Server Under the Mountain (SUM)

Problem

As a user or organization you cannot easily host a cryptographically secure server for specific data types such as notes, tasks, documents, media, contacts, and more.

Existing solutions are either proprietary and therefore not easily auditable for security or they require extensive configuration by a user with a background in IT infrastructure. Most popular application suites track user behavior and serve ads, which is a major privacy concern.

Open source solution for managing a **private, secure, and highly scalable** data repository.

Server Under the Mountain (SUM)

SUM Notes

SUM Gallery

SUM Calendar

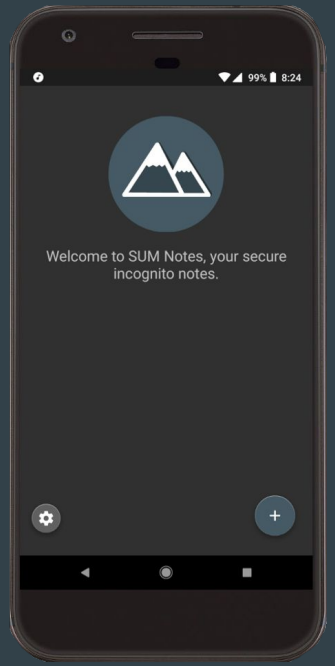
... and more applications built around privacy and security.

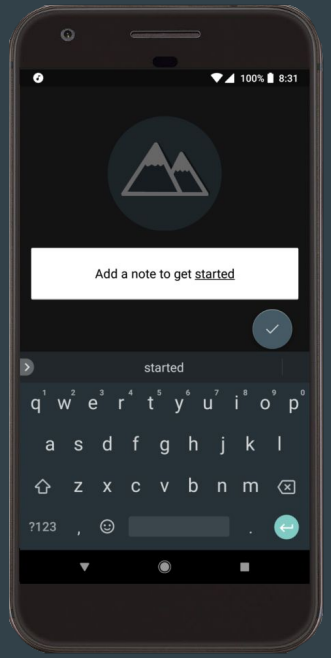
Primary Roles

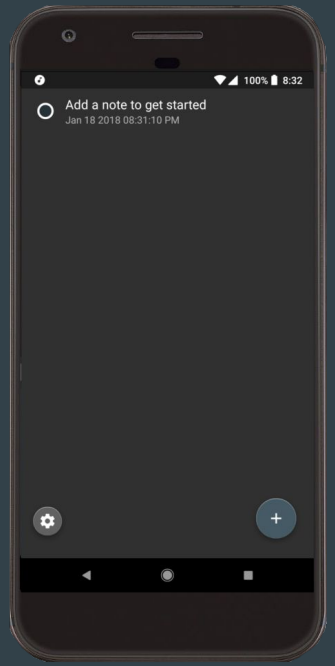
Alex	Full Stack & Cross-Platform Developer
Collin	Architecture Lead, Full Stack & Cross-Platform Developer
Michael	Web Developer, Release Lead
Luke	Project Manager, Scrum Master, Android Developer
Jessica	Security Architect, Threat Analysis Documentor, Android Developer

SUM Notes - Built for short thoughts and long markdown documents.

Proof of Concept for supporting mobile devices on our cross-platform software suite.







Security Options

a. **Complete Lockdown** - For the ultra paranoid

   Data never leaves one device, it's only stored locally and all data is encrypted.

b. **Secure Cloud** - The average user

   All data is encrypted in a local database, zipped locally on a specified schedule, then the encrypted zip file is uploaded to a cloud storage provider. Even if your cloud provider is hacked they do not have the ability to decrypt your data since they do not own the key to decrypt the zip file. The cloud storage provider offers a layer of protection for your data because of authentication with TLS, optional 2FA, and optional U2F.

Additional Features

No Trackers

SUM applications do not use any analytics to monitor user behavior.

Scheduled Cleanups & Incognito Modes

Delete select types of data on a schedule or purge everything across multiple apps.

Highly Extensible

Developers can add SUM services to existing applications to offer more security.

Safe Import & Export

Easily move data from your secure repository to other apps, or the other way around.

Minimal Footprint & Enhanced Accessibility

No bloatware and easily accessible open source files mean quicker security audits and localization.

Easily Side-Loadable

Basic instructions for how to compile and load onto devices instead of going through an app store.

