Faculty of Electronic Engineering,
Menofia University,
CSE Department.

KidSafe

Android Parental Control App

A project submitted
in partial fulfillment of the requirements for the degree of
Bachelor of Computer Engineering.

by

Mahmoud Elsyaed Mohamed Mansour

Khaled Samir Goma Rizk

Supervised by

Dr. Marwa Abbas

7 2019

ACKNOWLEDGMENT

We would like to express our deepest appreciation to all those who provided us the possibility to complete this project. A special gratitude we give to our supervisor, Dr. Marwa Abbas, whose contribution in stimulating suggestions and encouragement, helped us to coordinate our project and inspired us to give our best. Dr. Marwa has shown a great interest and passion about the topic and it was rewarding to us.

Furthermore we would also like to acknowledge with much appreciation to all who helped and motivated us.

UNDERTAKING

This is to declare that the project entitled “KidSafe” is an original work done by undersigned, in partial fulfillment of the requirements for the degree “Bachelor of Computer Engineering” at Computer Science and Engineering Department, Faculty of Electronic Engineering, Menofia University.

All the analysis, design and system development have been accomplished by the undersigned. Moreover, this project has not been submitted to any other college or university.

Student 1

Student 2

ABSTRACT

smartphones have become essential and this could be both a good or a bad thing. If we look at the positives, having a phone keeps us connected to our friends and family. For safety reasons, it is a boon as it helps us contact people in case we are stranded somewhere or need help. The disadvantage of having a mobile phone is the fact that so many people are so involved in the digital world, that they forget to live, contribute and participate in the present. We agree that smartphones have practically placed the world at our fingertips, but maintaining a balance is essential. Children today cannot even fathom a life pre-internet a life where school work involved visits to libraries and phone calls required you to stay in one spot, since the telephone was attached to the wall. Kids spend an inordinate amount of time on their smartphones, communicating with friends (and possibly strangers) via text, Twitter and Facebook, and work to keep up their Snapstreaks on Snapchat. Even toddlers are proficient in navigating their way around a wireless tablet these days. So we thought of something to provide the parents some control over their children's phones or tablets and gain access to their activity. That's why we developed KidSafe.

Table Of Contents

1

INTRODUCTION

One in four children under the age of six has a smartphone, a survey has found. Despite parents insisting that 11 is the "ideal" age for children to have a phone, a poll found 25 per cent of children aged six and under already have their own mobile and nearly half of these are spending an average of 23 hours a week on smartphones and other gadgets - twice as much time as they spend conversing with their parents, polling suggests.

The survey of 2,000 families with children below the age of 14 found that on average they were spending 3 hours 18 minutes a day on personal devices. By contrast, they were found to be spending 1 hour 43 minutes a day engaged in conversation with members of their family. The survey found four in five parents said they had tried to persuade their children to spend less time on their personal devices. And two in five admitted to giving children devices in order to keep them occupied. Overall, children were found to be spending an average of 23 hours a week isolated on their mobiles, tablets and games consoles at home, almost double the 12 hours they spend conversing with their parents.

Two thirds of parents said they wished they had more family time. The new guidance on screen time and social media follows a review of the evidence about the impact of screen-time on children's mental health and well being. It found that heavy use of social media was associated with a doubling in depressive symptoms.
UK's four chief medical officers suggests parents should take a "precautionary approach" and not allow children to spend more than two hours at a time on smartphones and other gadgets. Prof Dame Sally Davies, England's chief medical officer, said parents should talk to their children about the content of what they are watching, and look out for changes in behavior. She also recommends that parents try using tracking features which measure how much time they and - with permission - their children spend looking at screens, or on social media.

Families are urged to have “screen-free mealtimes” with “adults giving their full attention to children” away from televisions, tablets and smartphones.

The guidance, published by the chief medical officers, also says parents should never assume a child is happy to have their photo published online and should talk to them about the fact that photographs can be manipulated.

The review found 38.1 per cent of teenage girls spending more than five hours a day on social media suffered from depressive symptoms, compared with rates of 18.1 per cent among those spending between one to three hours on such sites. Levels of depression among teenage boys rose from 6.8 per cent to 14.5 per cent, in the group spending longer on such sites.

From restricting the time they spend on the device, to keeping a close eye on what they are downloading, there are many steps parents can go through to limit usage. Other than making calls and sending messages, it also emerged that 38 per cent of children used their mobile phone to play games.

So we thought of something that can provide parents control over their children’s phones or tablets such as locking and unlocking apps or the device itself. Or set a daily screen time timer when the child exceeds it the device will be locked automatically. And to keep your children’s activity under your sight, we thought we should allow parents to get the real time location of their children. Furthermore, they should be able set a Geo-fence, which if the child exceeds, the parents should be notified. We also will allow parents to access their children’s SMS messages and phone calls.

2

PROPOSAL

The following proposal describes the basic idea of the project "KidSafe", its features, the tools used in the development, the participants and their roles.

