

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО

МОБІЛЬНИЙ ДОДАТОК ОБМІНУ ЗАХИЩЕНИМИ ДАНИМИ З ВИКОРИСТАННЯМ ЗВУКОВИХ СИГНАЛІВ

Підготував:
Пономарьов Микола
студент групи: ТВ-з71м

Керівник:
к.т.н Карпенко Євген Юрійович

Актуальність роботи

Мобільні додатки стали одним з головних трендів у розвитку інформаційних технологій в останні роки. Кількість розробників мобільних додатків збільшується, кількість доступних додатків зростає. Все більше компаній зацікавлені в розробці програми, яка допоможе їм досягти успіху в своїй галузі і обійти конкурентів.

Основною перевагою мобільних додатків є те, що користувач може отримати доступ до них, перебуваючи в будь-якому місці і в будь-якій ситуації. Це відкриває великі можливості щодо впровадження різних сервісів, які раніше були недоступні. Важливу роль також відіграє соціалізація додатків, тобто додавання функцій соціальних мереж, які дозволяють користувачем ділитися своїми досягненнями і знаходити нових друзів.



Одним з безлічі типів додатків для мобільних пристроїв є додатки для подорожей і туризму. Особливо під час таких подорожей мобільні додатки повинні краще працювати в оффлайн режимі, тому що то завжди у будь який момент часу у вас буде доступ до інтернету або мобільного оператора. На даний момент багато туристів мають мобільні пристрої і використовують їх під час подорожей, і компанії, що не мають таких додатків, втрачають безліч потенційних клієнтів.

Мета дослідження

Метою роботи є розробка мобільного додатку, який використовує звукові сигнали як спосіб обміну даними між користувачами, а також й інші методи за допомогою яких можна здійснювати обмін даними.

Поставлені завдання

1. Розглянути та проаналізувати мови програмування для розробки мобільного додатку.
2. Розглянути та проаналізувати моделі реалізації мобільного додатку.
3. Розглянути та проаналізувати технології обміну даними.
4. Створити алгоритм роботи мобільного додатку.
5. Реалізувати алгоритм.

Об'єкт

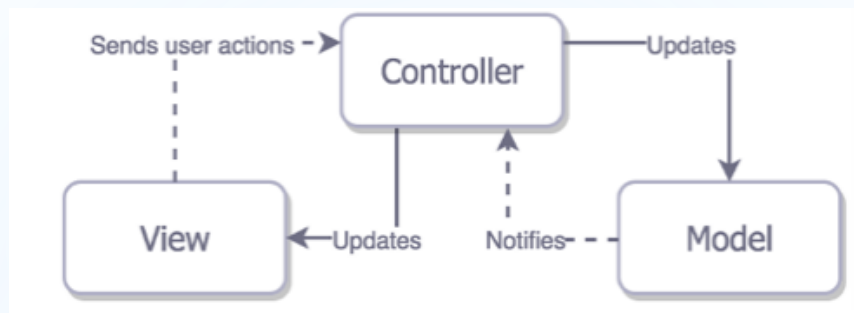
Обмін захищеними даними з використанням звукових сигналів.

Предмет

Мобільний додаток з обміну захищеними даними.

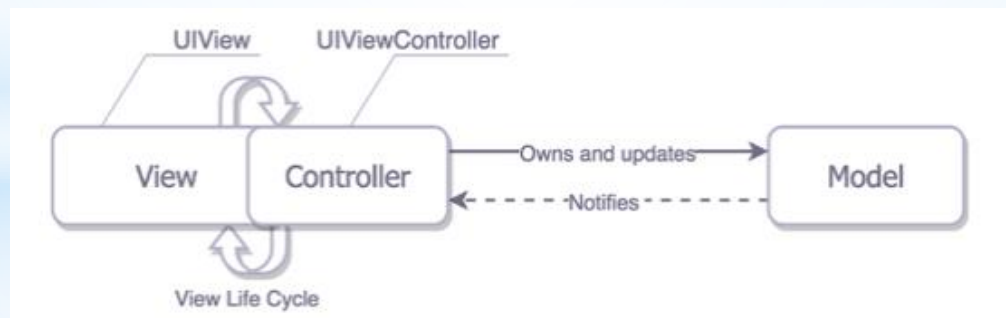
Архітектура мобільного додатку

У шаблоні архітектури Apple MVC контролер буде посередником між View і Model, щоб ці два об'єкти не знали про існування один одного. Найбільш часто використовуваним об'єктом буде контролер. У цьому є плюси, тому що в додатку повинно бути місце для всієї складної бізнес-логіки, яка не вписується в Model.