End of Proposal

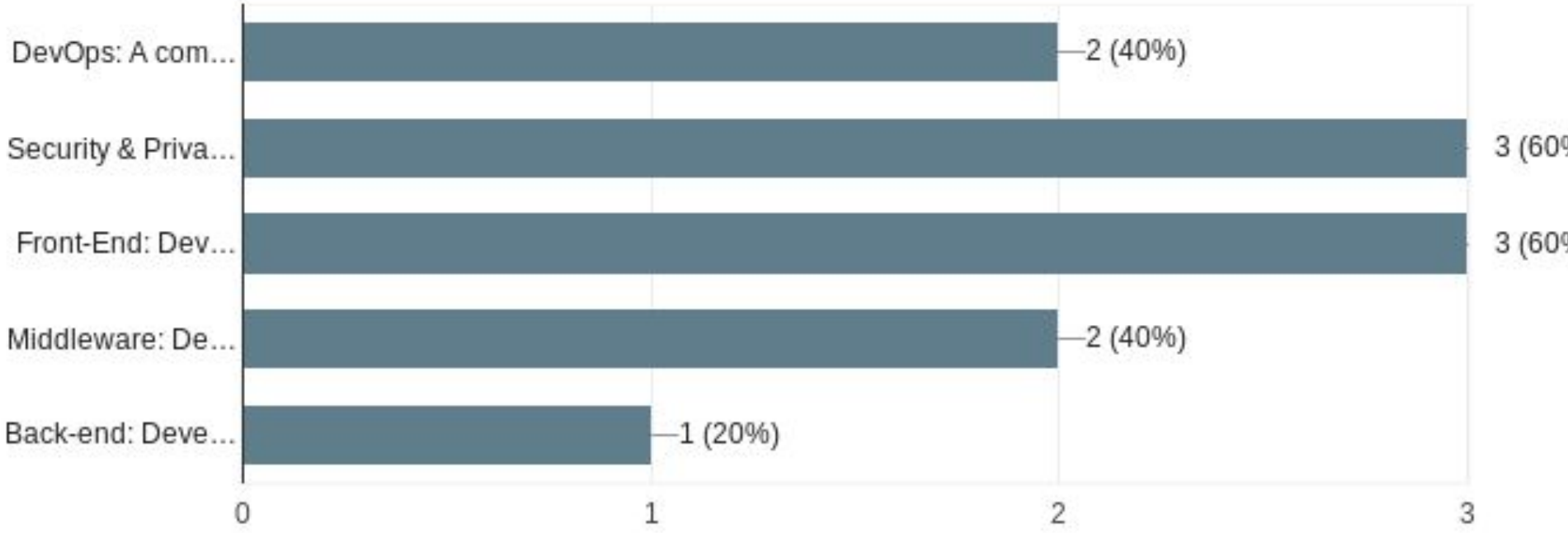
Up Next: Roadmap & Sprint Planning →

Server Under the Mountain (SUM)

Roadmap & Sprint Planning

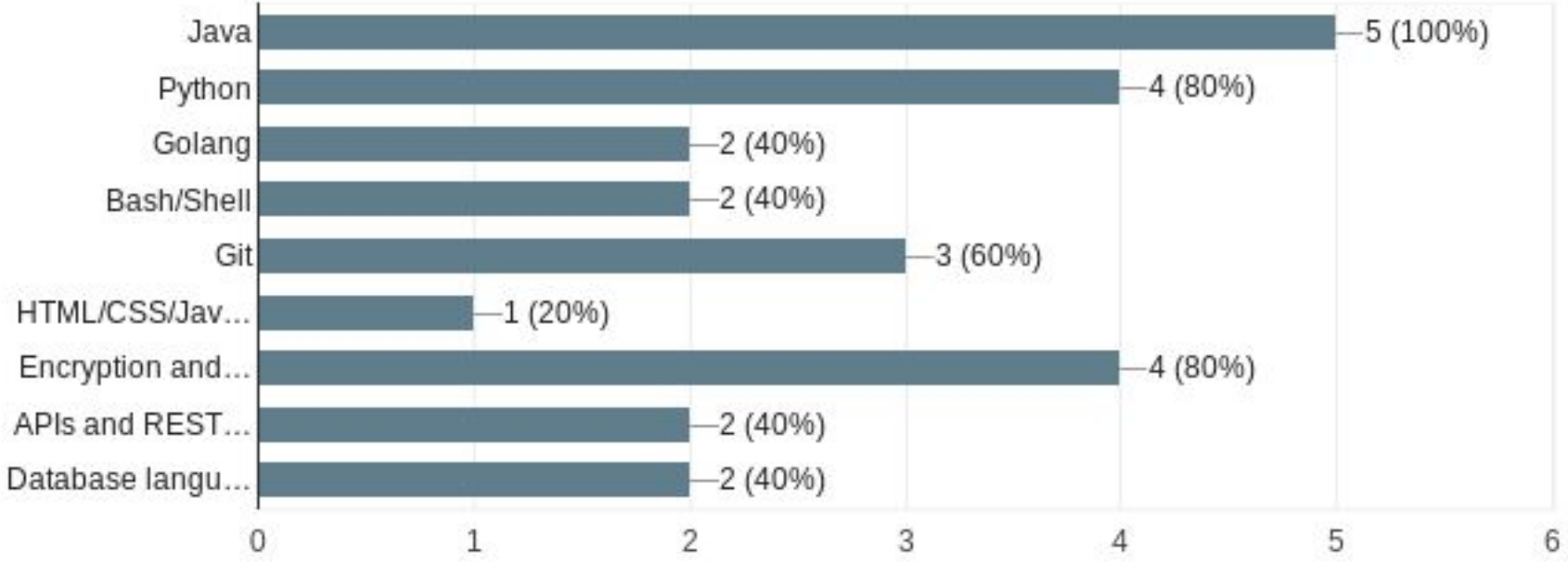
Select 1 to 3 roles you want to focus on