Project Title: KidSafe – Android Parental Control

Project Type: Graduation Project

Supervisor: D. Marwa Abbas

Project Description:

Many parents believe their teens are too attached to their phones—maybe even addicted. This project aims to keep the child's activity under control by his parents. As parents will be allowed to do the following:

- Lock/Unlock the child's smartphone or tablet
- Screen time control
- App blocking
- Location tracking
- Geo-Fencing
- View the child's activity (SMS messages and phone calls)

Project Tools:

All the tools used in the development of KidSafe are free and some of them are open source. That's why we wanted to contribute back to this awesome community by making KidSafe free and open source under the MIT License.

1. Programming Language: Java
2. Back End: Google's Firebase
3. Front End: HTML, CSS and JavaScript
4. IDE: Android studio and Visual studio code
5. Graphics: InkScape and GIMP

Participants

1. Mahmoud Mansour – Mobile App Developer
2. Khaled Samir – Mobile App Developer

Project Development Life Cycle:

Visit this trello board to check the progress of the project.
https://trello.com/b/23AGFhoj/kidsafe-android-parental-control

Project Source Code:

Visit this github repository for the source code of the project.
https://github.com/xMansour/KidSafe

3

WHAT IS KIDSAFE?

KidSafe is an android parental control app which when installed on the child's device and linked with his parent's, will provide the parents remote access to that device, giving them the ability to control, block or manage certain features that can ensure your child's safety and digital well being.

Why should parents use KidSafe?

Parents whose children are spending a lot of time on their smartphones or tablets should use KidSafe to control their children screen time or activity. KidSafe makes it easy to set the boundaries for your child. You can manage their screen time, find out the installed applications, block addictive applications, locate them on real time or set a Geo-fence on them. You can also access their SMS messages or phone calls.

KidSafe's Features:

1. Lock/Unlock the child's device
2. Screen time control
3. App blocking
4. Tracking location
5. Geo-Fencing
6. View their activity (SMS and Phone calls)

KidSafe is free and open source under MIT license. A copy of the license is attached in the next page.

MIT License

4

FEATURES IN DETAILS

In the following section we will introduce all the features of KidSafe and how they can help the parents keep the children's activity under their sight and remotely control their devices.

Locking and Unlocking the child's smartphone or tablet

KidSafe allows the parents to lock and unlock their children's smartphones or tablets remotely.

Screen time control

With screen time control, parents can set a daily usage period of time.
If the child exceeded this period, the phone or the tablet locks automatically until the next day.

App blocking

If your child is kinda addictive to an app or a game, KidSafe allows you to lock and unlock his installed apps with your fingertips. Once you check the switch, if he is online the app will be locked immediately. If he is not online, once he get connected to internet changes will apply.

It is really useful if you want to block app usage during study or sleep time.

Tracking location

With KidSafe's real time location tracking, you can track your child's location in real time as long as he is connected to the internet. If he is not connected, you will see the most recently location he was at when he was last connected to the internet.

Geo-Fencing

KidSafe allows the parents to set a Geo-fence around their children's current location or the parent's.
Once the fence is active, the parent will be alerted when the child exceeds the limits of that fence.

View their activity

With KidSafe, parents will be able to access their children's SMS messages and phone calls data. Once the child receives a SMS or a phone call it will be forwarded to the parent.

The parent will be able to see the sender/receiver phone number, message body, and sending/receiving time if it is a SMS message.

If it is a phone call, the parent will be able to see the call type (outgoing or incoming), caller or called phone number, contact name if the number is saved in your child's contacts, the duration of the call, and the time when this call was received or made by the child.

5

WHY GOOGLE's FIREBASE?

Google's firebase is a free **back end as a service** (**BaaS**) meaning there is no server infrastructure needed. This shortens development time and removes a layer of complexity for developers. The best thing about BaaS, though, is that it frees developers from the tedium of building out a backend. Instead, they can direct all of their focus to creating dynamic, user-oriented apps.

One of the Firebase's biggest draws is its **robust**, **well-tested** feature set. It has tools for nearly everything a developer could need. Some, like Google analytics, are built in free. Other can be incorporated as needed, such as:

1. Real-time NoSQL database
2. Authentication
3. Hosting
4. Push notifications
5. Real-time messaging
6. Cloud storage
7. Performance monitoring
8. Machine learning kit
9. And many other features

KidSafe uses Google's firebase as a back end. We use firebase's real time database, firebase's Authentication and firebase's storage. We shall take about them in the following section.

Firebase's NoSQL Real-time database

KidSafe store and sync data with firebase's NoSQL cloud database. Data is synced across all clients in realtime, and remains available when KidSafe goes offline.

The Firebase Realtime Database is a cloud-hosted database. Data is stored as JSON and synchronized in realtime to every connected client. All the clients share one Realtime Database instance and automatically receive updates with the newest data.

Key capabilities

Real-time: Instead of typical HTTP requests, the Firebase Realtime Database uses data synchronization—every time data changes, any connected device receives that update within milliseconds. Provide collaborative and immersive experiences without thinking about networking code.

Offline: Firebase apps remain responsive even when offline because the Firebase Realtime Database SDK persists your data to disk. Once connectivity is reestablished, the client device receives any changes it missed, synchronizing it with the current server state.

