CIA Layers:

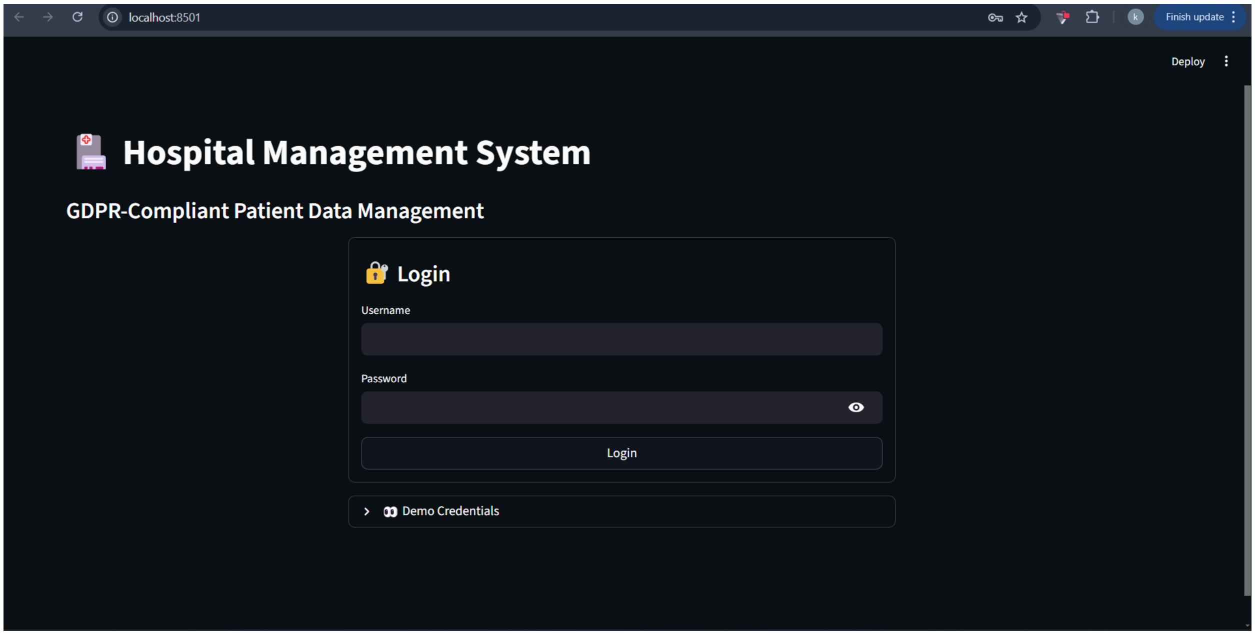
```
 -----------------------------------------------------
|                  CONFIDENTIALITY                    |
| - Masking/anonymization                             |
| - Encryption                                        |
| - RBAC (Admin/Doctor/Receptionist)                  |
| - Login authentication                              |
 -----------------------------------------------------
|                     INTEGRITY                       |
| - Activity logs (who did what)                      |
| - Validation + DB constraints                       |
| - Audit trail (admin only)                          |
 -----------------------------------------------------
|                    AVAILABILITY                     |
| - Stable DB access                                  |
| - Error handling                                    |
| - Backup/export                                     |
| - System uptime indicator                           |
 -----------------------------------------------------
```

The Hospital Management System is structured into three CIA layers.
Confidentiality protects patient identity through anonymization, encryption, and RBAC.
Integrity ensures accuracy by logging all user actions and enforcing access controls.
Availability maintains reliable system access using backups, exception handling, and continuous uptime.

Project report - K225096 - K225046

Screenshots:-

Login:



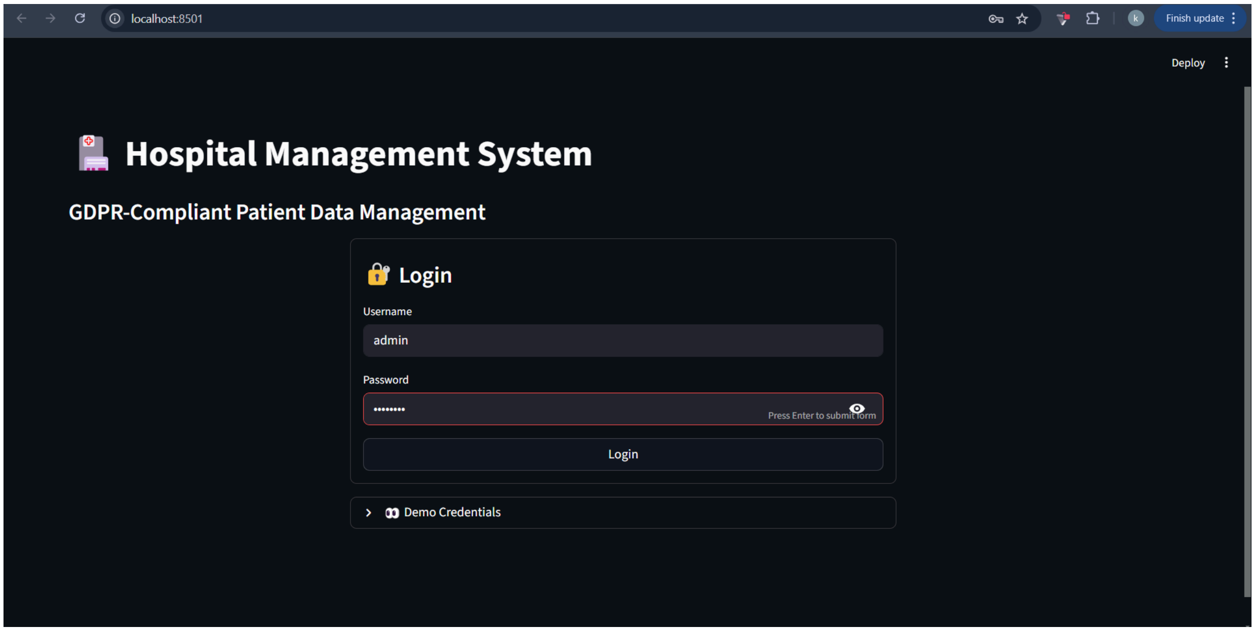
Hospital Management System

GDPR-Compliant Patient Data Management

Login

Username

Password



Hospital Management System

GDPR-Compliant Patient Data Management

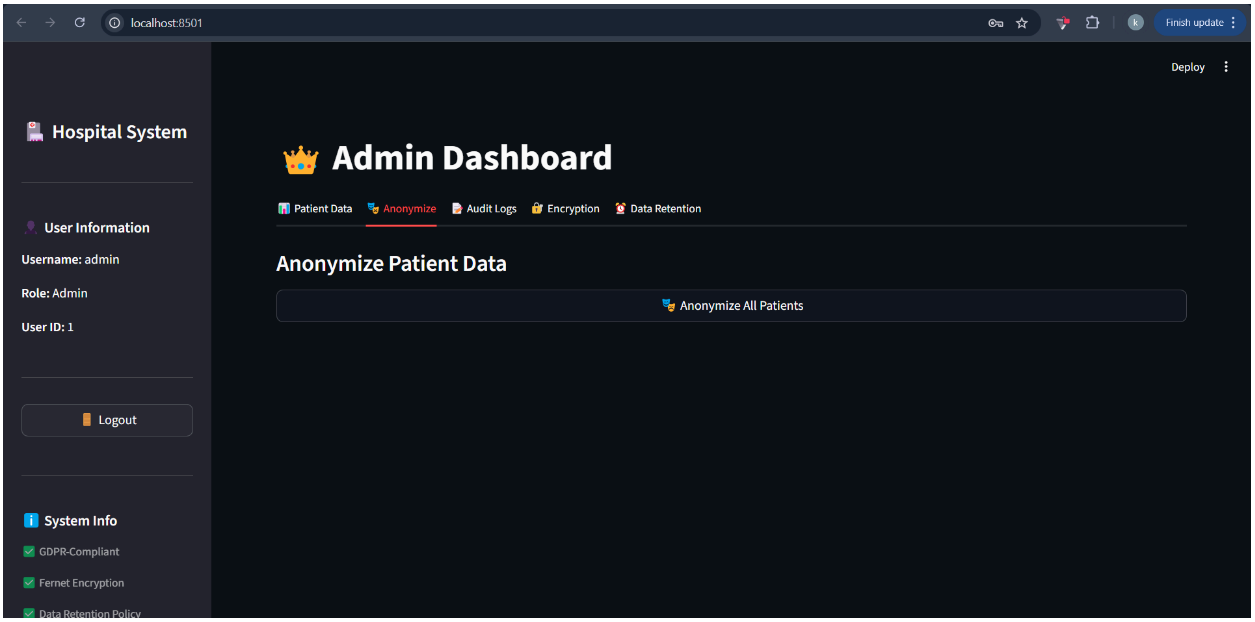
Login

Username: admin

Password: ••••••••

Press Enter to submit form

Anonymization:



Hospital System

User Information

Username: admin

Role: Admin

User ID: 1

System Info

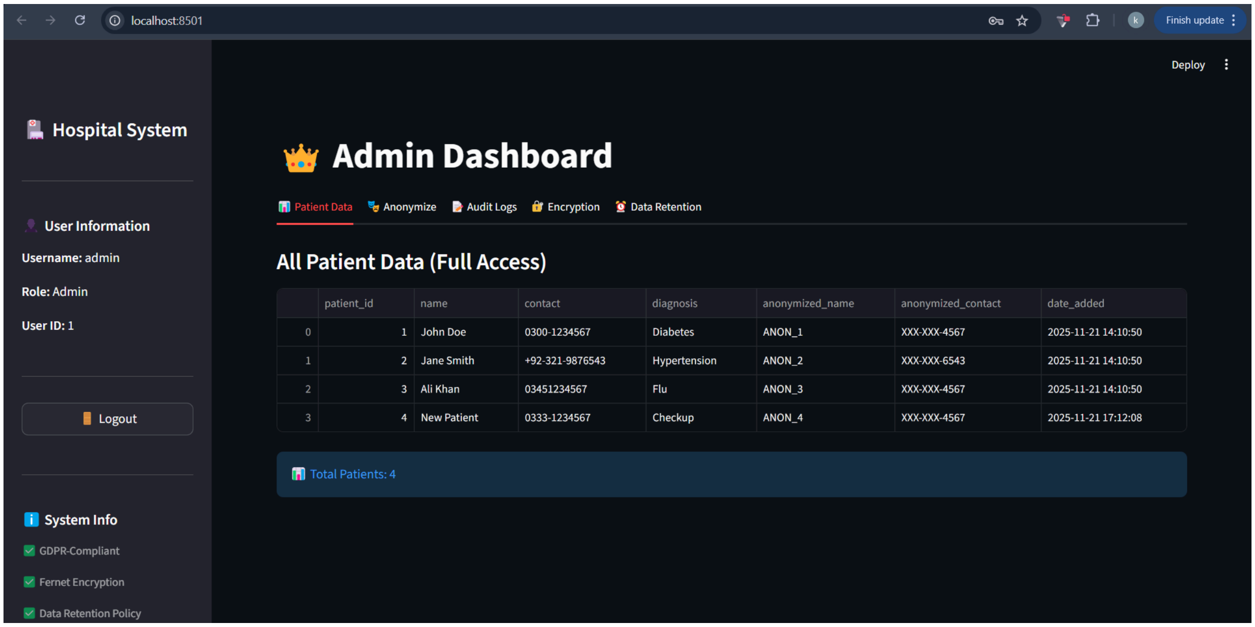
✓ GDPR-Compliant

✓ Fernet Encryption

✓ Data Retention Policy

Admin Dashboard

Anonymize Patient Data



Hospital System

User Information

Username: admin

Role: Admin

User ID: 1

System Info

✓ GDPR-Compliant

✓ Fernet Encryption

✓ Data Retention Policy

Admin Dashboard

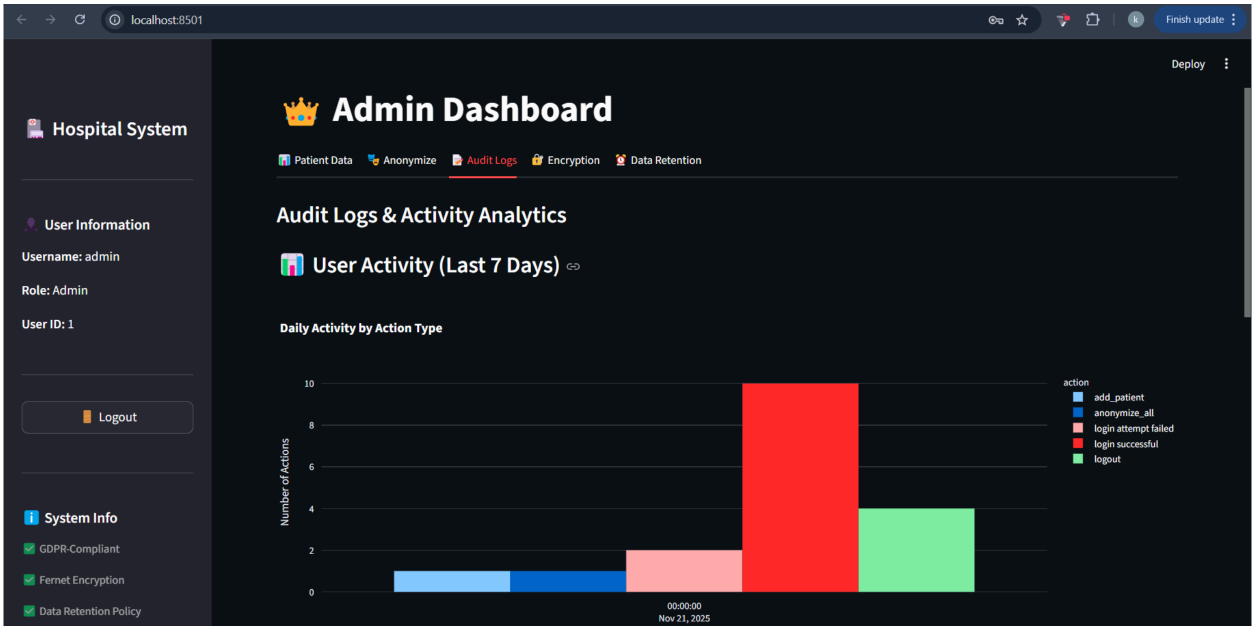
All Patient Data (Full Access)

	patient_id	name	contact	diagnosis	anonymized_name	anonymized_contact	date_added
0	1	John Doe	0300-1234567	Diabetes	ANON_1	XXX-XXX-4567	2025-11-21 14:10:50
1	2	Jane Smith	+92-321-9876543	Hypertension	ANON_2	XXX-XXX-6543	2025-11-21 14:10:50
2	3	Ali Khan	03451234567	Flu	ANON_3	XXX-XXX-4567	2025-11-21 14:10:50
3	4	New Patient	0333-1234567	Checkup	ANON_4	XXX-XXX-4567	2025-11-21 17:12:08

Total Patients: 4

Log Screens:

Project report - K225096 - K225046



Admin Dashboard

User Information

Username: admin

Role: Admin

User ID: 1

System Info

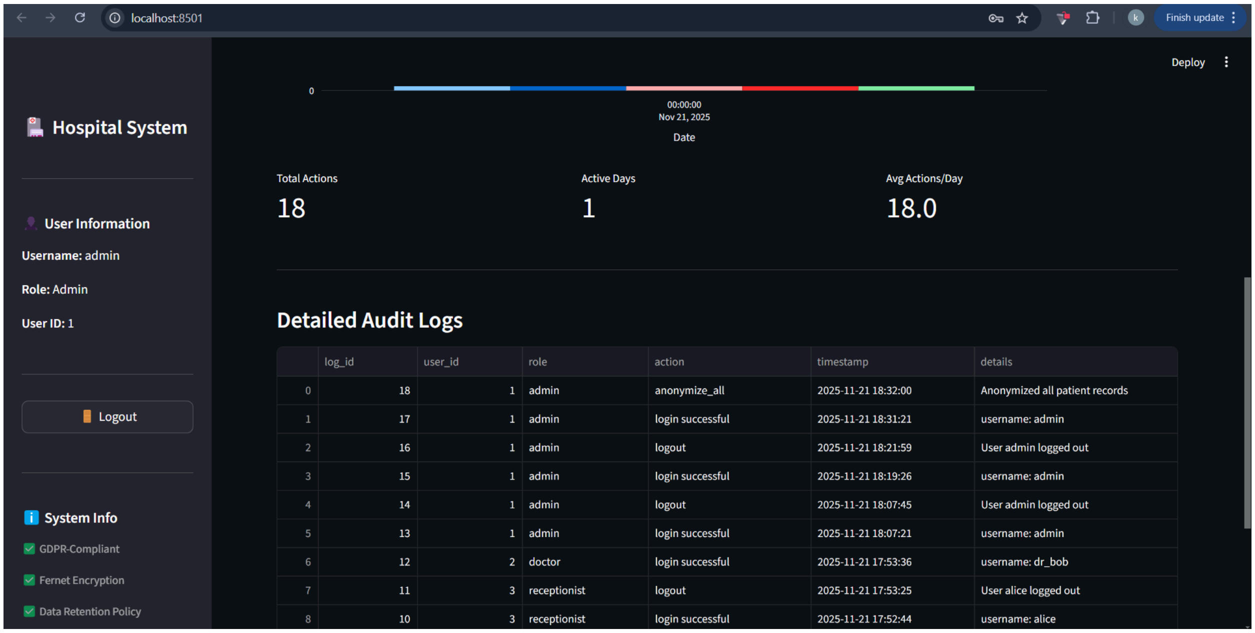
☑ GDPR-Compliant

☑ Fernet Encryption

☑ Data Retention Policy

Audit Logs & Activity Analytics

User Activity (Last 7 Days)



User Information

Username: admin

Role: Admin

User ID: 1

System Info

☑ GDPR-Compliant

☑ Fernet Encryption

☑ Data Retention Policy

Total Actions 18

Active Days 1

Avg Actions/Day 18.0

Detailed Audit Logs

	log_id	user_id	role	action	timestamp	details
0	18	1	admin	anonymize_all	2025-11-21 18:32:00	Anonymized all patient records
1	17	1	admin	login successful	2025-11-21 18:31:21	username: admin
2	16	1	admin	logout	2025-11-21 18:21:59	User admin logged out
3	15	1	admin	login successful	2025-11-21 18:19:26	username: admin
4	14	1	admin	logout	2025-11-21 18:07:45	User admin logged out
5	13	1	admin	login successful	2025-11-21 18:07:21	username: admin
6	12	2	doctor	login successful	2025-11-21 17:53:36	username: dr_bob
7	11	3	receptionist	logout	2025-11-21 17:53:25	User alice logged out
8	10	3	receptionist	login successful	2025-11-21 17:52:44	username: alice

🏥 Discussion on CIA Implementation & GDPR Alignment (For Hospital Management System)

🔵 Confidentiality (C)

In the HMS, confidentiality is ensured by restricting access to sensitive patient information. Only the Admin can see full patient details, while Doctors receive partially anonymized medical data, and Receptionists only see non-sensitive fields (e.g., appointment schedule). Sensitive attributes (name, CNIC, disease type) are masked or encrypted during processing. User authentication is mandatory before accessing any module.

🔍 GDPR Alignment – Confidentiality

GDPR requires *data minimization* and *purpose limitation*.
Our system aligns with this by:

- Showing only necessary data to each role (least privilege).
- Masking identifiable fields unless strictly required for treatment.
