**Application Name:** Carbon

**Author:** Nathanael Memis

**Introduction:**

Carbon is a password manager built for multi-device usage. Carbon is built using proper information security techniques which includes hashing, encryption, and Google sign in service.

**Tech stack:**

1. Authentication: Google Sign In
2. Backend & Database: Firebase
3. Frontend: HTML & CSS

**Data Flow:**

1. Sign In using Google.
2. Firebase returns encrypted user data.
3. Frontend decrypts user data using the user’s UID + saved account UID. This method allows salting to have different encryptions for each saved account.
4. Frontend displays decrypted user data.

**Database No SQL in JSON:**

user\_uid {

account\_uid {

“account\_name”: “encrypted\_string”,

“account\_password”: “encrypted\_string”

},

…

}

**Encryption/Decryption Protocol:**

Encryption/Decryption should be done 300 times using AES algorithm.