Accessable from client devices: The Firebase Realtime Database can be accessed directly from a mobile device or web browser; there's no need for an application server. Security and data validation are available through the Firebase Realtime Database Security Rules, expression-based rules that are executed when data is read or written.

Scale across multiple databases: With Firebase Realtime Database on the Blaze pricing plan, you can support your app's data needs at scale by splitting your data across multiple database instances in the same Firebase project. Streamline authentication with Firebase Authentication on your project and authenticate users across your database instances. Control access to the data in each database with custom Firebase Realtime Database Rules for each database instance.

How does it work?

The Firebase Realtime Database lets you build rich, collaborative applications by allowing secure access to the database directly from client-side code. Data is persisted locally, and even while offline, realtime events continue to fire, giving the end user a responsive experience. When the device regains connection, the Realtime Database synchronizes the local data changes with the remote updates that occurred while the client was offline, merging any conflicts automatically.

The Realtime Database provides a flexible, expression-based rules language, called Firebase Realtime Database Security Rules, to define how your data should be structured and when data can be read from or written to. When integrated with Firebase Authentication, developers can define who has access to what data, and how they can access it.

The Realtime Database is a NoSQL database and as such has different optimizations and functionality compared to a relational database. The Realtime Database API is designed to only allow operations that can be executed quickly. This enables you to build a great realtime experience that can serve millions of users without compromising on responsiveness. Because of this, it is important to think about how users need to access your data and then structure it accordingly.

Firebase's Authentication

Most apps need to know the identity of a user. Knowing a user's identity allows an app to securely save user data in the cloud and provide the same personalized experience across all of the user's devices.

Firebase Authentication provides backend services, easy-to-use SDKs, and ready-made UI libraries to authenticate users to your app. It supports authentication using passwords, phone numbers, popular federated identity providers like Google, Facebook and Twitter, and more.

Firebase Authentication integrates tightly with other Firebase services, and it leverages industry standards like OAuth 2.0 and OpenID Connect, so it can be easily integrated with your custom backend.

Authentication Methodologies

Email and password based authentication: Authenticate users with their email addresses and passwords. The Firebase Authentication SDK provides methods to create and manage users that use their email addresses and passwords to sign in. Firebase Authentication also handles sending password reset emails.

Federated identity provider integration: Authenticate users by integrating with federated identity providers. The Firebase Authentication SDK provides methods that allow users to sign in with their Google, Facebook, Twitter, and GitHub accounts.

Phone number authentication: Authenticate users by sending SMS messages to their phones.

There are a lot of ways in which a user can authenticate using firebase authentication. This makes it easy-to-use for the user. However KidSafe allows both email and password and google authentication.

How does it work?

To sign a user into your app, you first get authentication credentials from the user. These credentials can be the user's email address and password, or an OAuth token from a federated identity provider. Then, you pass these credentials to the Firebase Authentication SDK. Our backend services will then verify those credentials and return a response to the client.

After a successful sign in, you can access the user's basic profile information, and you can control the user's access to data stored in other Firebase products. You can also use the provided authentication token to verify the identity of users in your own backend services.

Firebase's Cloud Storage

Cloud Storage is built for app developers who need to store and serve user-generated content, such as photos or videos.

Cloud Storage for Firebase is a powerful, simple, and cost-effective object storage service built for Google scale. The Firebase SDKs for Cloud Storage add Google security to file uploads and downloads for your Firebase apps, regardless of network quality. You can use our SDKs to store images, audio, video, or other user-generated content. On the server, you can use Google Cloud Storage, to access the same files.

KidSafe uses cloud storage to upload the profile images of each authenticated user.

Key capabilities

Robust operations: Firebase SDKs for Cloud Storage perform uploads and downloads regardless of network quality. Uploads and downloads are robust, meaning they restart where they stopped, saving your users time and bandwidth.

Strong security: Firebase SDKs for Cloud Storage integrate with Firebase Authentication to provide simple and intuitive authentication for developers. You can use our declarative security model to allow access based on filename, size, content type, and other metadata.

High scalability: Cloud Storage for Firebase is built for exabyte scale when your app goes viral. Effortlessly grow from prototype to production using the same infrastructure that powers Spotify and Google Photos.

How does it work?

Developers use the Firebase SDKs for Cloud Storage to upload and download files directly from clients. If the network connection is poor, the client is able to retry the operation right where it left off, saving your users time and bandwidth.

Cloud Storage stores your files in a Google Cloud Storage bucket, making them accessible through both Firebase and Google Cloud. This allows you the flexibility to upload and download files from mobile clients via the Firebase SDKs, and do server-side processing such as image filtering or video transcoding using Google Cloud Platform. Cloud Storage scales automatically, meaning that there's no need to migrate to any other provider. Learn more about all the benefits of our integration with Google Cloud Platform.

The Firebase SDKs for Cloud Storage integrate seamlessly with Firebase Authentication to identify users, and we provide a declarative security language that lets you set access controls on individual files or groups of files, so you can make files as public or private as you want.