

NoteVault

The Private Note Taking App

Team 2



The Need

Privacy sensitive
processes involved



Minimal anonymity

By design, all the note taking apps tend to collect identifying information about the users.



User profiling

Once identities are established for note login, big tech is able to create profiles of users and correlate the info. across different products.



Mining user's content

Data is often used to offer enhanced experiences which is very broadly defined.

✕ Overburdened User

Often for the simple act of note taking, the user has to jump through multiple hoops before they can get to actually taking notes. (linking profiles, cloud storage plans and tiers, familiarising with trademarked features)

✕ Security

Most of the note taking apps do not offer encryption for across their entire suite of services.




✕ Privacy by default

Most of the note taking apps are invasive by nature and try to gain as much user info. as possible unless the user takes special steps to not allow this.

✕ Transparency and Clarity

Not opensource
Vague user data handling practices: hit a dead end



System/ Application	NoteVault	 Evernote	 Google Keep	 OneNote
Anonymous Usability	✓	X	X	X
Notes are encrypted	✓	Only selected content is encrypted.	Attachments are encrypted but content can be accessed.	All notes are not end to end encrypted by default.
No mining of user's content for any purpose	✓	Content retained unless deleted.	Keep uses data to improve your experience	Data used to improve experience.
Open source	✓	X	X	X
Web3 compatible	✓	X	X	X
Price you pay	None	7.99 USD	Your Data	6.99 USD



Our Privacy Features



No PII collected



No collection or linkage
of user data with
identities of users.



Your data is
protected



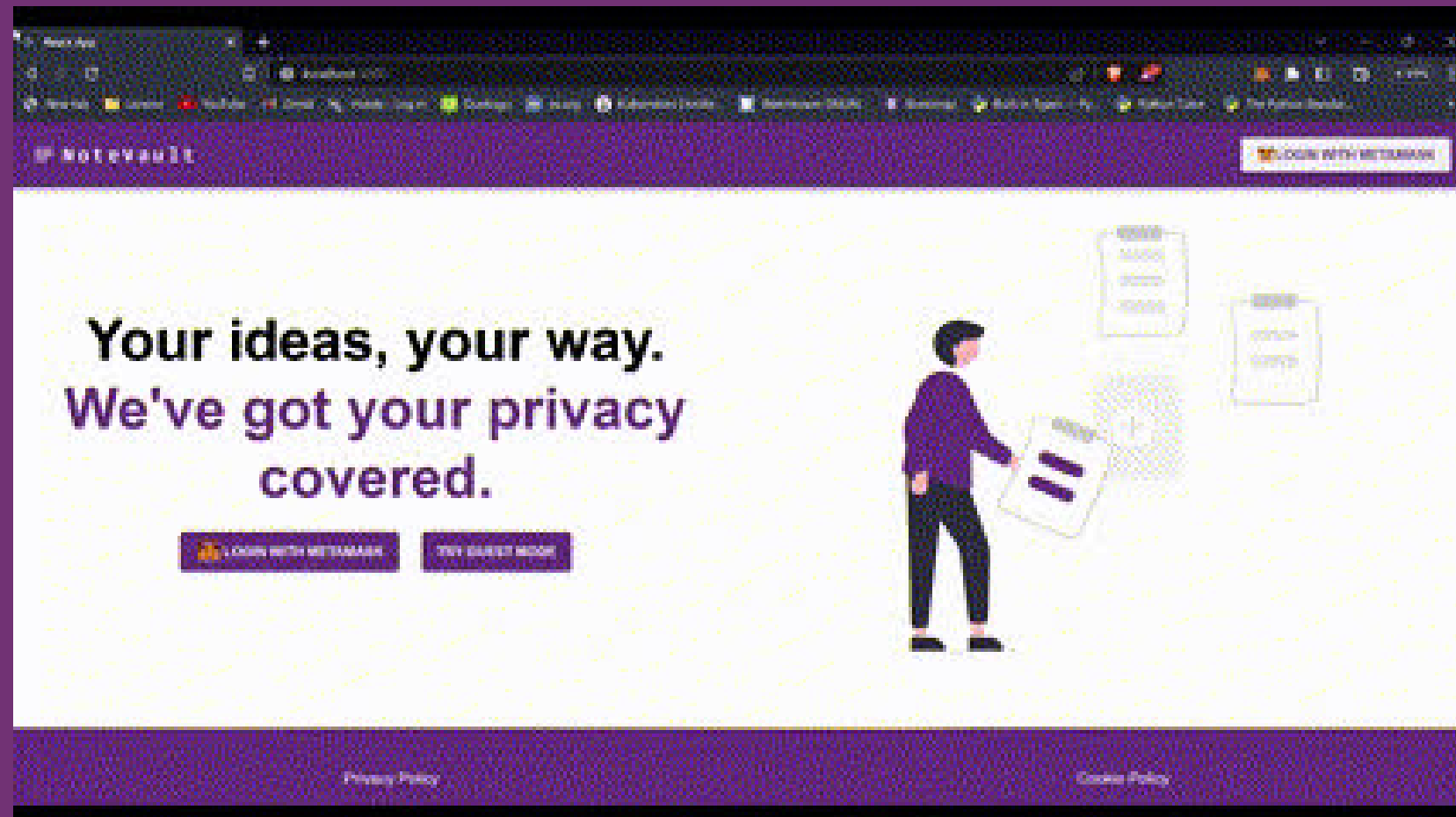
Flexibility to the
user to handle their
data

