Data Integrity and Authentication Final Project Report

Team Members:

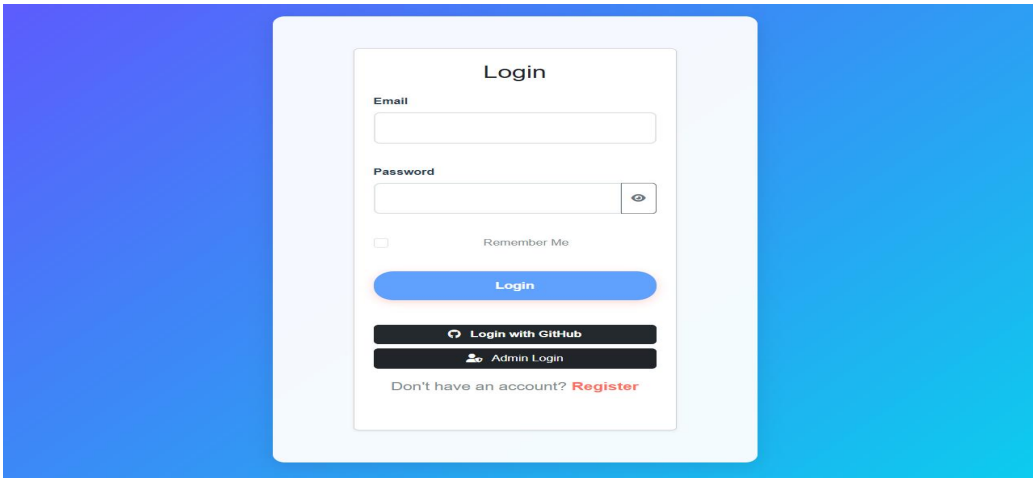
Omar Hossam Ahmed	2205150
Sally Bahgat Mofeed	2205190
Abdelrahman Aymen Elsayed	2205197
Hossam Ahmed Eldousky	2205097
Tarek Gamal Mohamed	2205029

Introduction:

SecureDocs is a secure, web-based document management platform focused on protecting sensitive digital content through strong authentication, encryption, and access control. It provides users with a safe environment to upload, sign, store, and manage documents—simulating enterprise-grade document security used in legal, HR, or enterprise settings.

In this project we uses a combination of modern login and credit lines, ensuring that each user is securely verified. The system includes:

Login Page:



The user can log in in 3 ways:

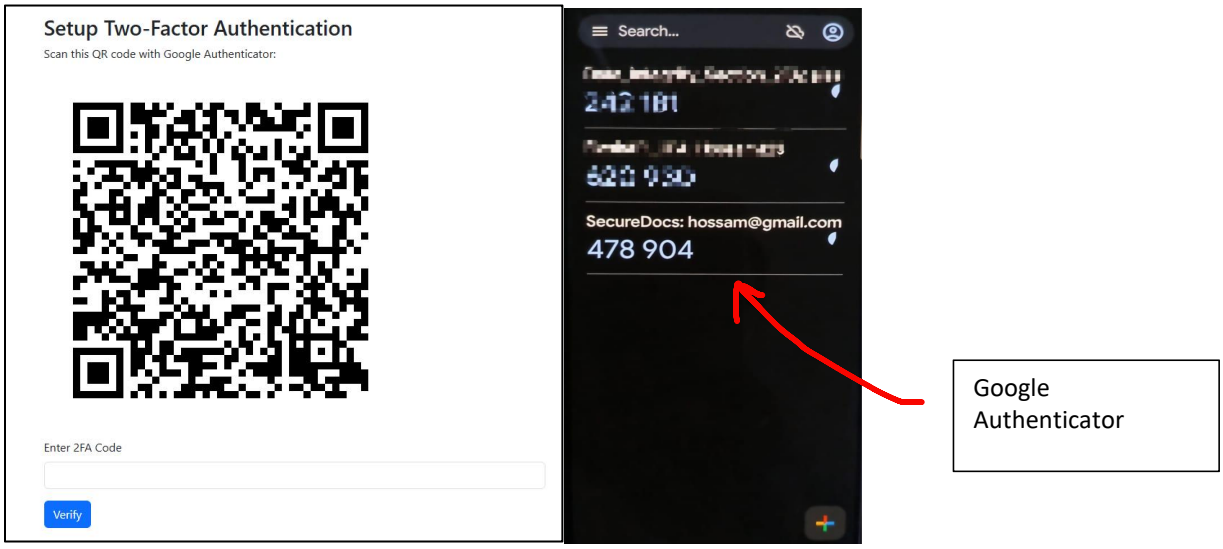
- Manual Login: Using their email and password.
- GitHub OAuth Login: Using OAuth 2.0, the user is redirected to GitHub to log in, and their credentials (email and GitHub ID) are then retrieved.
- Google OAuth

The password is verified using **bcrypt**, a powerful library for securely hashing passwords.