Apple MVC

В реальності шаблон Apple MVC працює по-іншому. Перевантажений контролер містить в собі велику кількість бізнеслогіки, перетворюючи Model View-Controller в Massive-View-Controller. Cocoa MVC заохочує писати Massive-View-Controller, тому що вони дуже сильно залучені в життєвий цикл View, що призводить до нероздільності цих двох сутностей.



Практичний Apple MVC

Приклади моделей мобільного додатку

Середовище X-Code має свій framework для роботи з базами даних - це CoreData. Завдяки ньому можна створювати суб'єкти баз даних на системі управління MySQL.

Attribute	Type
 about	String
 chirpID	String
 city	String
 country	String
 date	String
 email	String
 firstName	String
 foundBy	String
 fullName	String
 jobTitle	String
 lastName	String
 location	String
 metLat	Double
 metLon	Double
 phone	String
 photo	Binary Data
 photoLink	String
 photoThumb	Binary Data
 photoThumbLink	String
 sectionTitle	String
 status	String
 timestamp	String
 type	String
 uid	String
 webSite	String

Суб'єкт CardContact, з його атрибутами

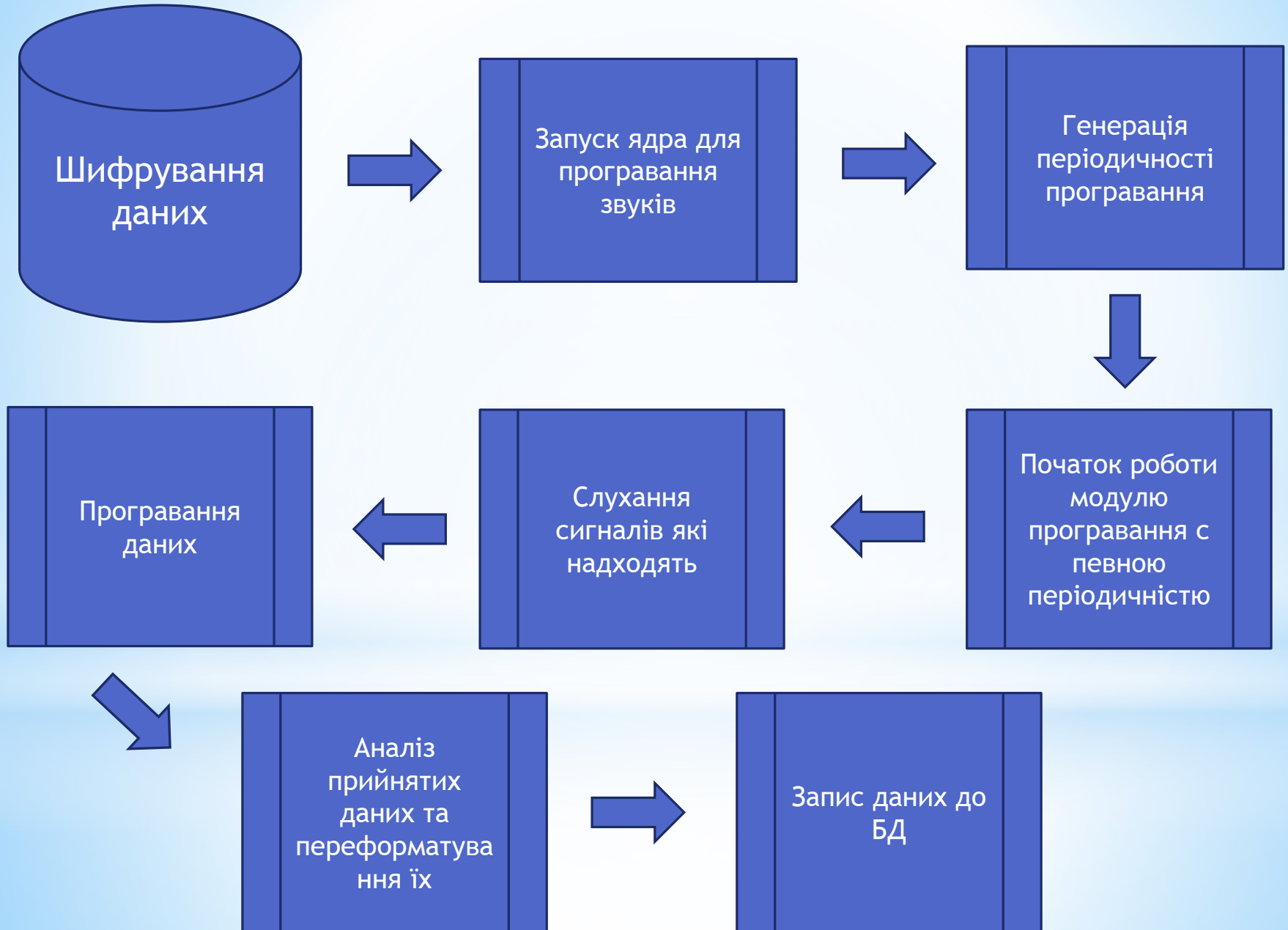
Attribute	Type
 identifier	String

Relationship	Destination	Inverse
--------------	-------------	---------

Fetches Property	Predicate
------------------	-----------

Суб'єкт ChirpContact, з його атрибутами

Архітектура модулю обміну даними за допомогою звукових сигналів



Стандарт кодування даних який використовується