1

Log in with a single click.

Practically unhackable.

No PII collected.



Sounds too good?

Thank the fox!

Passwordless secure login with MetaMask

- Most trusted and easy to use blockchain wallet
- Secure anonymous digital signatures & log in
- Doesn't collect private data like IP address
- Why Metamask?
- Don't trust, verify



2

But what if you don't
want an account?

Be my guest !
With Guest Mode



Notes stored
locally

3

Your data. Your choice.

Switch effortlessly at the flick of a switch!



IndexedDB (Local)



MongoDB (Cloud)

4

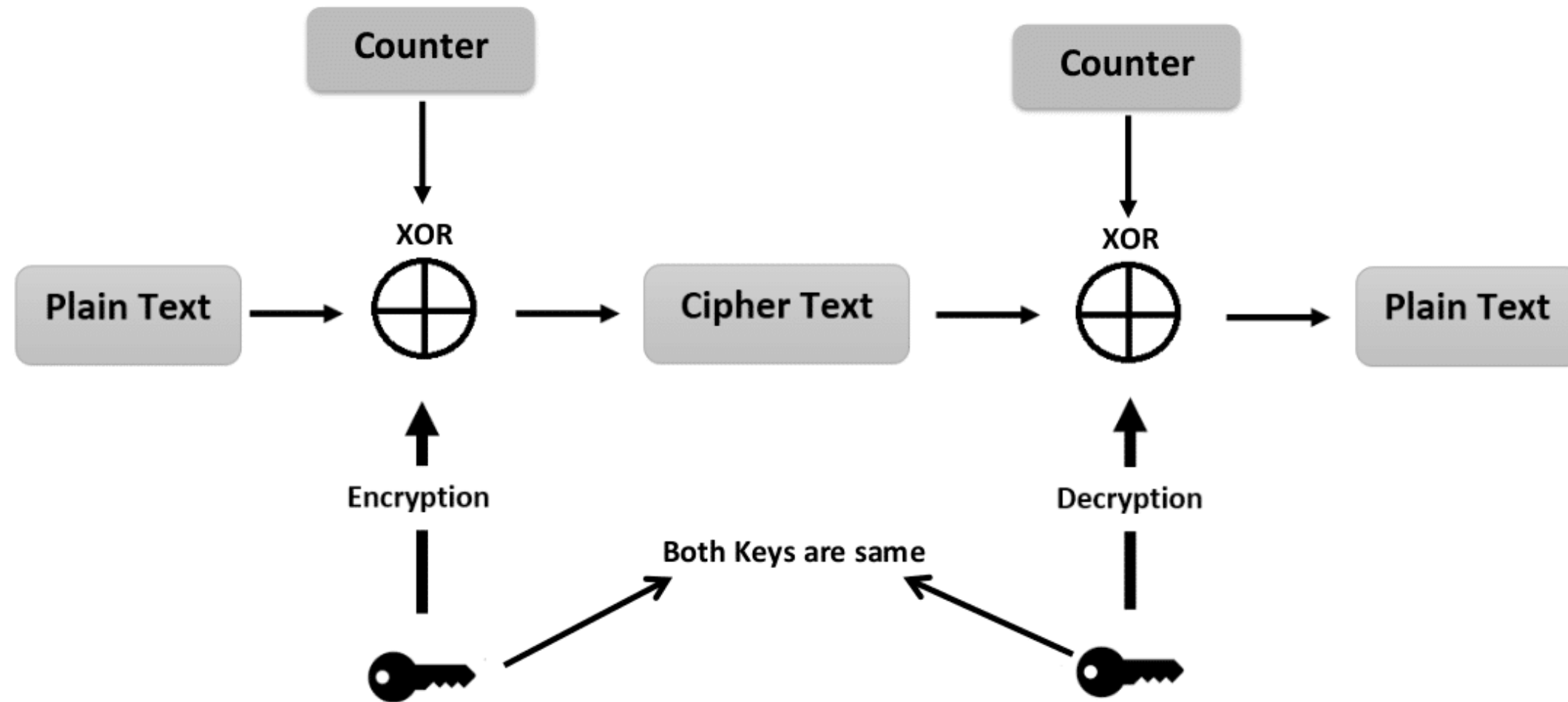
Write out your deepest secrets
without a worry ;-)