2FA (QR Code + Verification):

After logging in, the user must complete the two-factor authentication process:
Files: 2fa_setup.html, 2fa_verify.html

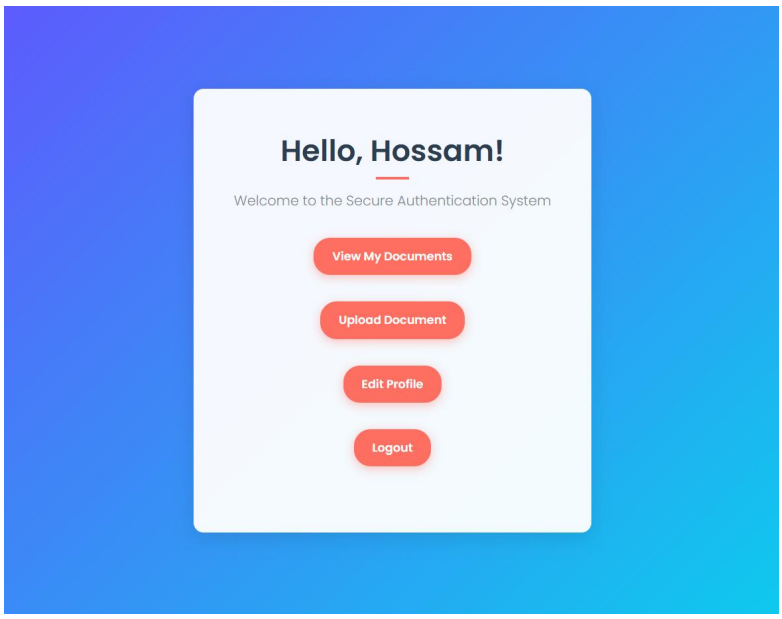
- The secret key is generated using the pyotp library.
- A QR code is displayed for scanning using an app such as Google Authenticator.
- The user must enter the TOTP to confirm the verification.
- If the code is correct, 2FA is enabled and the user is logged in.



User Session (Session Management)

- A session is created for each user using Flask session.
- Sessions are valid for 7 days (or until the user logs out).
- Successful and failed logins are logged in the LoginLog table to track activity.

User Home Page:



Features:

- **Welcome Message**

A simple greeting:
"Welcome to the Secure Authentication System"
This confirms that the user is authenticated and logged in securely.

- **View My Documents**

Redirects the user to a page listing all their uploaded documents.
Users can view file names, upload dates, and download documents.

- **Upload Document**

Navigates to the secure document upload page.
Users can upload new files (PDF, DOCX, TXT), which are encrypted and stored securely.

When user Upload file :

1. The file is encrypted using AES (by Fernet key).
2. An encrypted copy is saved within the database.
3. The file is SHA-256-based to prevent duplication and verify integrity.

When the user downlaods the file:

1. The private key is downloaded.
2. A new Fernet key is generated.
3. It is then used to decrypt the content and present it to the user.

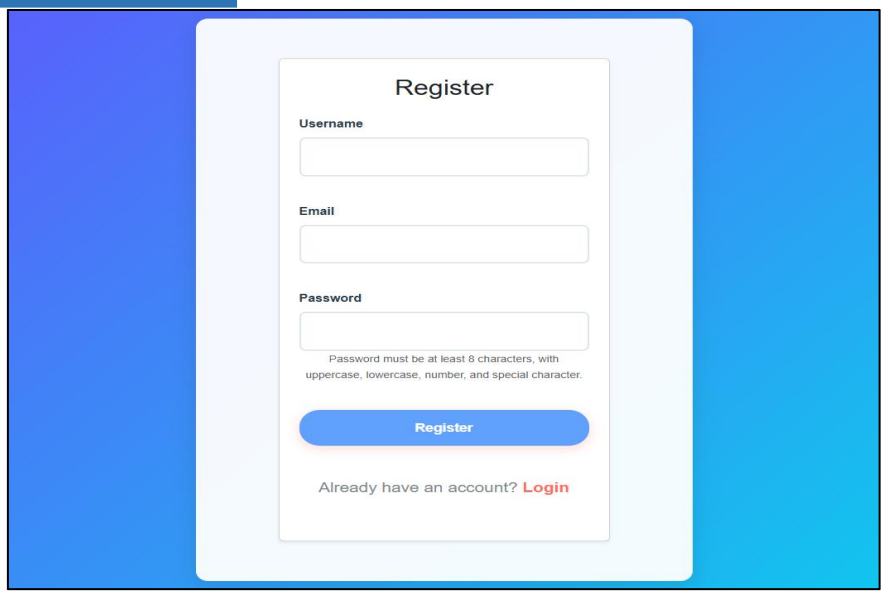
- **Edit Profile**

Allows users to update their personal information including username, email, and password.
Secure password policy enforcement is maintained here.

- **Logout**

Ends the user's session securely.
Also logs the session duration in the activity log for security auditing.

