MobiPass - Tool that uses smartphone biometrics for browser password management

Password managers are essential utility tools that save us the trouble of entering username passwords for every website we visit. Such password managers are often based on a login mechanism that enables access to all the passwords stored. The login is usually password based. When users enter correct passwords, the system then autofill login credentials on websites visited.

Most existing systems are based on following mechanisms:

1. The password manager is often a browser plugin.
2. The user decides a master password that is used to encrypt all other passwords and store them locally on the machine (Or on cloud)
3. The individual logins for websites are detected by browser extensions, encrypted and stored. Whenever the website login form is detected again, the extension auto-fills the credentials.

What is wrong in existing solutions?

1. Master password if compromised, all security features lost
2. Storing passwords locally (Even if encrypted) does have some level of risks. Encryption can be broken.
3. No way to grant partial access to others trying to login.

Proposed solution:

1. Smartphone fingerprint replaces passwords
2. Browser extension exists, but encrypted data stored only on smartphones.
3. Every time user tries to login, plugin notifies smartphone. Smartphone authenticates fingerprint and then sends the login credentials to browser plugin.
4. Data transfer between smartphone and browser is end to end encrypted (So no man in middle can steal credentials)
5. Browser plugin knows which smartphone to send authentication request to by entering a unique key (device identifier).

6. When user authenticates on smartphone, the smartphone prompts which device is requesting the login details, and also prompts the website name.
7. Users can share their smartphone ID to friends trying to login. The browser plugins on the friend’s browser will send request to user smartphone. The user will verify fingerprint and confirm the access to a particular website.
8. Saving a new password is equally easy – when the browser plugin detects a new website login, it generates a barcode. Scan the barcode on smartphone to save the credentials.
9. Alternatively, enter the smartphone ID as default password management device.
10. Cloud backup of the encrypted data will allow users to easily change devices

How I plan to implement the solution:

1. Chrome/Firefox plugin in Python or JS
2. Android app with biometrics
3. Internet/Wifi/Bluetooth based smartphone discovery by browser
4. Using fingerprint for encrypting/decrypting all credentials
5. The data encrypted by fingerprints will be backed up to Google drive of the user. This will ensure security – Data sits behind password protected google drive that too in encrypted format.

I plan to make this entire system available as an open source project