Advanced Encryption Standard (AES) - симетричний алгоритм блочного шифрування, прийнятий урядом США як стандарт в результаті конкурсу, проведеного між технологічними інститутами. Він замінив застарілий Data Encryption Standard, який більше не відповідав вимогам мережевої безпеки, що ускладнилися в XXI столітті.

Криптографічний алгоритм вимагає ключ розміром в ту чи іншу кількість біт, щоб зашифрувати дані, як показано в схемі.

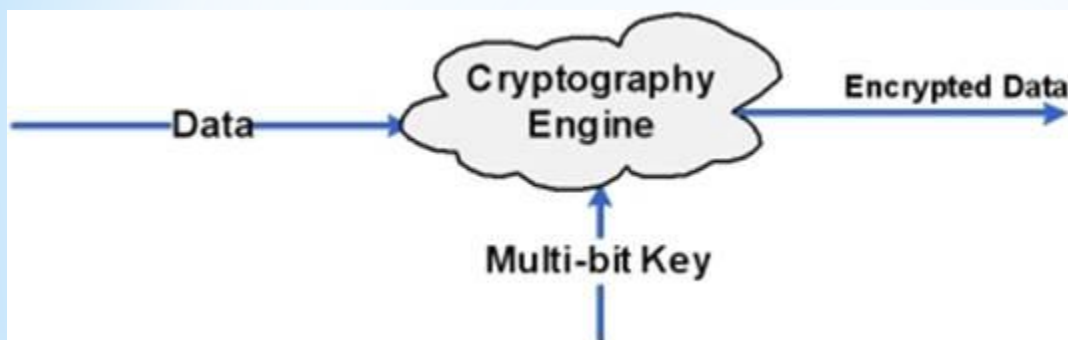


Схема 1

Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^9
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

Кількість комбінацій для розшифрування

Key size	Time to Crack
56-bit	399 seconds
128-bit	1.02×10^{18} years
192-bit	1.872×10^{37} years
256-bit	3.31×10^{56} years

Зверніть увагу на те, що в міру збільшення розміру ключа кількість комбінацій зростає експоненціально. Математичні обчислення доводять, що розмір ключа в 128 біт надійним чином захищає від лобової атаки.

Серверна частина



Firebase - американська компанія, постачальник хмарних послуг, заснована в 2011 році Ендрю Лі і Джеймсом Темпліном, і поглинена в 2014 році корпорацією Google.

Основний сервіс - хмарна СУБД класу NoSQL, що дозволяє розробникам додатків зберігати і синхронізувати дані між декількома клієнтами. Підтримані особливості інтеграції з додатками під операційні системи Android і iOS, реалізовано API для додатків на JavaScript, Java, Objective-C і Node.js, також можливо працювати безпосередньо з базою даних в стилі REST з ряду JavaScript-фреймворків, включаючи AngularJS, React, Vue.js, Ember.js і Backbone.js. Передбачено API для шифрування даних.