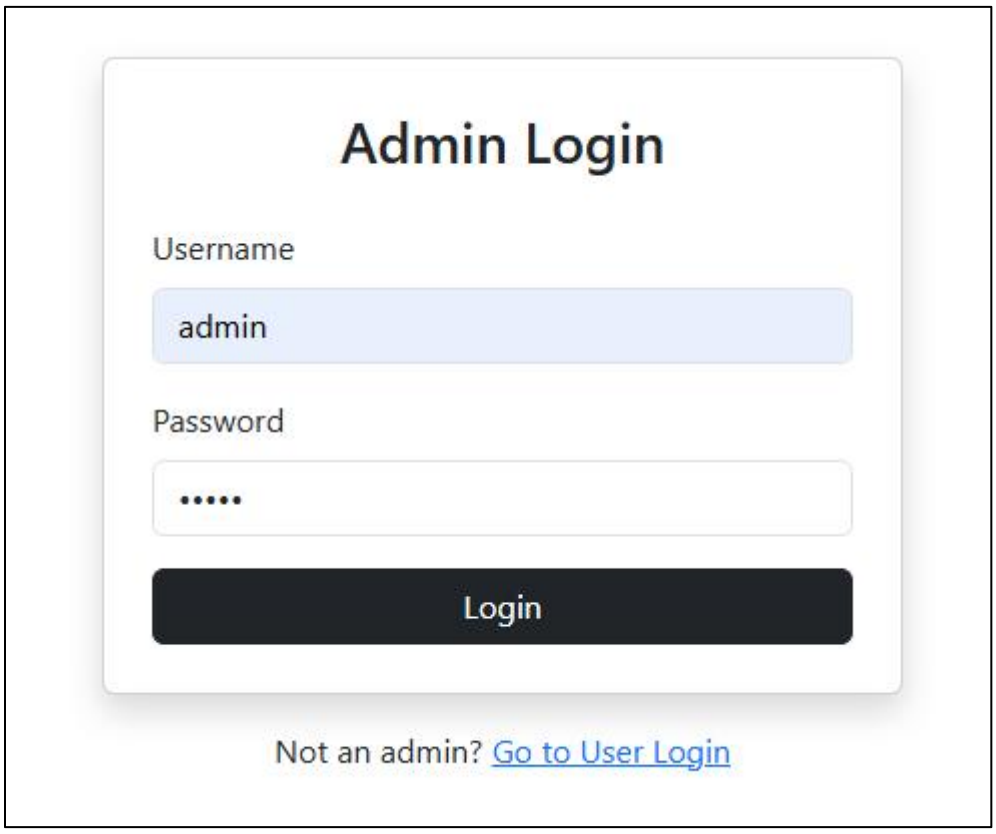
Register Page:



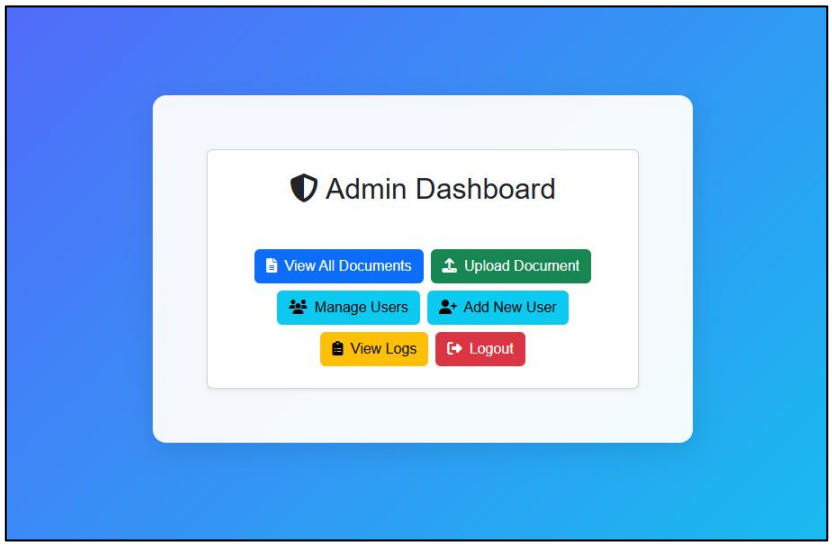
- The user can create a new account by entering their name, email address, and password.
- Check the password (length,capital/lowercase/number/symbol).
- Ensure that the email address or username does not already exist.

Admin Pages:

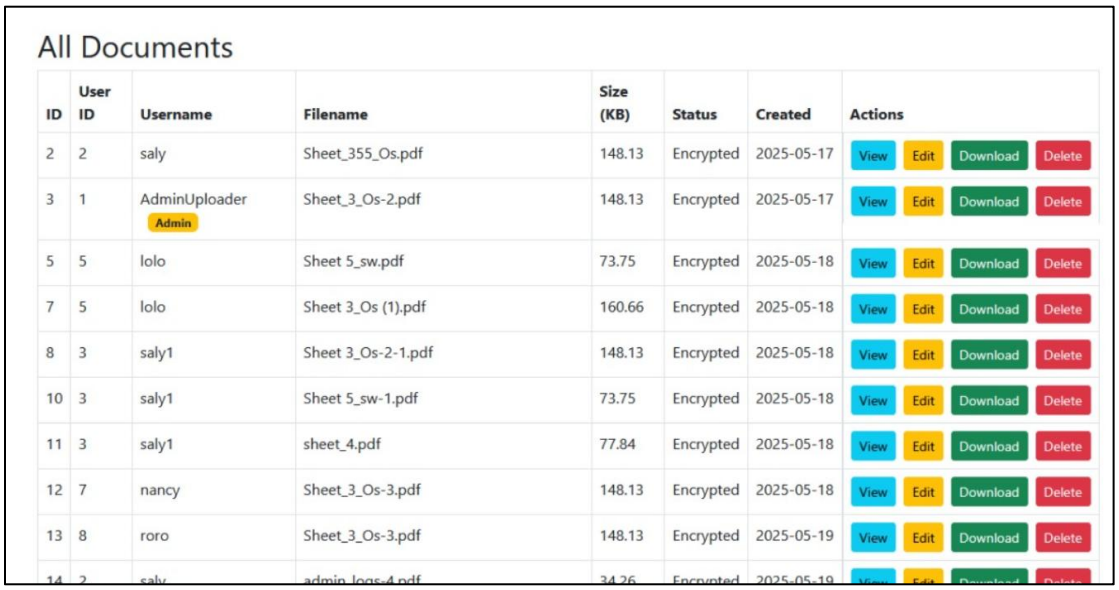
Login Page:



Home Page :



The admin dashboard represents the administrator's main interface after logging in, providing comprehensive permissions to manage users, files, and the entire system. The page contains direct links to key administrative tasks.