5 responses

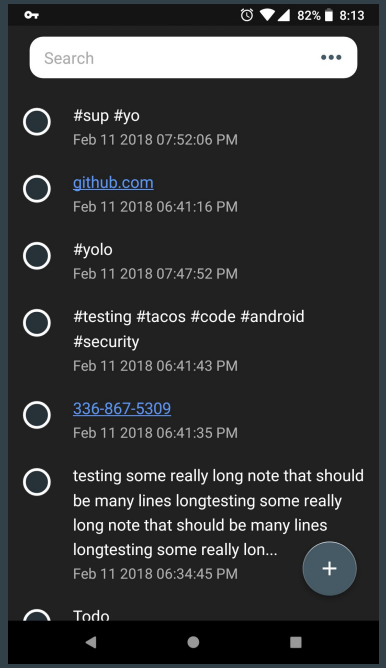


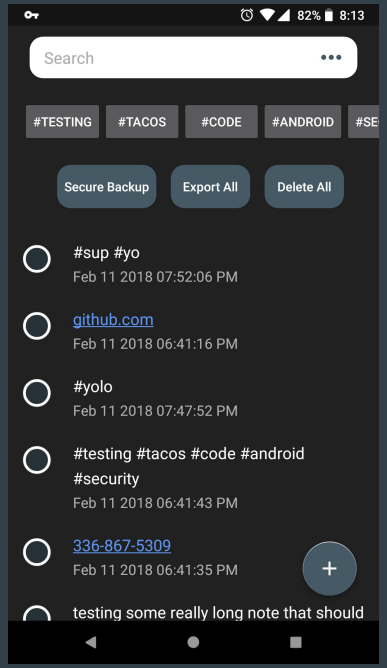
What languages and tools are you familiar with? (If you've written something slightly more complex than "hello world", but you don't have to be an expert in it)

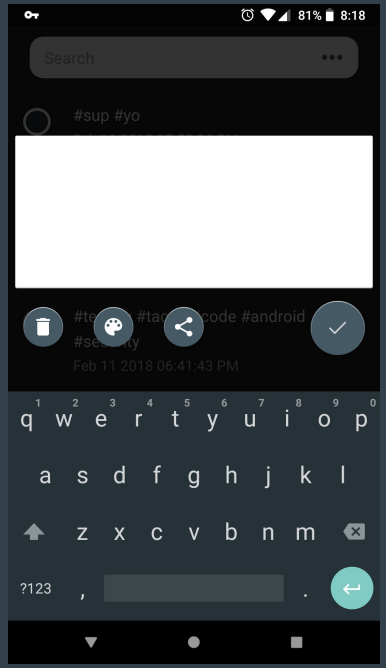
5 responses



SUM Notes - Progress







Automatically creates links for urls, phone numbers, email addresses, map addresses, and tags.

Ability to search through notes

Tap a tag below the search bar to show all notes with the same tag

Support for short notes and long lists

Blocks other apps from acquiring screen content, blocks screenshots, uses API to request incognito mode for keyboard

Option to export all data to another app that accepts strings or quick purge of all data

Mobile Clients

Supporting Android devices for all SUM apps (no iOS)

1. Start a Notes app with locally encrypted data in a SQLite database using SQLCipher
2. Expand the Note app's database capability to export an encrypted zip file of all content
3. Utilize cloud provider APIs to do user authentication and upload the encrypted zip file (of the notes) to a user's account

> We are going to support Mega as an open source cloud storage provider and DropBox as a proprietary option.

Once we have developed the back-end for an encrypted SQLite database and middleware for cloud storage APIs then we can expand our product offerings to other types of apps (SUM Calendar, SUM Gallery, etc).

Web Presence

Create a splash page that explains what SUM is and what we have to offer. This is served in the GitHub repo and requires no hosting or maintenance.

Getting started - HTML, CSS, Javascript

1. Create a repository on GitHub and use one of their "GitHub Pages Templates" as an initial version.
2. Customize the template, theme it, add logo, and start writing marketing content that tells users what we have to offer.

End of Roadmap & Sprint Planning

Up Next: Requirements -->

Server Under the Mountain (SUM)

Requirements

Problem

As a user or organization you cannot easily host a cryptographically secure server for specific data types such as notes, tasks, documents, media, contacts, and more.

Existing solutions are either proprietary and therefore not easily auditable for security or they require extensive configuration by a user with a background in IT infrastructure. Most popular application suites track user behavior and serve ads, which is a major privacy concern.