They're safe with encryption



AES-GCM
encryption

AES GCM



Confidentiality



Integrity (MAC)



Authenticity



Privacy
By Design

01

Proactive & Preventative

- Do not store encryption key
- Use public metamask key
- Toggle storage

02

Privacy as the Default Setting

- Minimal info. needed from user.
- No linkage to user's identity.
- No integration with third party apps
- Data deletion policy

03

Privacy Embedded into Design

- Keep things uncomplicated.
- Idea is to replicate the process of taking notes in a notebook.

04

Full Functionality - Positive-Sum

- Privacy
- Security
- Usability

05

End-To-End Security

- Collection of data
- Saving of notes
- Deletion

06

Keep it Open

- Opensource
- Transparent
- Clear

07

Respect for User Privacy

Do not collect PII

User-Centric: alternative to big tech.

Our site has no trackers :)



Fair Information Practices

- **Notice**
 - Through privacy policy, cookie policy & home page
- **Choice:**
 - Collect no PII, so nothing to process
 - Choice for data storage and authentication
- **Access and Control:**
 - Full access to notes and public address. Nothing else we collect.
 - Option to delete individual notes and whole account

Security

- Cryptographic verification of user through Metamask.
- Store JWT in HTTP-only cookie.
- AES-GCM encryption to store all notes.
- MongoDB Atlas uses its own encryption in transit and at rest (Enterprise).
- Private key for storage stored in IndexedDB with extractable property set to false, so no one can tamper with it. (Cannot be read by client side scripting in the browser)

GDPR

- Lawfulness, fairness and transparency - **Do not process any data**
- Purpose limitation - **Do not process any data**
- Data minimization - **Only data collected is notes written by user**
- Accuracy - **User has freedom to update notes at any time, we do not tamper with the notes.**
- Storage limitation - **We only store the notes and Metamask address, user can delete at any time.**
- Integrity and confidentiality - **Notes are encrypted**
- Accountability - **Privacy policy shows everything**



PIPEDA

1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection
5. Limiting Use, Disclosure, and Retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance

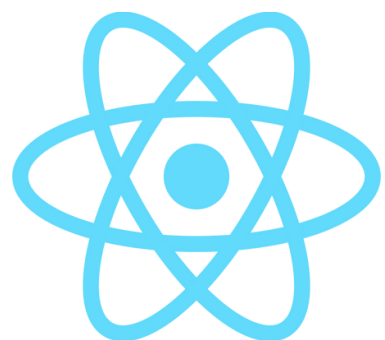


GDPR Compliant

Lawfulness, fairness and transparency	Do not process any personal data
Purpose limitation	Do not process any personal data
Data minimization	Only data collected is notes written by user
Accuracy	User has freedom to update notes at any time
Storage Limitation	We only store the notes and Metamask address, user can delete at any time.
Integrity and confidentiality	Notes are encrypted
Accountability	Privacy policy lays out everything