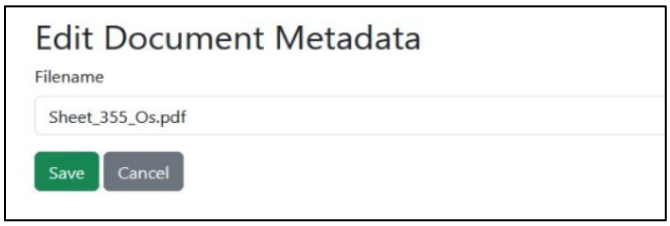


All Documents

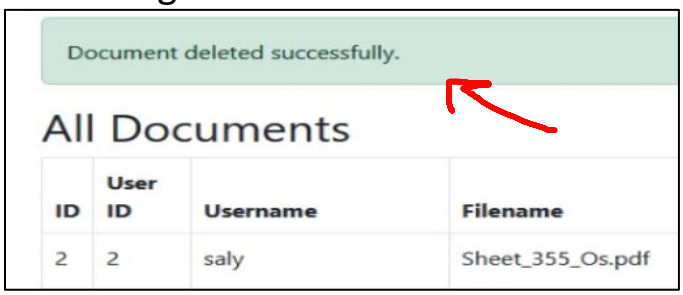
ID	User ID	Username	Filename	Size (KB)	Status	Created	Actions
2	2	saly	Sheet_355_Os.pdf	148.13	Encrypted	2025-05-17	View Edit Download Delete
3	1	AdminUploader Admin	Sheet_3_Os-2.pdf	148.13	Encrypted	2025-05-17	View Edit Download Delete
5	5	lolo	Sheet 5_sw.pdf	73.75	Encrypted	2025-05-18	View Edit Download Delete
7	5	lolo	Sheet 3_Os (1).pdf	160.66	Encrypted	2025-05-18	View Edit Download Delete
8	3	saly1	Sheet 3_Os-2-1.pdf	148.13	Encrypted	2025-05-18	View Edit Download Delete
10	3	saly1	Sheet 5_sw-1.pdf	73.75	Encrypted	2025-05-18	View Edit Download Delete
11	3	saly1	sheet_4.pdf	77.84	Encrypted	2025-05-18	View Edit Download Delete
12	7	nancy	Sheet_3_Os-3.pdf	148.13	Encrypted	2025-05-18	View Edit Download Delete
13	8	roro	Sheet_3_Os-3.pdf	148.13	Encrypted	2025-05-19	View Edit Download Delete
14	2	saly	admin_logs-4.pdf	34.26	Encrypted	2025-05-19	View Edit Download Delete

when accessing the Documents page, the administrator can:

- View the document: Decrypt the document and read its contents within the system.

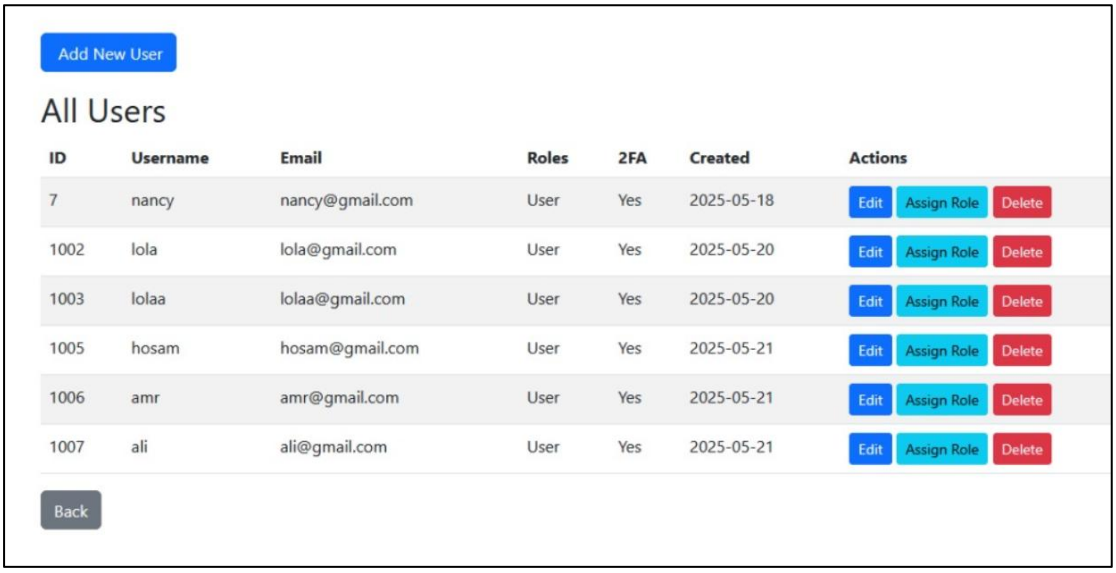


- Edit the file name: Change the document name while preserving its encrypted content.
- Download the document: Decrypt and download the file in its original format.

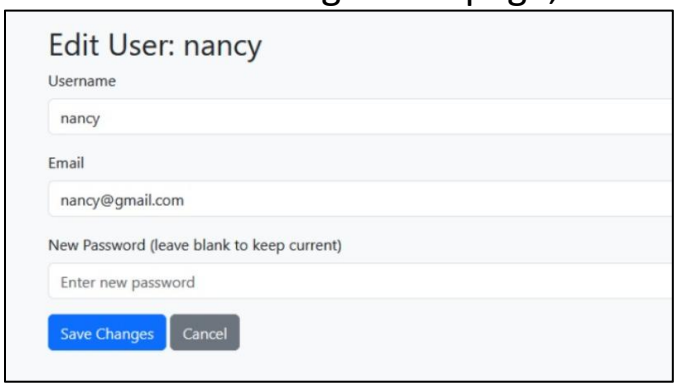


- Delete the document: Permanently delete the document from the database, along with the associated activity log.