Requirements

- Functional
  - Front-end application for input of Note content
  - Locally encrypted database
    - Read/Write locally encrypted database by entering the encryption password
    - Cloud provider APIs to upload or download encrypted file
- Usability
  - Minimalistic layout and controls designed for the average user
  - Technical functionality is available for more experienced users

Requirements

- System
  - Hardware: Mobile Device
  - Software: Android Operating System
  - Database: NoSQL DB (encrypted) and optional cloud storage providers with zero-access (NextCloud, DropBox)
- Privacy & Security
  - Block other apps from acquiring screen content
  - Block screenshots
  - Requests incognito mode from system keyboard
  - NoSQL database (AES 256 encrypted)
  - All data stays encrypted locally unless you use the export tool

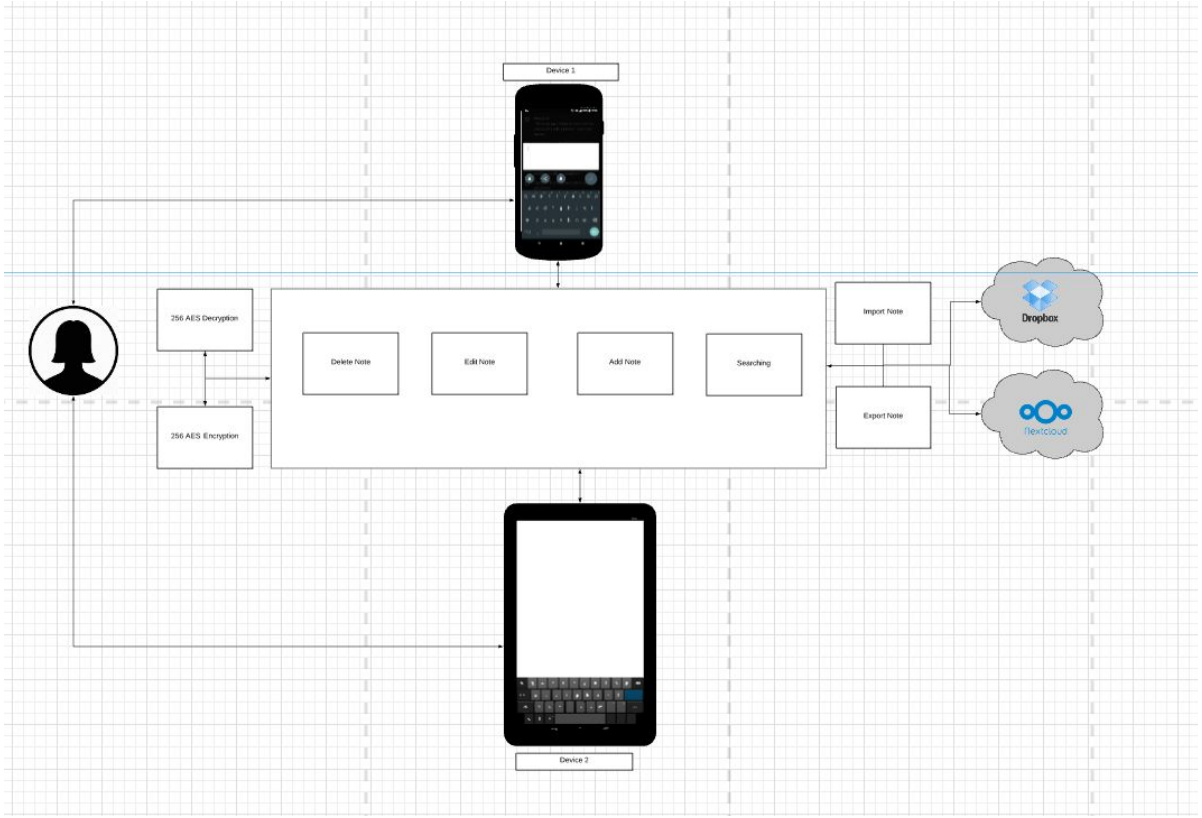
Subsystems

- **Encryption Subsystem**
  - AES encryption
  - AES decryption
- **File Management Subsystem**
  - Add, edit, delete notes
  - Broad data actions (eg. delete all)
- **Search Management Subsystem**
  - Search by tag: use a regular expression to parse hashtags in notes for categorical grouping
  - Search by phrase: raw string searching

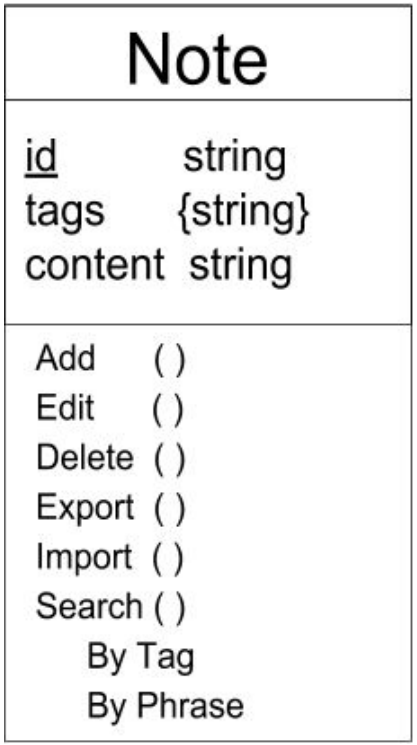
Subsystems

- **Import & Export Subsystem**
  - Local Storage: Import or export encrypted notes file
  - Cloud Storage: Authenticate to import or export encrypted data
- **UI & UX Subsystem**
  - Android app

