What is DSMS (Decentralized Secure Management System)?

DSMS is a **secure online platform** where people can **store, manage, and share important documents** (like marksheets, ID proofs, resumes, etc.) **without giving control to companies like Google or Dropbox**.

What Problem Are We Solving?

Right now, when you upload your documents to websites (like during admission, job applications, or KYC), here's what happens:

- You don't know **where the file is stored**

- You lose **control** once uploaded — they can keep, copy, or misuse it

- You **can't take it back**

- No proof of who accessed it or when

What Is Our Solution?

With DSMS, instead of uploading your files **to others' websites**, you:

1. Upload your documents **to your own secure space** on our platform.

2. **You own the file** — no one else can change or delete it.

3. You can **share it securely** with someone (like a college or company) through a link.

4. You can **set limits** — who can see it, for how long, how many times.

5. You can **revoke access anytime**.

6. You get **alerts and history** of who accessed your file.

So basically, **you stay in control of your data**. No more blind trust.

How Do We Handle Sharing with Other Websites?

Let's say a college wants your marksheet.
Instead of uploading it on their form, they:

- Send you a **document request** through DSMS.

- You get a **notification**.

- You choose **which document to send**, how long they can see it, and if they can download it.

- That college only gets **temporary, read-only access** — no copy, no theft.

We call this the **Trusted Document Bridge** — like a secure tunnel between you and the other website.

Why Is It More Secure?

Because:

- Your file is **stored in pieces** across a global system (called IPFS), not on one company's server.

- Your file is **locked and encrypted** — no one can read it without your permission.

- When someone accesses your file, we **log that event**, and you can check the full history.

- You can even **auto-expire links** or **block users later**.

What Technologies Are Involved (in simple words)?

Here's what's happening **in the background**, without going too technical:

Component	What it does (simple)
IPFS	Like Google Drive, but decentralized. Stores your file in pieces across the globe. No single owner.
Smart Contract (optional)	Acts like a robot judge: keeps records (like who saw your file) and can't be bribed or edited.
Blockchain (optional)	Like a public diary that logs events (like file access) which no one can fake or delete.
Firebase / MongoDB	Stores basic info like your profile, list of files, etc. (safe and fast)
Frontend	What users see — the website you interact with
Backend	The logic and engine that connects everything together behind the scenes

Don't worry if you don't understand blockchain or IPFS fully. Our goal is to build the system so that users don't need to understand it either.

Who Will Use It?

- Students sharing documents with colleges

- Job seekers sending resumes securely

- HR departments collecting candidate data without storing it

- Developers/freelancers sending files with tracking

- Government offices collecting ID proofs without owning them

---

What Will We Build First (Basic Version)?

- Login system (email or wallet)

- File upload system

- Dashboard to manage your documents

- Share file links with options (like expiry time)

- View file access history

- Trusted document request system for other websites

Then Later (Advanced Version)

- Add watermarking to shared files

- On-chain file logs (smart contracts)

- Encrypted storage and sharing

- Document approval system

- Mobile app

- Biometric login (face/fingerprint)

- AI for automatic tagging of documents

Example You Can Use to Explain to Anyone

Imagine a student applying for admission.
Instead of uploading all her documents to 5 different college websites (where she loses control), she uploads it once to DSMS.
Then she shares a special link with each college that **only allows view access for 7 days**.
She gets alerts if the college views it and can revoke access anytime.
Her documents are **safe, trackable, and under her control** — not floating around the internet.

Final Line to Your Team:

We're not just building another drive — we're building the **future of how people share important documents safely, transparently, and with full control**.
Even big tech hasn't done this right yet — and that's our opportunity.