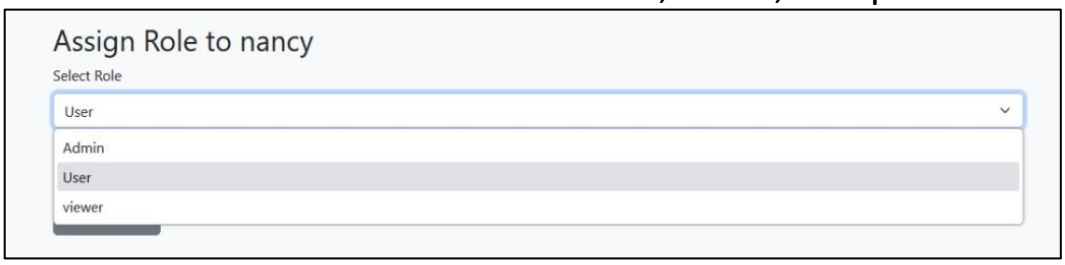
- Through this page, the administrator can upload a new document encrypted using the AES algorithm and securely stored within the database.
- Supported file types: .pdf, .docx, .txt.
- The document's user is assigned a special account named "AdminUploader."



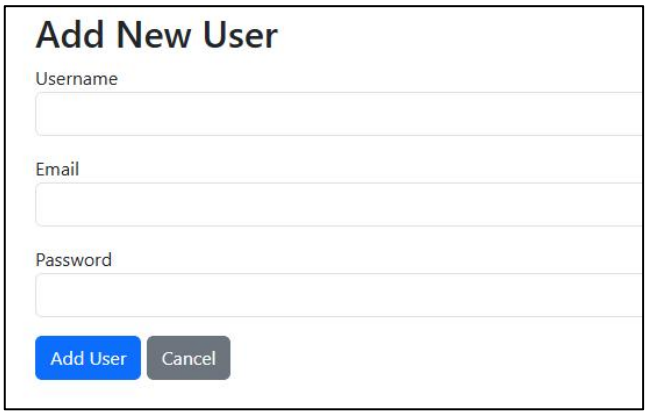
On the User Management page, the administrator can:



- Edit user information: such as name, email, and password.



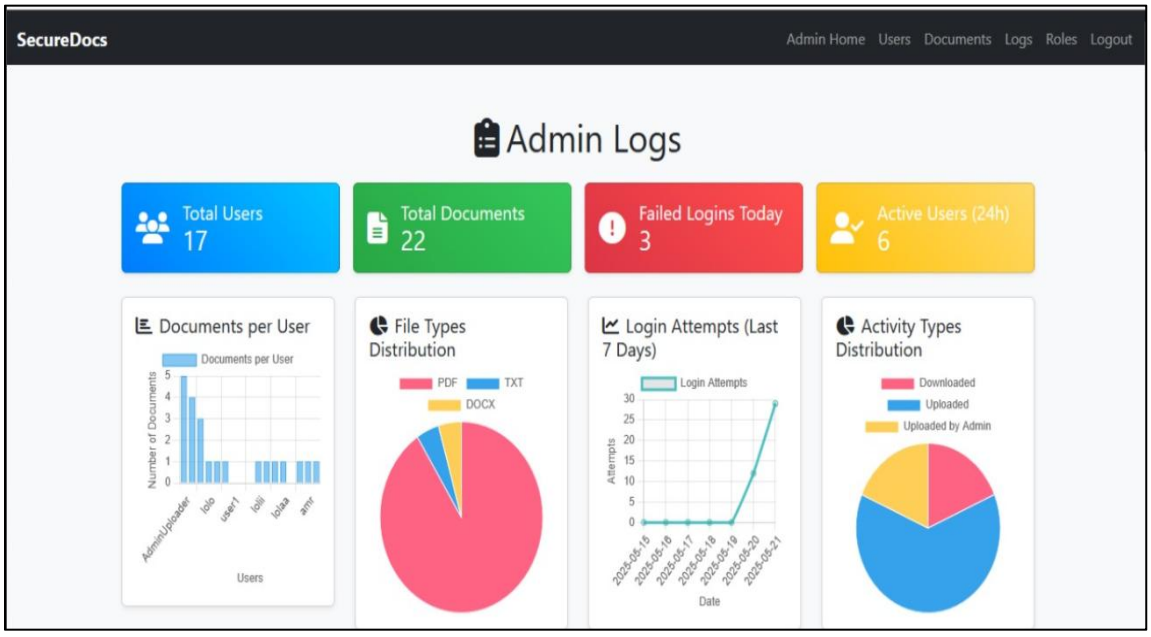
- Assign Role: Assign or change the user's role (User/Admin or any other role).
- Delete User: Permanently delete the user from the system, deleting all documents and activities associated with them.



