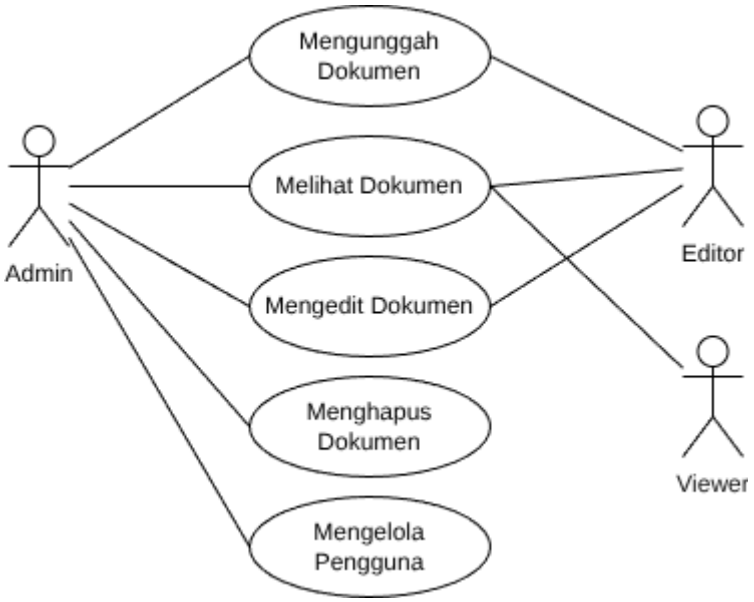
- **Login ke Sistem:** Proses masuk ke dalam sistem menggunakan kredensial (nama pengguna dan kata sandi).
- **Logout Sistem:** Proses keluar dari sistem.
- **Access Dashboard (Akses Dashboard):** Proses untuk masuk dan melihat halaman utama atau ringkasan (dashboard) sistem.

3. Hubungan (Interaksi)

Garis yang menghubungkan user dan *use case* menunjukkan bahwa user tersebut dapat menjalankan fungsi (*use case*) tersebut:

Use Case	Admin	Editor	Viewer	Penjelasan Interaksi
Login ke Sistem	Ya	Ya	Ya	Ketiga user (Admin, Editor, dan Viewer) harus melakukan Login ke Sistem untuk memulai interaksi.
Logout Sistem	Ya	Ya	Ya	Ketiga user dapat melakukan Logout Sistem untuk mengakhiri sesi.
Access Dashboard	Ya	Ya	Ya	Ketiga user dapat mengakses Dashboard setelah login.

4.2. Visualisasi Use Case 2



4.1.2 Diagram Use Case Fungsional (Manajemen Dokumen)

1. Use Case (Fungsi Sistem)

Terdapat lima fungsi utama yang digambarkan:

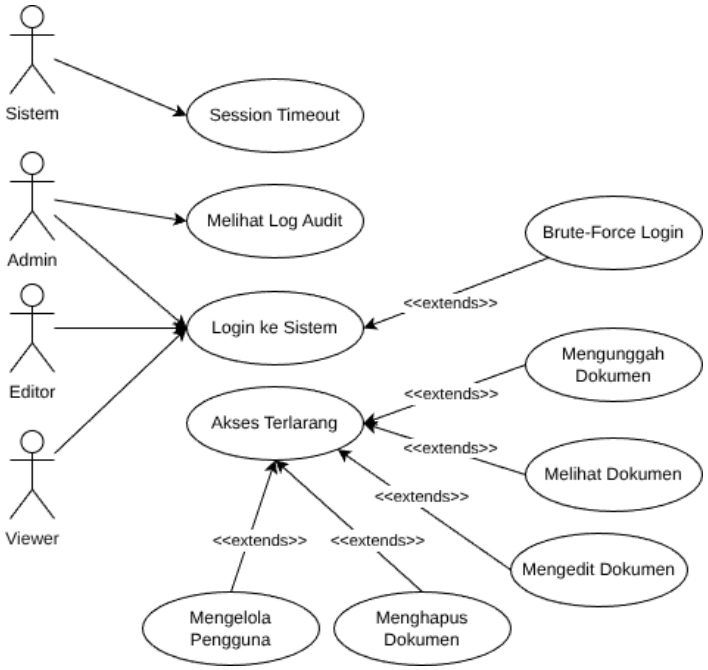
1. **Mengunggah Dokumen:** Proses menambahkan dokumen baru ke sistem.
2. **Melihat Dokumen:** Proses menampilkan atau membaca dokumen yang ada di sistem.
3. **Mengedit Dokumen:** Proses memodifikasi isi atau detail dari dokumen yang sudah ada.
4. **Menghapus Dokumen:** Proses menghilangkan dokumen dari sistem secara permanen.
5. **Mengelola Pengguna:** Proses mengatur akun pengguna lain, termasuk menambah, mengedit, atau menghapus pengguna.