Tech Stack



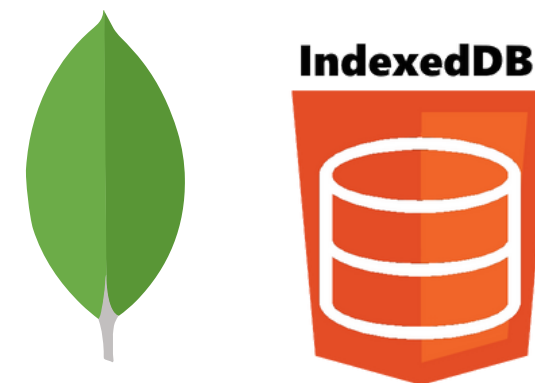
React

Frontend



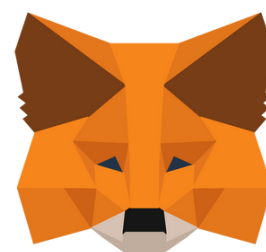
Node.js

Backend



Storage

Database: MongoDB
(or) IndexedDB



Metamask

Login scheme



Vulnerabilities from NVD

React	CVE-2018-6341	Fixed
Dexie	CVE-2022-21189	Fixed, but we don't use the affected method
Axios	CVE-2020-28168	Fixed
Axios	CVE-2021-3749	Fixed