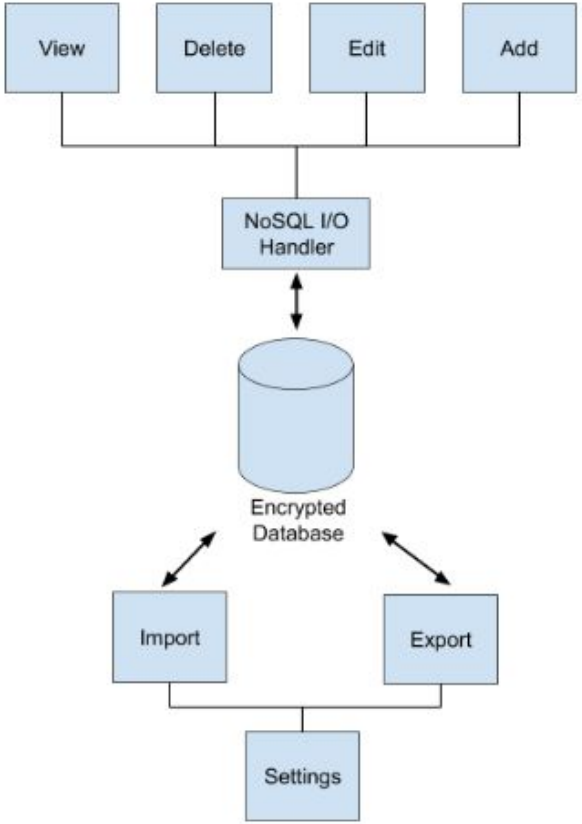
Subsystems


Device 1
256 AES Decryption
256 AES Encryption
Delete Note
Edit Note
Add Note
Searching
Import Note
Export Note
Dropbox
nextcloud
Device 2