2. Hubungan dan Hak Akses (Ringkasan Interaksi)

Berikut adalah detail hak akses dan interaksi setiap user terhadap fungsi-fungsi tersebut:

Use Case	Admin	Editor	Viewer	Penjelasan Hak Akses
Mengunggah Dokumen	Ya	Ya	Tidak	Admin dan Editor dapat mengunggah dokumen baru. Viewer tidak bisa.
Melihat Dokumen	Ya	Ya	Ya	Semua user dapat melihat dokumen. Ini adalah hak akses paling dasar.
Mengedit Dokumen	Ya	Ya	Tidak	Admin dan Editor dapat mengedit dokumen. Viewer hanya bisa melihat.
Menghapus Dokumen	Ya	Tidak	Tidak	Hanya Admin yang memiliki hak untuk menghapus dokumen. Editor dan Viewer tidak memiliki hak ini.
Mengelola Pengguna	Ya	Tidak	Tidak	Hanya Admin yang dapat mengelola pengguna lain. Ini menegaskan bahwa Admin adalah user dengan hak administrator penuh.

4.3. Visualisasi Use Case 3



4.1.3 Diagram Use Case Keamanan dan Mitigasi Zero Trust

1. **user (Pelaku)**

   user yang terlibat adalah:

- **Sistem:** user non-manusia yang mewakili sistem itu sendiri, biasanya menginisiasi tindakan internal.
- **Admin, Editor, Viewer:** Pengguna sistem, seperti di diagram sebelumnya.

2. **Use Case (Fungsi Sistem)**

- **Session Timeout (Waktu Sesi Habis):** Fungsi yang diinisiasi oleh Sistem.
- **Melihat Log Audit:** Fungsi untuk melihat catatan semua aktivitas dan perubahan dalam sistem.
- **Login ke Sistem:** Proses masuk (diinisiasi oleh semua pengguna).
- **Akses Terlarang:** *Use case* yang menggambarkan kegagalan atau penolakan akses ke fungsi tertentu.

- **Fungsi Dokumen & Pengguna:**
    - Mengunggah Dokumen
    - Melihat Dokumen
    - Mengedit Dokumen
    - Menghapus Dokumen
    - Mengelola Pengguna

3. Hubungan Lanjutan dan *Extends*

Di diagram ini, ada dua jenis hubungan penting selain hubungan user ke *use case* (yang sudah Anda lihat sebelumnya):

A. Hubungan

Interaksi	Penjelasan
Sistem → Session Timeout	Sistem secara otomatis menginisiasi proses "Session Timeout" (misalnya, mengeluarkan pengguna setelah waktu tertentu tanpa aktivitas).
Admin → Melihat Log Audit	Hanya Admin yang dapat melihat catatan keamanan dan aktivitas (Log Audit), menekankan peran Admin dalam pemantauan keamanan.
Admin, Editor, Viewer → Login ke Sistem	Ketiga user dapat melakukan proses Login ke Sistem.

B. Hubungan *Extends* (<<extends>>)

Hubungan *extends* menunjukkan bahwa sebuah *use case* tambahan (ekstensi) dapat terjadi secara opsional dari *use case* dasar dalam kondisi tertentu.

1. **Login ke Sistem ← Brute-Force Login**
    - Jika proses Login ke Sistem dilakukan dengan cara yang mencurigakan (misalnya, mencoba kata sandi berulang kali dalam waktu singkat), maka skenario Brute-Force Login akan terjadi sebagai ekstensi/kasus opsional dari *use case* dasar.
2. **Akses Terlarang ← (Fungsi Dokumen & Pengguna)**
    - Ini adalah bagian yang paling signifikan. Jika seorang pengguna mencoba salah satu fungsi yang terhubung (Mengunggah, Melihat, Mengedit, Menghapus Dokumen, atau Mengelola Pengguna), tetapi pengguna tersebut tidak memiliki hak akses yang memadai untuk fungsi tersebut, maka skenario Akses Terlarang akan terjadi sebagai ekstensi.
    - Contoh: Jika Viewer (yang hanya boleh Melihat) mencoba Mengedit Dokumen, maka sistem akan mengaktifkan *use case* Akses Terlarang.