0.1 Common Technologies

0.1.1 Google Cloud Messaging

0.1.1.1 Design Overview For our system we intend to utilize push notifications as the main way of initialising contact between our server and the users phone. As our system is initially being developed for the Android platform, we are going to implement the Google Cloud Messaging (GCM) [10] system as the main method of sending and receiving these notifications.

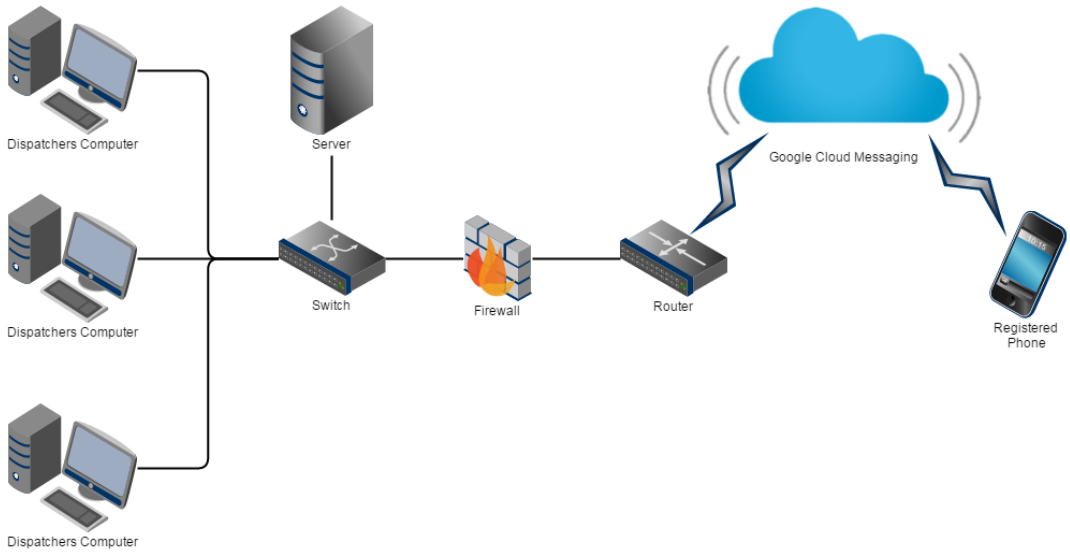

Figure 1: Network map of how our system will communicate between devices and the server

We have chosen to use this system for a few reasons. Firstly as our app is initially being developed for Android (due to current limitations with IOS) so using GCM is advisable as it is heavily embedded with the operating system and so reduces strain (such as power usage) [11]. GCM also allows the notifications to be received when the app is not running which is of huge benefit to the user who then does not have to keep the app open to offer their help. Other notable reasons include that it is free to use, can handle large scale push notifications [11], notifications can be canceled at a later time using a collapse key and that you can send data (up to 4096 bytes) as a payload to be used by the app. GCM can also be integrated with ISO push notifications [13] which could be useful if, in the future, an IOS app was being developed.

As a result of deciding to use GCM, we need to keep a database of the registered app users. This is because GCM uses a registration ID system to send a message to a specific phone, we need to store and relate this ID to a user of our system.

0.1.1.2 GCM Setup We intend to use GCM primarily for its ability to push notifications to a clients device. There are several things which we need to have set up before the notifications

can be sent. Firstly, each phone will have a unique key associated with it which is used to identify an individual's phone so messages can be sent to it. This is obtained by the app when it registers with the GCM service. In order for our server to send messages to this device we need to know and store this registration ID, therefore the device will need to send it to our server to be stored in a secure database. The detailed setup instructions are available directly from google and have example code to assist in the setup [14].

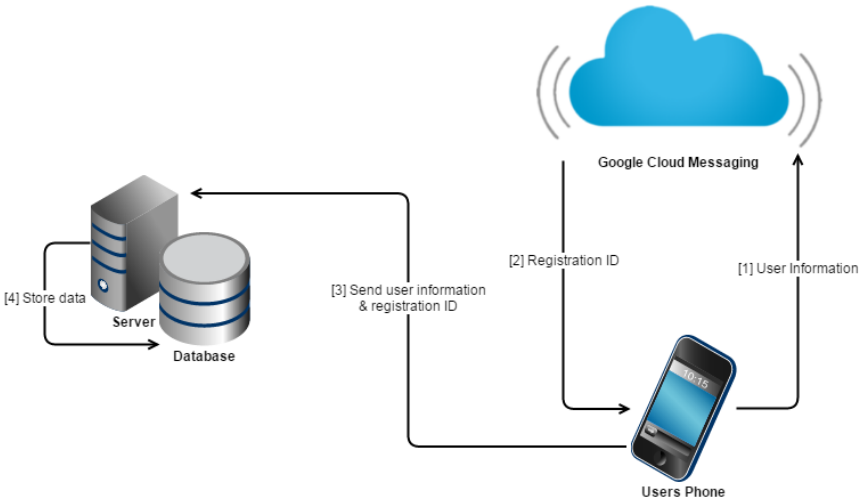

Figure 2: Diagram of the initial setup and registration with Google Cloud Messaging

We will also have to setup the database to store the information of the user that the phone is registered to along with the Registration ID (token) obtained from GCM. This design is detailed in the database section.