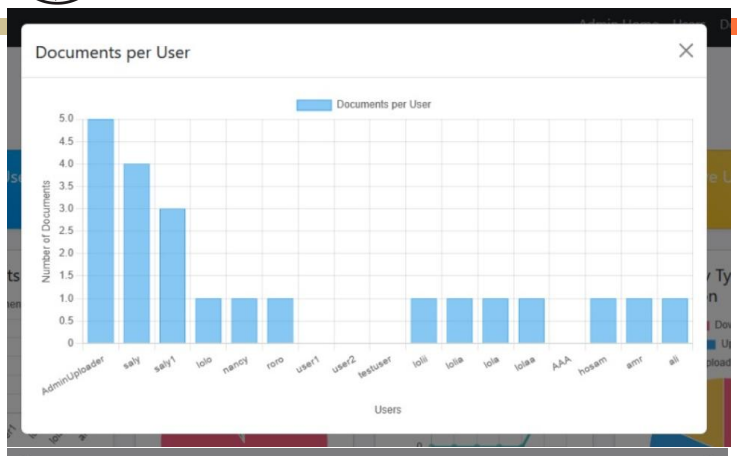
From this page, the administrator can create a new user account:

- Enter a name, email address, and a strong password.
- The primary role (User) is automatically assigned.

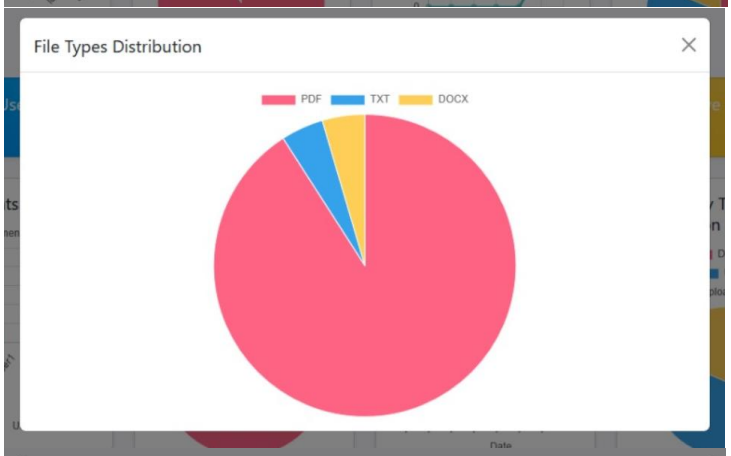
Admin Logs Page :



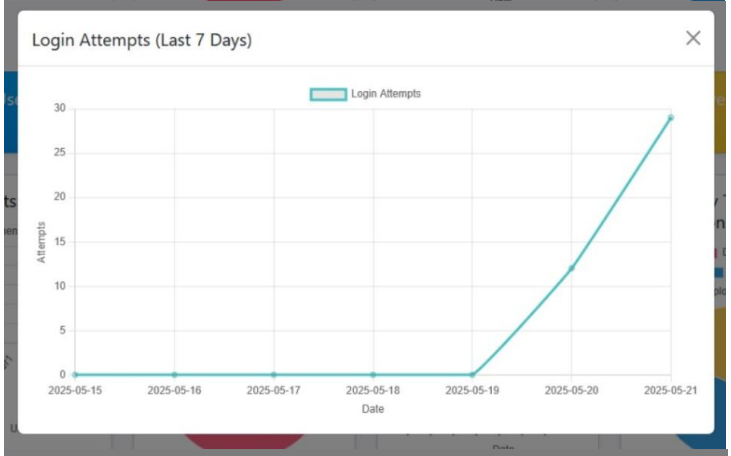
It contains an advanced panel to display and analyze activities in the system:



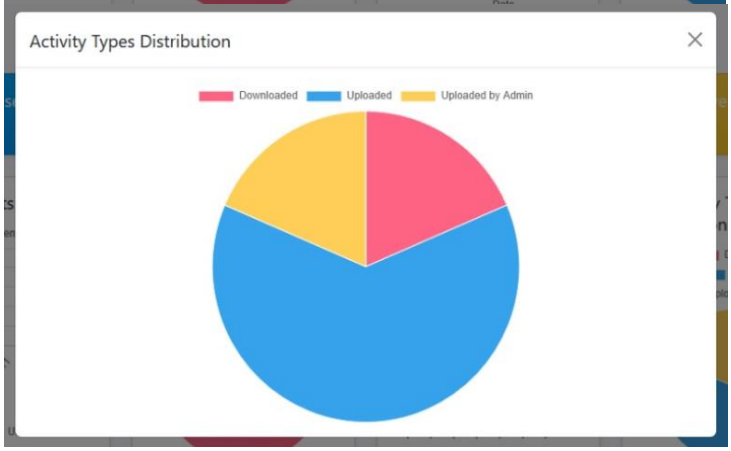
Number of documents uploaded by each user.



Distribution of uploaded file types (PDF, DOCX, TXT).



Number of login attempts in the last 7 days.



Distribution of activity types such as (Upload, Download, Delete...).

Search logs... | 05/14/2025 | 05/21/2025 | All Activity Types | All Login Statuses | Filter

Login Logs — Auto-Refresh: Off

ID	User	Admin	Email	Status	IP Address	Country	Timestamp	Duration
58	None	Admin	admin	Success	127.0.0.1	Unknown	2025-05-21 18:59:10	N/A
57	ali	N/A	ali@gmail.com	Success	127.0.0.1	Unknown	2025-05-21 18:57:22	1m 28s
56	None	Admin	admin	Success	127.0.0.1	Unknown	2025-05-21 18:24:31	31m 39s
55	amr	N/A	amr@gmail.com	Success	127.0.0.1	Unknown	2025-05-21 18:21:27	2m 52s
54	None	Admin	admin	Success	127.0.0.1	Unknown	2025-05-21 17:06:57	N/A
53	None	Admin	admin	Success	127.0.0.1	Unknown	2025-05-21 17:03:08	N/A
52	None	Admin	admin	Success	127.0.0.1	Unknown	2025-05-21 17:00:13	N/A
51	None	Admin	admin	Success	127.0.0.1	Unknown	2025-05-21 16:56:23	N/A
50	None	Admin	admin	Success	127.0.0.1	Unknown	2025-05-21 16:48:54	N/A