Серед інших послуг, що надавалися компанією - запущений 13 травня 2014 року хостинг для зберігання статичних файлів (таких як CSS, HTML, JavaScript), що забезпечує доставку через CDN і сервіс аутентифікації клієнта з використанням коду тільки на стороні клієнта з підтримкою входу через Facebook, GitHub, Twitter і Google (Firebase Simple Login).

```
245
246 - (void)createUserWithParams:(NSDictionary *)params completion:
      (UFLoginManagerCreateUserCompletionBlock)completion {
247
248     [[FIRAuth auth] createUserWithEmail:params[k_email] password:params[k_passw]
      completion:completion];
249
250 }
251
252 - (void)signInWithParams:(NSDictionary *)params completion:
      (UFLoginManagerCreateUserCompletionBlock)completion {
253
254     [[FIRAuth auth] signInWithEmail:params[k_email] password:params[k_passw]
      completion:completion];
255
256 }
```

Приклад створення нового користувача, або аунтифікація старого

Архітектура БД серверної частини

Основний сервіс - хмарна СУБД класу NoSQL. Метод роботі з СУБД полягає у тому що вона створюється за допомогою вузлів. Та використовує API від Firebase для взаємодії.

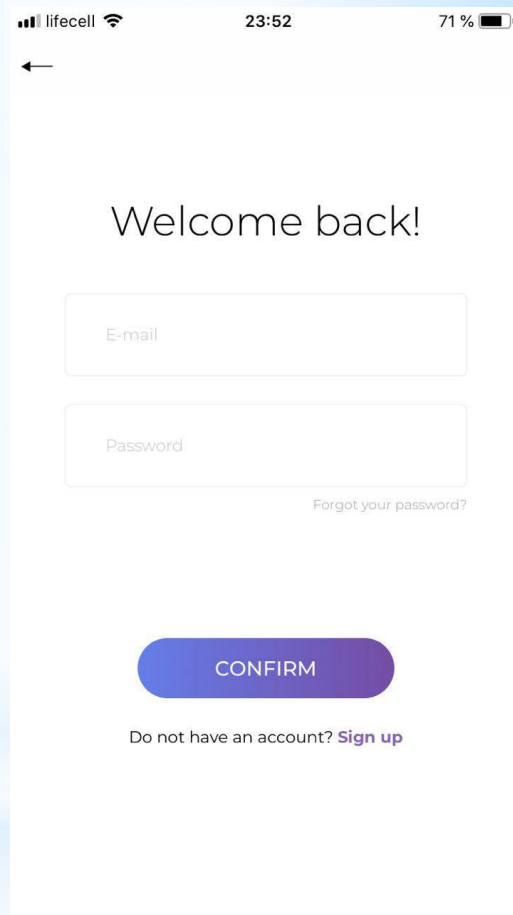
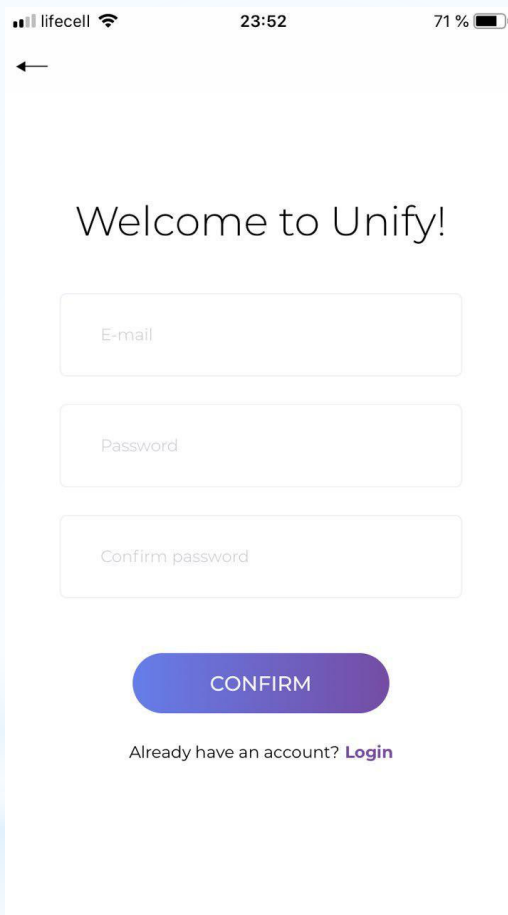
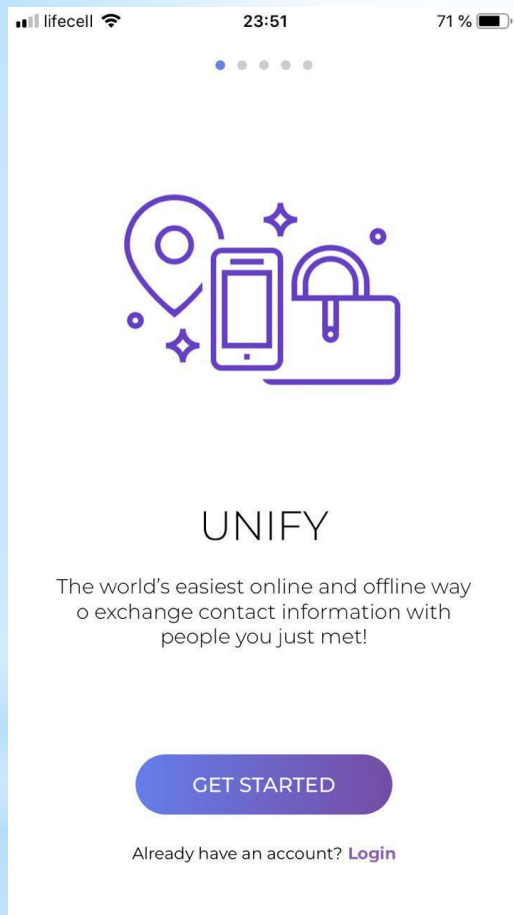
The image displays three screenshots of the Firebase Realtime Database interface, illustrating the database structure for a project named 'unif-test'.

