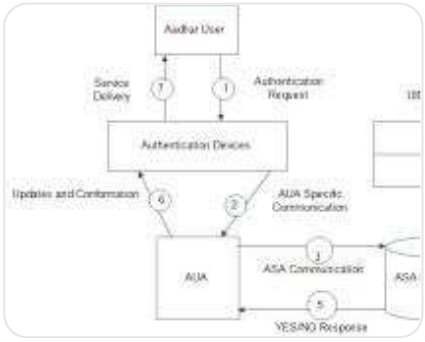
Mini-case Study: Privacy Risk Map
Pick a real technology (e.g., ChatGPT, Google Photos, Aadhar).
Students create a privacy risk diagram showing:
 What data is collected
 Where it is stored
 Who can access it
(Focus: investigation, small experiments, structured thinking)

Here is a **simple and clear mini–case study** with a **Privacy Risk Map** for **Aadhaar (UIDAI System)** — you can directly use it in assignments or presentations.

Mini-Case Study: Privacy Risk Map – Aadhaar System



Aadhaar is India's nationwide digital identity system managed by UIDAI. It collects sensitive personal and biometric data to authenticate individuals for government schemes, banking, telecom services, and more.

---

1. What Data is Collected

A. Personal Information

- Full Name
- Date of Birth / Age
- Gender
- Address

- Mobile Number
- Email ID

B. Biometric Information (Highly Sensitive)

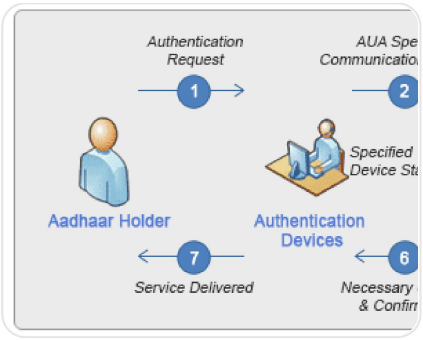
- Fingerprints (all 10 fingers)
- Iris scans (both eyes)
- Facial image

C. Usage Data

- Authentication logs (when, where, which service accessed Aadhaar)
- Device and operator used for authentication

---

2. Where the Data is Stored



A. Central Identity Data Repository (CIDR)

- Core Aadhaar database
- Stores **biometrics + demographic data**
- Highly secured servers managed by UIDAI

B. Local Registrar / Enrollment Agency Systems

- Temporary storage during enrollment
- Data is encrypted and transferred to CIDR
- Must be deleted after upload (risk if mishandled)

C. Service Providers' Databases (Indirect Storage)

Many banks, telecom companies, and apps store:

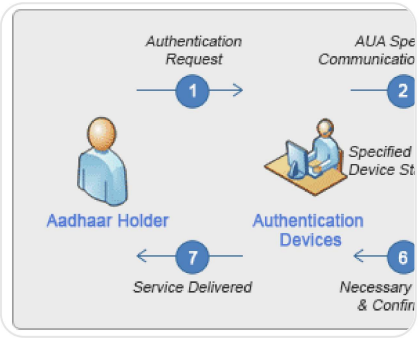
- Aadhaar Number (sometimes masked)
- Last 4 digits

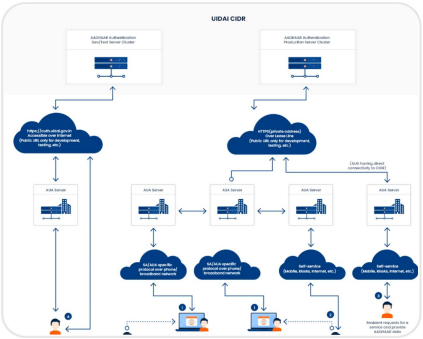
- Authentication tokens
- KYC documents linked with Aadhaar

Privacy risk: Multiple third parties storing Aadhaar-linked data increases chances of leaks.

---

3. Who Can Access the Data





A. UIDAI Officials / Systems

- Full access to CIDR
- Automated matching systems access biometrics for authentication

B. Authorized Service Providers

These entities can access Aadhaar for verification:

- Banks
- Telecom companies
- Government departments (subsidies, tax filing, pensions)
- PAN services
- Welfare schemes

They **cannot** access biometric data; only **authentication response** ("yes/no" or eKYC data).