1 2 3 4 5 Next

Login Logs

ID	User	Admin	Email	Status	IP Address
48	None	Admin	admin	Success	127.0.0.1
47	None	Admin	admin	Success	127.0.0.1
46	None	N/A	hosam@gmail.com	Failed	127.0.0.1
45	None	N/A	hosam@gmail.com	Failed	127.0.0.1
44	None	Admin	admin	Success	127.0.0.1
43	hosam	N/A	hosam@gmail.com	Success	127.0.0.1
42	None	Admin	admin	Success	127.0.0.1
41	None	N/A	saly1@gmail.com	Failed	127.0.0.1
40	None	Admin	admin	Success	127.0.0.1

- The table contains details of all login attempts (for users and administrators).
- The status column contains:
- Success: Successful login.
- Failed: Failed login attempt.
- The IP address, geographic address, and login time are displayed.

Document Activity Logs

ID	Username	Document ID	Document Name	Action	IP Address	Timestamp
33	AdminUploader	27	admin_logs-2.pdf	Uploaded by Admin	127.0.0.1	2025-05-21 19:07:44
32	AdminUploader	26	try.txt	Uploaded by Admin	127.0.0.1	2025-05-21 19:00:51
31	ali	25	admin_logs-11.pdf	Uploaded	127.0.0.1	2025-05-21 18:58:22
30	AdminUploader	24	admin_logs-10.pdf	Uploaded by Admin	127.0.0.1	2025-05-21 18:25:17
29	amr	23	admin_logs-8.pdf	Uploaded	127.0.0.1	2025-05-21 18:22:52
28	hosam	22	admin_logs-9.pdf	Uploaded	127.0.0.1	2025-05-21 04:04:21
27	lolaa	21	Final_Project_SW.pdf	Uploaded	127.0.0.1	2025-05-20 23:29:56
26	lola	20	Sheet_1__Introduction_to_OS_Security.pdf	Uploaded	127.0.0.1	2025-05-20 21:29:09
25	lolia	19	Sheet_2_OS_security.pdf	Uploaded	127.0.0.1	2025-05-20 21:09:38

1 2 3 Next

Export as CSV

Displays all actions performed by users on documents:

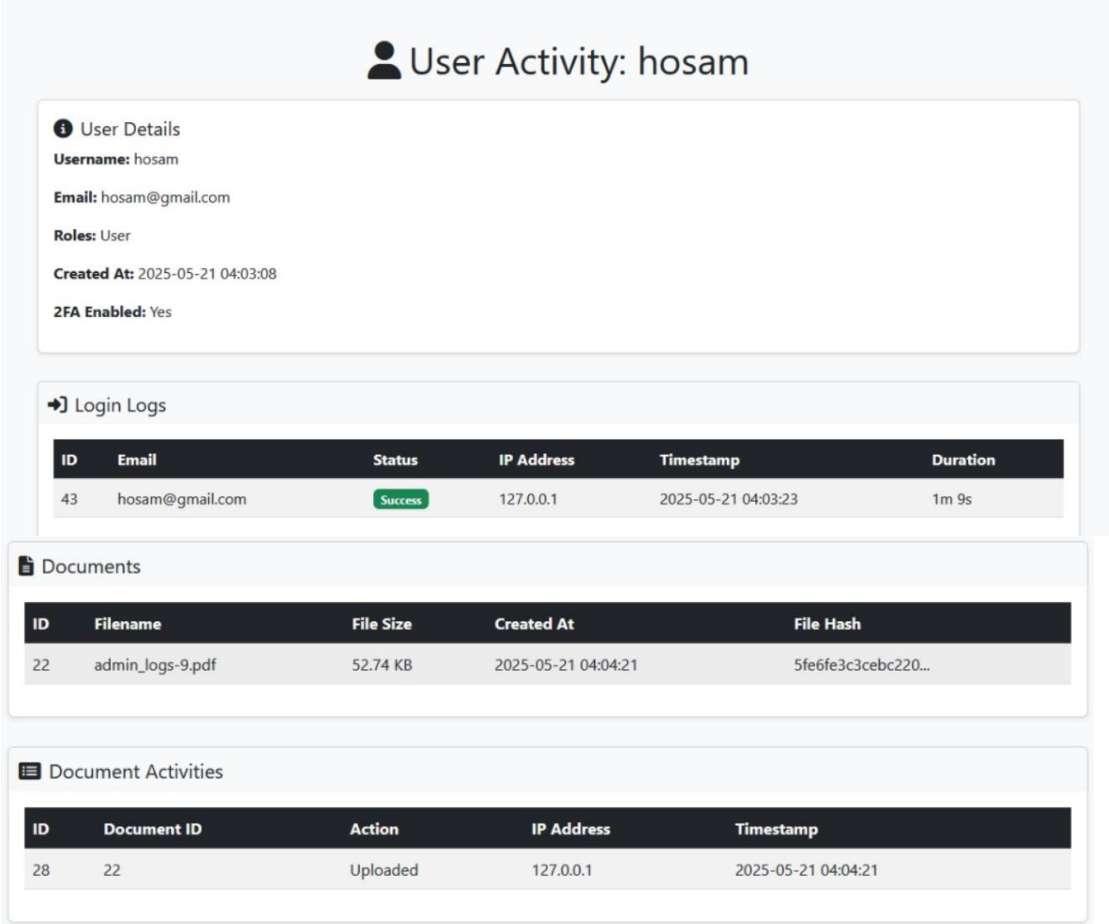
- Uploaded
- Downloaded
- Deleted
- The user name, document, time, and IP address are displayed.