Left Screenshot: Shows the 'unif-test' database structure. The root node is 'unif-test', which contains several child nodes: 'chats', 'chirp', 'chirp-approved', 'pending', 'qr-connect', 'qr-stack', 'reports' (with a search bar), and 'users'.

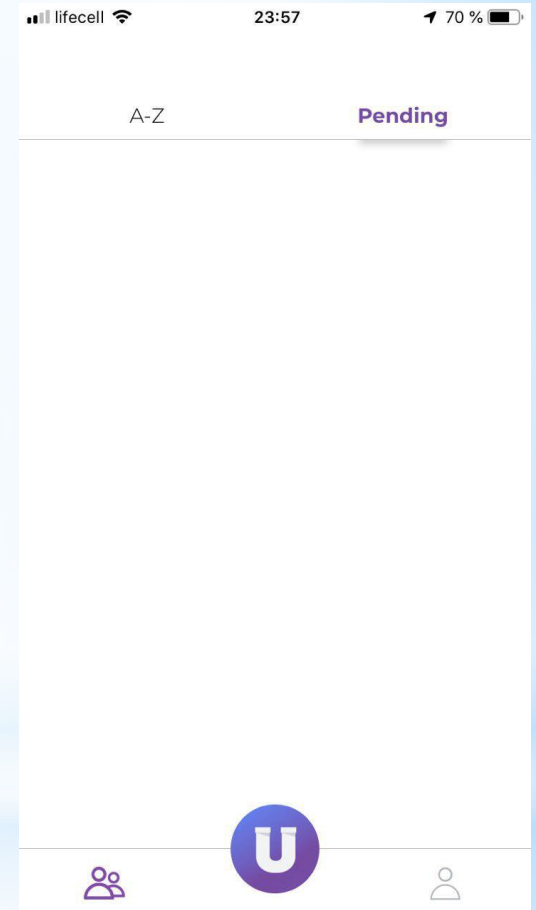
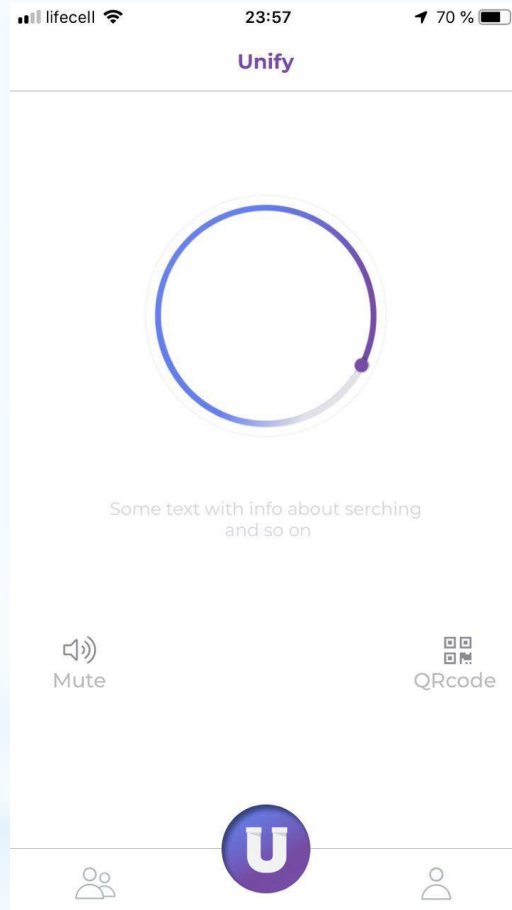
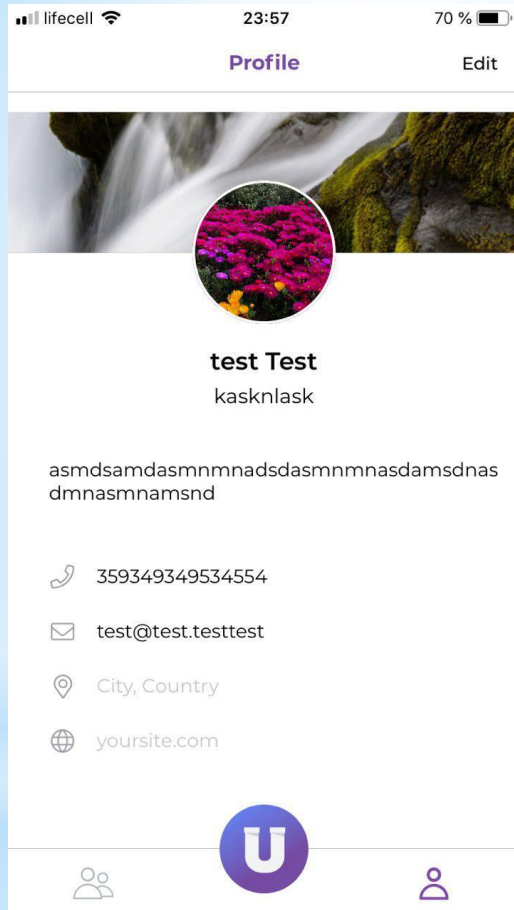
Middle Screenshot: Shows the 'Database' view for the 'unif-test' database. The root node is 'UNIF-TEST', which contains a child node 'Database'. The 'Database' node contains a child node 'VR40wmXTbbejsfEE4zNMIK0ghz22'. This node contains a child node 'data', which contains a child node 'about' (with value 'catch me, if you can'). The 'data' node also contains a child node 'photo', which contains a child node 'uid' (with value 'VR40wmXTbbejsfEE4zNMIK0ghz22').

Right Screenshot: Shows the 'Database' view for the 'unif-test' database. The root node is 'unif-test', which contains several child nodes: 'chats', 'chirp', 'chirp-approved', 'pending', 'qr-connect', 'qr-stack', 'reports', and 'users'. The 'qr-connect' node contains a child node '1536245812736', which contains a child node 'BiPS19J0y1fj94um67wG7Ud7DWy1'. The 'qr-connect' node also contains a child node 'VR40wmXTbbejsfEE4zNMIK0ghz22' (with a search bar), which contains a child node '1537347081000', which contains a child node '-LMI0rICorPLhR0g1jh2'.

Головна сторінка мобільного додатку з можливістю увійти в акаунт або зареєструвати інший



Інтерфейс користувача після авторизації



Практичне значення

Розроблений мобільний додаток обміну захищеними даними з використанням звукових сигналів.

Висновки

- Удосконалено методи обміну даними між мобільними пристроями в оффлайн режимі за допомогою алгоритму використання звукових сигналів
- Набуло подальшого розвитку застосування методів обміну даними за допомогою звукових сигналів
- Представлено гнучкий функціонал, адаптований для мобільних пристроїв на платформі iOS, з можливістю збереження результатів в оффлайн режимі

Дякую за увагу