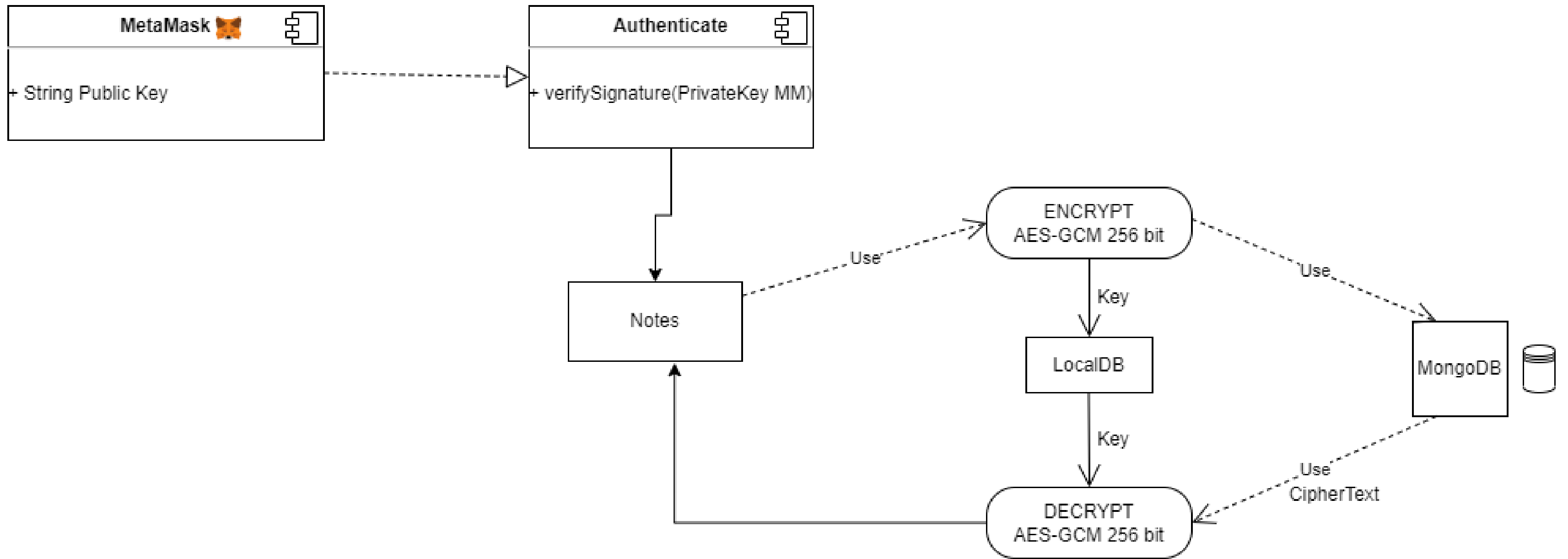
Possible concerns

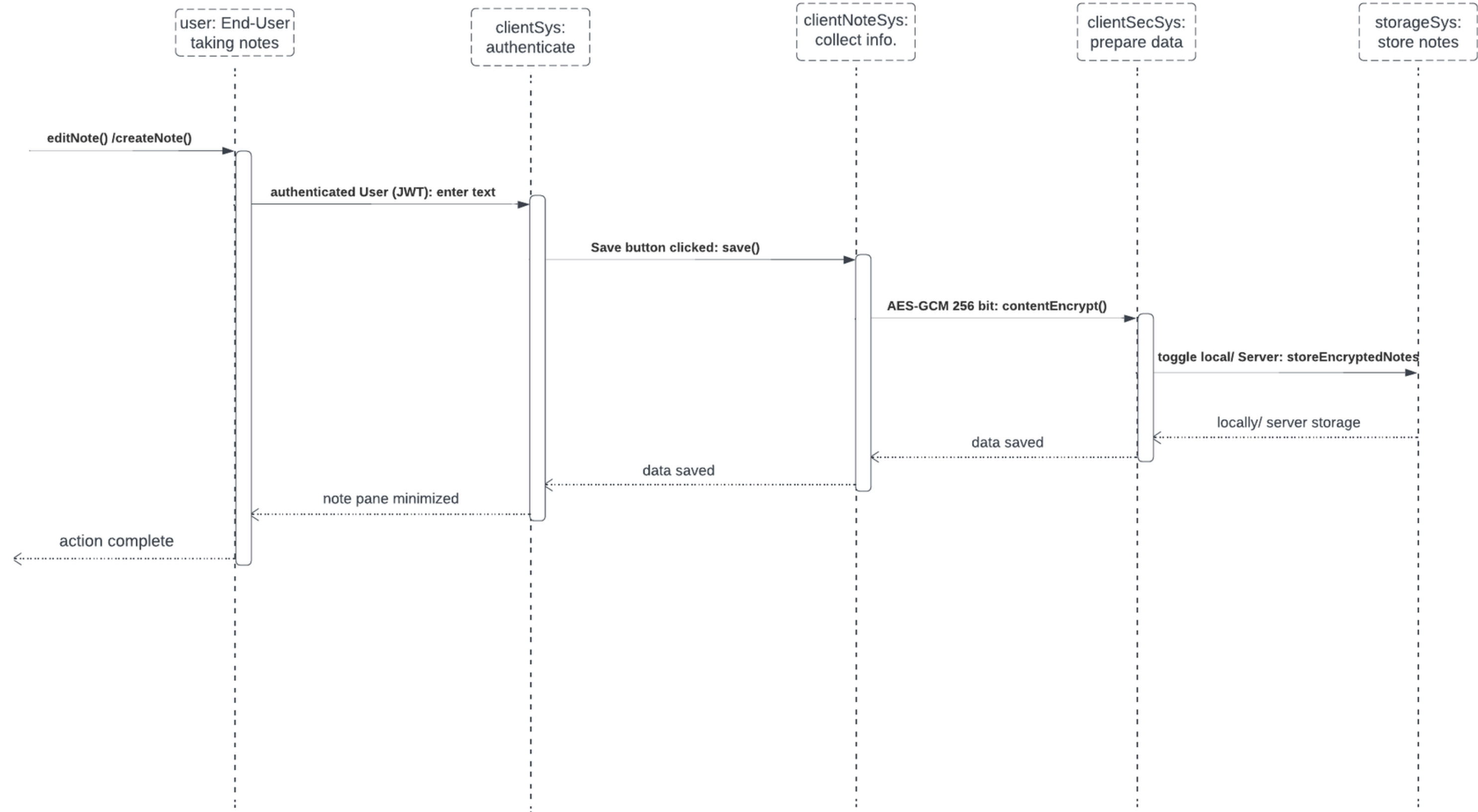
Identification possible, although subject to how user uses Metamask

- Data is heavily anonymized using Metamask public address.
- But depends on usage of user. Can always create a new wallet.