Entity Relationship Model

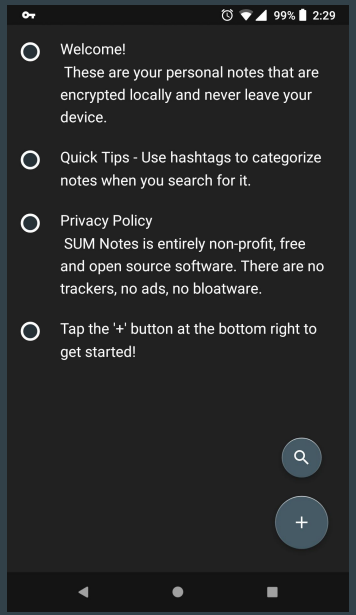


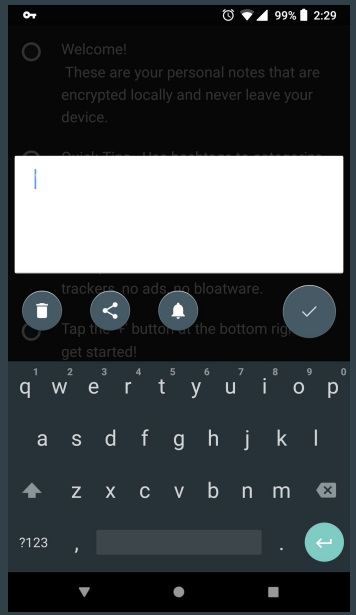
Sub-System Communication

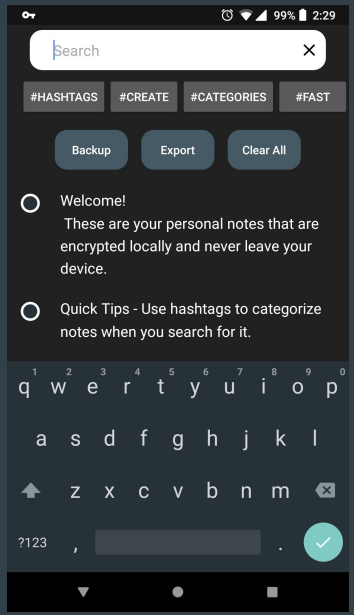


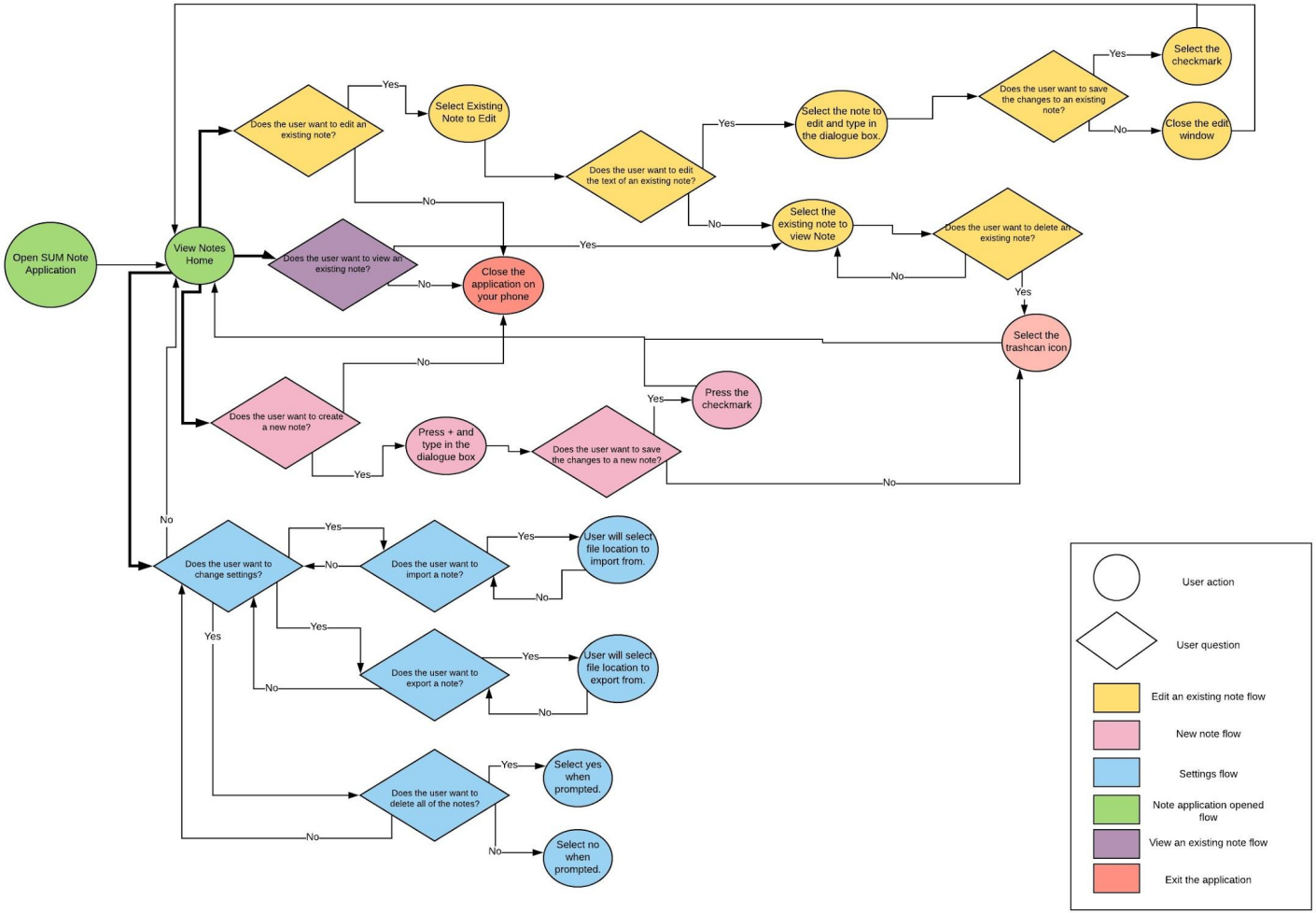
User Flow

1. Download the app from the Google Play Store and open it
2. Learn about the privacy policy and security features by reading the default notes
3. Enter personal note content








Open SUM Note Application
View Notes Home
Does the user want to edit an existing note?
Yes
Select Existing Note to Edit
No
Does the user want to edit the text of an existing note?
Yes
Select the note to edit and type in the dialogue box.
No
Select the existing note to view Note
Does the user want to save the changes to an existing note?
Yes
Select the checkmark
No
Close the edit window
Does the user want to delete an existing note?
No
Yes
Select the trashcan icon
Does the user want to view an existing note?
Yes
No
Close the application on your phone
Does the user want to create a new note?
No
Yes
Press + and type in the dialogue box
Does the user want to save the changes to a new note?
Yes
Press the checkmark
No
No
Does the user want to change settings?
Yes
Does the user want to import a note?
Yes
User will select file location to import from.
No
No
Yes
Does the user want to export a note?
Yes
User will select file location to export from.
No
No
Yes
Does the user want to delete all of the notes?
Yes
Select yes when prompted.
No
Select no when prompted.
No
User action
User question
Edit an existing note flow
New note flow
Settings flow
Note application opened flow
View an existing note flow
Exit the application