Admin Activity Logs

ID	Admin Username	Action	IP Address	Timestamp
133	admin	Uploaded document 27	127.0.0.1	2025-05-21 19:07:44
132	admin	Deleted document 7	127.0.0.1	2025-05-21 19:06:20
131	admin	Uploaded document 26	127.0.0.1	2025-05-21 19:00:51
130	admin	Logged in	127.0.0.1	2025-05-21 18:59:10
129	admin	Logged out	127.0.0.1	2025-05-21 18:56:10
128	admin	Assigned role User to user 7	127.0.0.1	2025-05-21 18:32:24
127	admin	Exported user_activity logs as CSV	127.0.0.1	2025-05-21 18:30:59
126	admin	Uploaded document 24	127.0.0.1	2025-05-21 18:25:17
125	admin	Logged in	127.0.0.1	2025-05-21 18:24:31

It records everything administrators do, including:

- Deleting a user.
- Modifying a file.
- Assigning a role.
- Uploading a document.
- Authenticated by time, IP address, and administrator name.



When you select a specific user, a page containing all of their activities is displayed:

- User Details: Name ,Email ,Creation Date ,

Role (User / Admin...)

- Login Logs:

Login attempts with time and status (successful or failed).

- Documents:

All files uploaded by the user.

- Document Activities:

All actions performed by the user on files (upload, download, delete...).

Wireshark Capture Summary Demonstrating Secure Communication :

Note : The system uses HTTPS for communication.

- When user login on https://127.0.0.1:4000/login

This what happened in wireshark "**Handshake TLS**"

37	6.940114	127.0.0.1	127.0.0.1	TLSv1.3	1745 Client Hello
39	6.946471	127.0.0.1	127.0.0.1	TLSv1.3	2287 Server Hello, Change Cipher Spec, Appl
41	6.946975	127.0.0.1	127.0.0.1	TLSv1.3	124 Change Cipher Spec, Application Data
43	6.947238	127.0.0.1	127.0.0.1	TLSv1.3	299 Application Data

- This proves that a TLS session has been successfully initiated between the browser and the server.
- All data sent after a Handshake appears in Wireshark as **Application Data**.

None of the actual content inside it, such as

1. email and passwords, can be read.
2. Files are uploaded or downloaded.

- When user open on http://127.0.0.1:4000/login

http

No.	Time	Source	Destination	Protocol	Length	Info
15	11.079755	127.0.0.1	127.0.0.1	HTTP	881	GET /admin/login HTTP/1.1
19	11.083433	127.0.0.1	127.0.0.1	HTTP	1141	HTTP/1.1 200 OK (text/html)
36	24.163299	127.0.0.1	127.0.0.1	HTTP	1043	POST /admin/login HTTP/1.1 (application/x-www-form-urlencoded)
52	24.259282	127.0.0.1	127.0.0.1	HTTP	253	HTTP/1.1 302 FOUND (text/html)
56	24.262520	127.0.0.1	127.0.0.1	HTTP	979	GET /admin/home HTTP/1.1
62	24.265813	127.0.0.1	127.0.0.1	HTTP	1837	HTTP/1.1 200 OK (text/html)
71	24.293963	127.0.0.1	127.0.0.1	HTTP	824	GET /static/styles.css HTTP/1.1
73	24.297624	127.0.0.1	127.0.0.1	HTTP	324	HTTP/1.1 304 NOT MODIFIED
86	34.094529	127.0.0.1	127.0.0.1	HTTP	887	GET /admin/upload HTTP/1.1
90	34.096975	127.0.0.1	127.0.0.1	HTTP	722	HTTP/1.1 200 OK (text/html)
352	74.944835	127.0.0.1	127.0.0.1	HTTP	444	POST /admin/upload HTTP/1.1 (application/pdf)
388	74.976791	127.0.0.1	127.0.0.1	HTTP	257	HTTP/1.1 302 FOUND (text/html)
394	74.981635	127.0.0.1	127.0.0.1	HTTP	1022	GET /admin/upload HTTP/1.1
398	74.983674	127.0.0.1	127.0.0.1	HTTP	984	HTTP/1.1 200 OK (text/html)
411	78.496063	127.0.0.1	127.0.0.1	HTTP	887	GET /admin/home HTTP/1.1
415	78.498558	127.0.0.1	127.0.0.1	HTTP	1511	HTTP/1.1 200 OK (text/html)
421	78.523793	127.0.0.1	127.0.0.1	HTTP	824	GET /static/styles.css HTTP/1.1
423	78.526498	127.0.0.1	127.0.0.1	HTTP	324	HTTP/1.1 304 NOT MODIFIED
435	81.733822	127.0.0.1	127.0.0.1	HTTP	890	GET /admin/documents HTTP/1.1
453	81.742898	127.0.0.1	127.0.0.1	HTTP	2538	HTTP/1.1 200 OK (text/html)

If the same application is run without an SSL certificate , the sensitive data in Wireshark will appear as:

```
    [HTTP request 1/1]
    [Response in frame: 52]
    File Data: 29 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "username" = "admin"
  ▸ Form item: "password" = "admin"
```

Text item (text), 14 bytes