- Ensuring that protected health information (PHI) is never exposed to unauthorized roles.

🟢 Integrity (I)

Integrity is maintained through strict control over who can add, edit, or delete hospital records. Every modification is logged with timestamp, role, and activity type to maintain accountability. Database constraints prevent invalid or incomplete data entry. Doctors cannot modify administrative fields, and receptionists cannot change medical reports.

🔍 GDPR Alignment – Integrity

GDPR mandates *accuracy* and *traceability*.
The HMS meets this by:

- Keeping an audit trail of all modifications (who changed what).
- Ensuring only authorized staff can alter medical information.
- Preventing data tampering through validation rules and edit restrictions.

🟡 Availability (A)

The system ensures availability by maintaining stable database access and using error-handling to avoid unexpected crashes. Backup/export features (CSV snapshots) help restore data if the system fails. The system dashboard remains accessible for staff during working hours, and uptime information is displayed to the admin.

🔍 GDPR Alignment – Availability

GDPR requires *availability and resilience of processing systems (Art. 32)*.
The HMS supports this by:

- Maintaining frequent database backups.
- Implementing safeguards to ensure continuous access for authorized staff.
- Allowing rapid restoration of data during system errors.

Conclusion:

The Hospital Management System incorporates CIA principles by protecting patient privacy (Confidentiality), ensuring accurate and trustworthy records (Integrity), and maintaining reliable access to healthcare information (Availability). Its design aligns with GDPR through data minimization, access restrictions, audit logging, accuracy enforcement, and strong backup mechanisms. Together, these measures ensure that sensitive health data remains secure, compliant, and accessible.

Short Demo Video Link:

https://drive.google.com/file/d/1mVg2e0CUbCGD36v8dHyXtN8yBK0EEZT3/view?usp=sharing