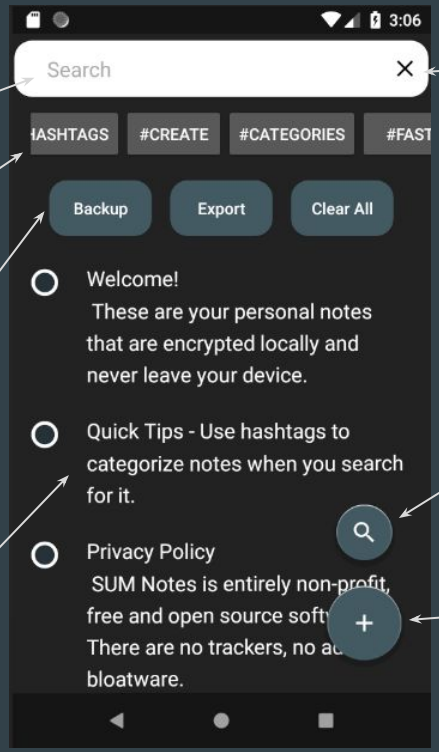
Detailed Design and Controls

Lets the user search by string or hashtag

Direct way to search by available hashtags

Quick commands for all data

A note. This one is preloaded as a user guide



Closes search bar and commands

Opens search bar and commands

Opens new note editor

Data Dictionary

One primary object that's stored in an encrypted database: Note (long id, string content, string tags)

Table Structure	`CREATE TABLE NOTES ( _ID INTEGER PRIMARY KEY AUTOINCREMENT, CONTENT TEXT, TAGS TEXT)`
Add Note	`INSERT INTO NOTES ( CONTENT , TAGS )`
Update Note	`UPDATE NOTES SET ( CONTENT, TAGS ) WHERE _ID = X`
Remove Note	`DELETE FROM NOTES WHERE _ID = X`

Algorithm Analysis

- Loading encrypted data: SQLCipher.getWriteableDatabase(<pw>)
- Writing encrypted data: SQLCipher.insert(<string>)
- Downloading data from cloud provider: Small text strings, not resource intensive
- Parsing tags: Search newly inserted note content for hashtags using regex and store the list with references to the row ID - O(n) for string length

(Optional) Cloud Services

Dropbox is a popular and easy to use service for Syncing and Sharing files.

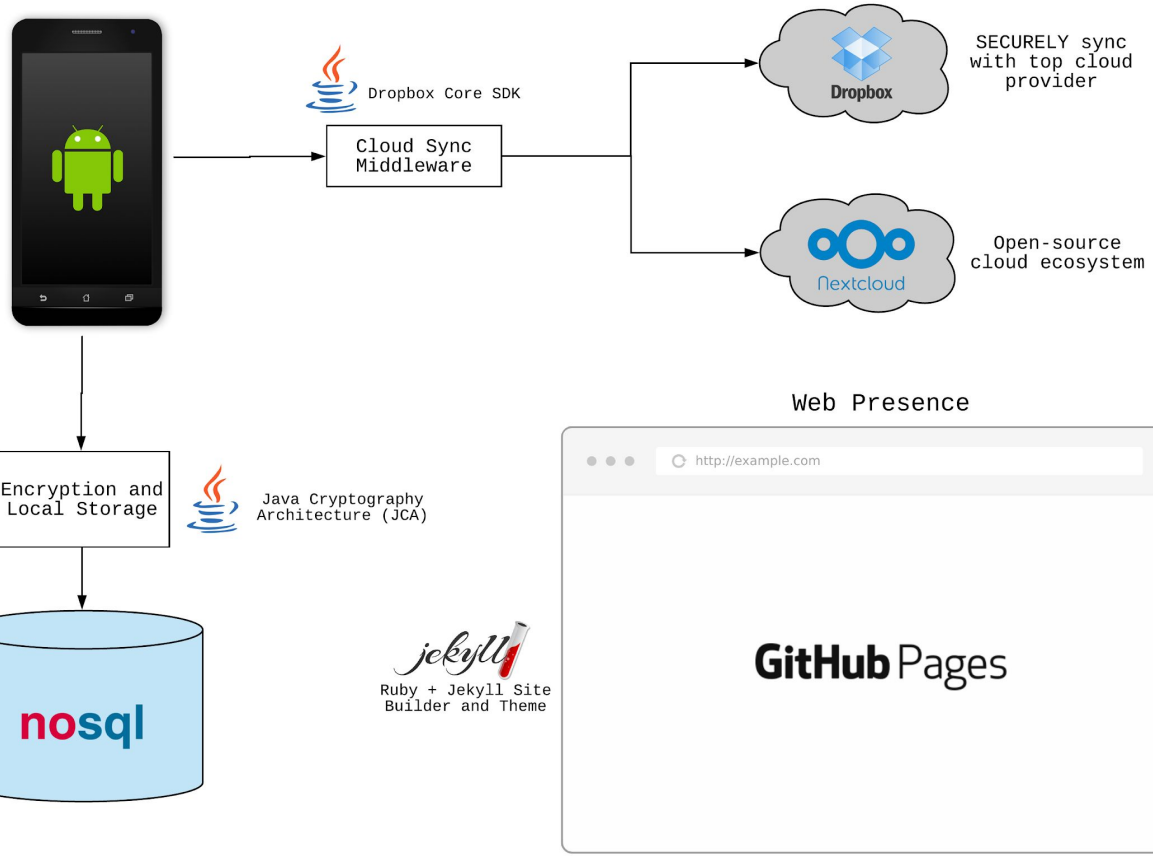
- Gives users an easy and reliable method to store data encrypted using our service
- Smooth and easy API

Nextcloud is a open source Enterprise File Sync and Share.