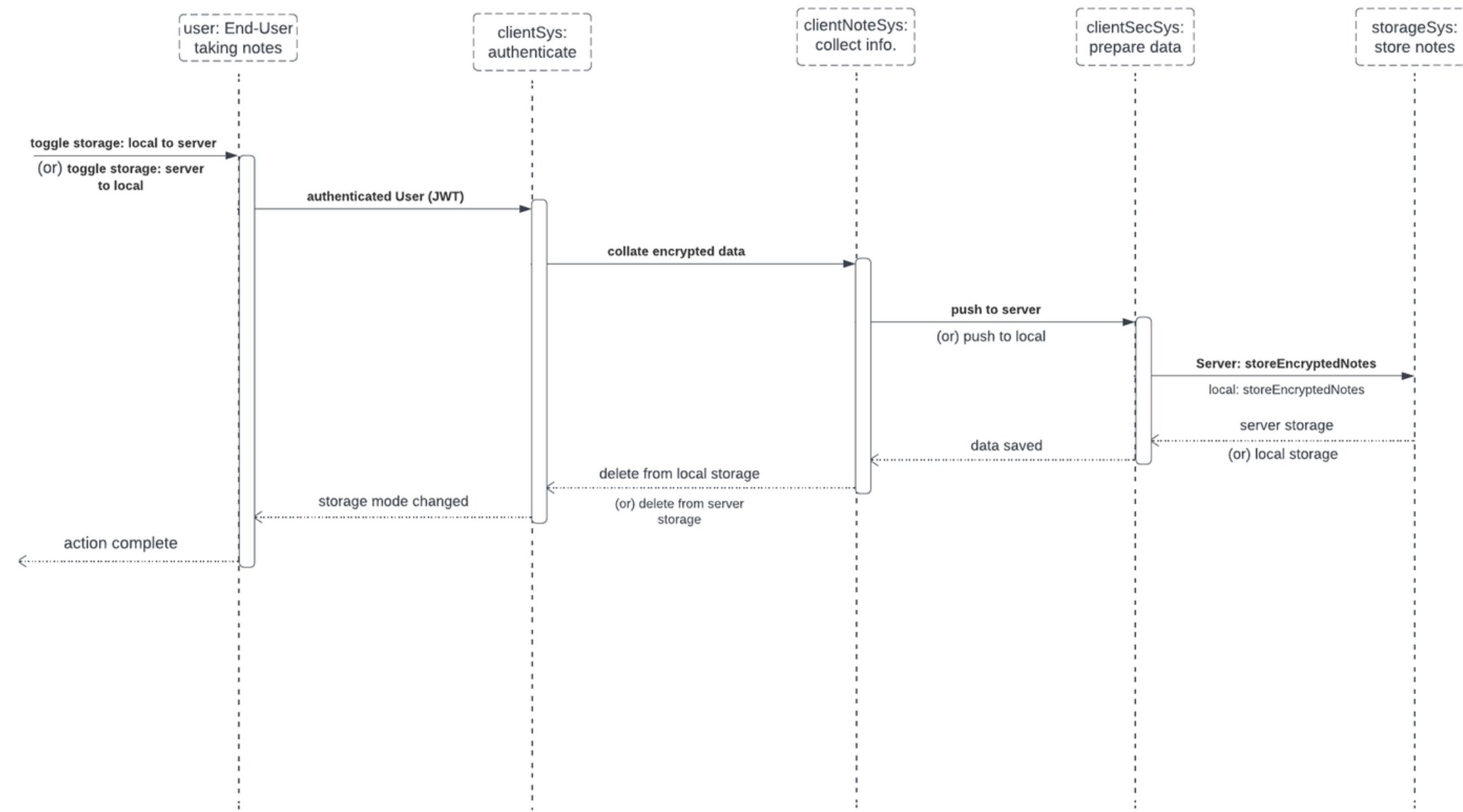
Architecture Diagrams







Storage Modes



Data deletion

(when mode toggled)

(retention
practices by
default)

Demo



Future enhancements

- 01 Decentralized Instantiation: Have a set of trusted devices.
- 02 Secure notes sharing with multimedia
- 03 Empowering authors: Using texts written as NFTs and receive payments for their work under pseudonyms.