C. Enrollment Agencies

- Temporary access during enrollment
- Risk if security guidelines are not followed

D. Potential Unauthorised Actors (Risks)

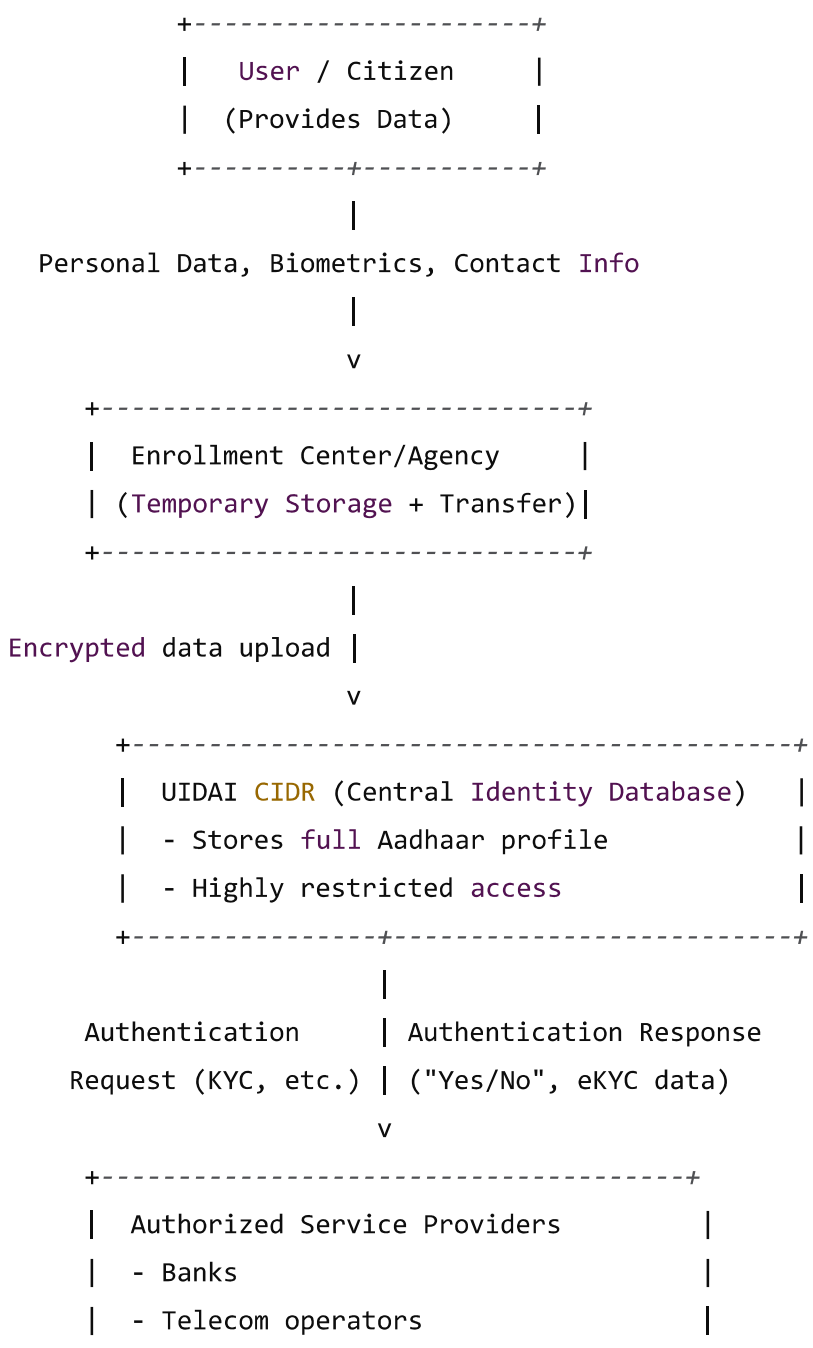
- Data brokers

- Hackers targeting weak links (local storage, third-party apps)
- Insider threats
- Misuse by service providers (excessive data collection)

Privacy Risk Map (Simplified Diagram)

Here is a text-based privacy risk map you can draw in your notebook or convert into a visual diagram:

pgsql Copy code



```
|  - Govt. welfare systems              |
+---------------------------------------+
                    |
 Possible risk: Oversharing, leaks
```

Key Privacy Risks Identified

1. Centralized Biometrics

- Single target for attacks (CIDR).
- Irreversible if leaked (you cannot change fingerprints).

2. Third-Party KYC Storage

- Banks/telecoms may store Aadhaar numbers improperly.
- Multiple copies increase attack surface.

3. Authentication Tracking

- Logs may reveal user behavior (when/where Aadhaar was used).

4. Insider Misuse

- Enrollment staff or agency misuse before deletion.

5. Linking of Databases

- Aadhaar number can become a universal identifier → profiling risk.

Conclusion

Aadhaar enables fast and large-scale identity verification but also introduces significant privacy risks due to:

- Centralized sensitive data
- Widespread usage
- Third-party storage
- Potential misuse of authentication logs

A structured privacy risk map helps understand how personal information flows and where interventions (encryption, access controls, audits) are needed.

If you want, I can also create:

✅ A **PowerPoint slide**

✅ A **clean infographic-style diagram**

✅ A **case study on ChatGPT or Google Photos instead**

Just tell me!