- Can be audited for extra assurance
- AES-256 E2E Encryption over TLS
- Users can visit the site and create accounts anonymously without providing personally identifiable information
- Publicly available threat model

SUM Architecture

Michael Burke, Jessica Denney, Collin Guarino, Alex Hahn, Luke Roosje



End of Requirements

Up Next: Scrum Report →

Server Under the Mountain (SUM)

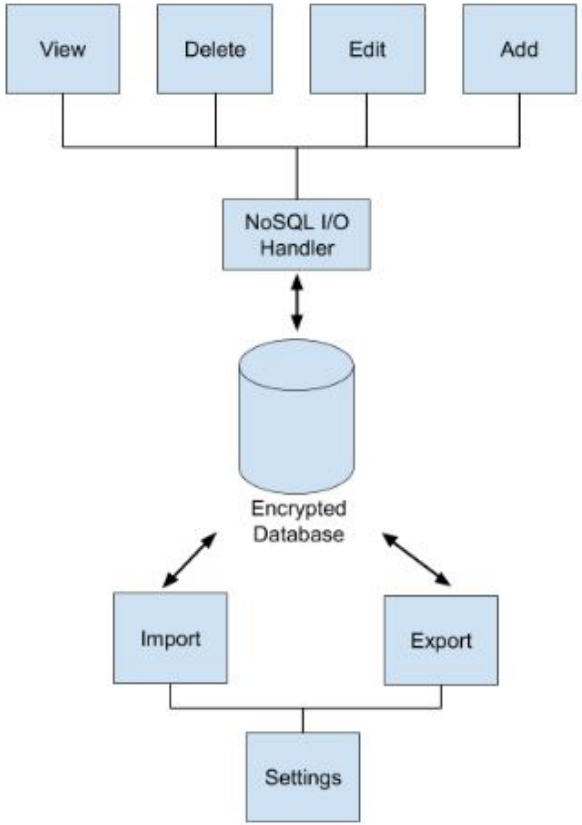
Scrum Report

Problem

As a user or organization you cannot easily host a cryptographically secure server for specific data types such as notes, tasks, documents, media, contacts, and more.

Existing solutions are either proprietary and therefore not easily auditable for security or they require extensive configuration by a user with a background in IT infrastructure. Most popular application suites track user behavior and serve ads, which is a major privacy concern.

Sub-System Communication



Sprint Roadmap (2 week sprints)

1

(1/22 - 2/2)

Basic Notes App
- Local storage
- No encryption
- Add notes
- Edit notes
- Delete notes

2

(2/5 - 2/16)

Encryption/Decryption
- Encrypt with AES
- Decrypt with AES

Searching/Tag Filtering
- Add tags to notes
- Removes tags
- Search for a tag
- Select a tag

3

(2/19 - 3/2)

Security
- Master password to access secure notes file

Cloud Sync
- Send encrypted notes to cloud storage

Web Presence

Information detailing…
- Security in the app
- Privacy policies
- Functionality and instructions

Sprint Roadmap (2 week sprints)

4

(3/12 - 3/23)

Password Manager

- Add passwords
- Edit passwords
- Delete passwords
- Copy/autofill password to another application for login

5

(3/26 - 4/6)

Security Audit

- Detail flow of information
- Detail security measures

Web Presence 2.0

Information detailing...

- Storage of password data
- Functionality and instructions

Product Backlog

TOTAL: 121 HOURS

Story Points	User Story
3	As a user I want to add a note
2	As a user I want to delete one note
2	As a user I want to delete all notes
3	As a user I want to scroll through all notes I have saved
4	As a user I want to edit a note and its tags
7	As a user I want to export my notes to another app (cloud provider)
10	As a user I want to search for a note based on its content
10	As a user I want to search for a note based on its tag
5	As a user I want to set an encryption key phrase
10	As a user I want all data to be encrypted
3	As a developer I want to decrypt the notes database for user on a desktop
20	As a developer I want to easily view security audits of the app
5	As a developer I want to easily view the source code of the app
5	As a user I want to understand what security tools mean for me
5	As a user I want to understand the app's privacy policy and what data is stored in what location(s)
7	As a user I want to download the app from the Google Play Store
20	As a user I want to learn about the app from a public web page