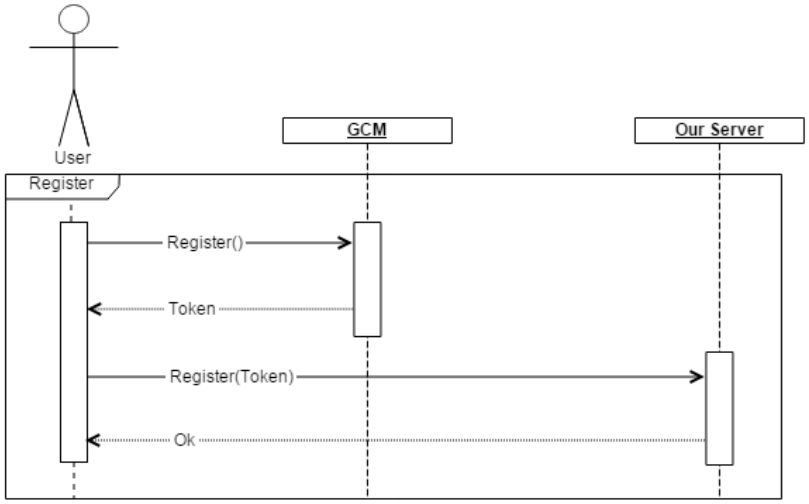

Figure 3: Sequence diagram showing interactions when registering a device

0.1.1.3 Sending Downstream Messages Once the initial setup is completed we can focus more on the message sending and receiving parts of the application. In order to push a notification to our users phone our server needs to send a request containing the registration ID and the message to Googles Messaging Server which then sends it directly to the device associated with that ID.

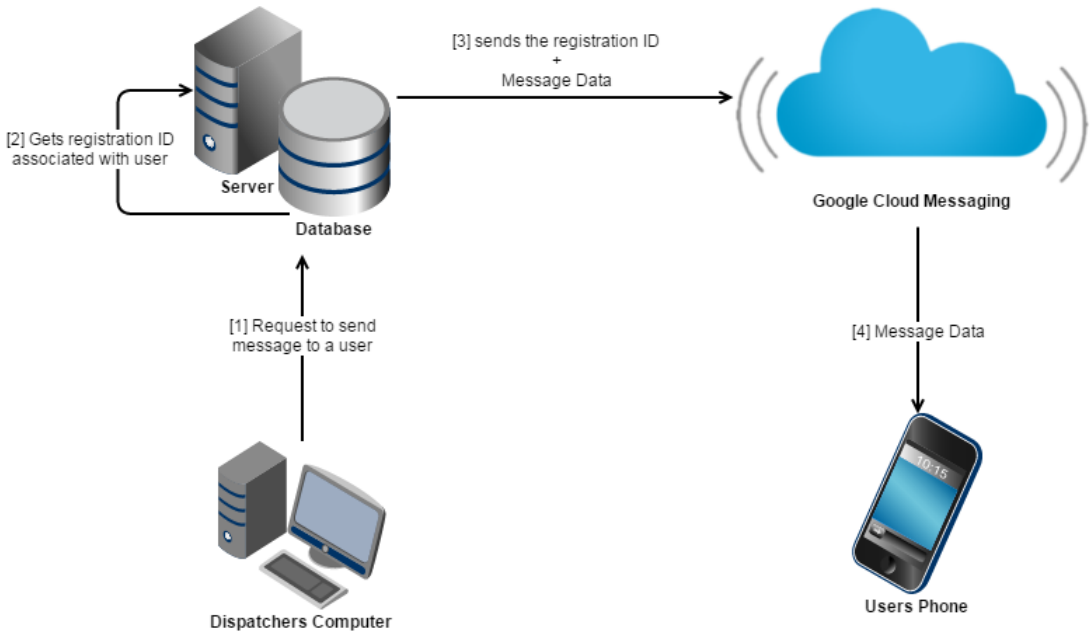

Figure 4: Diagram illustrating sending of a message to a clients device

We have decided to use the XMPP protocol as the connection between our server and GCMs server. This was chosen (over HTTP) for a few reasons. Firstly, the XMPP protocol is faster than HTTP and so would allow the system to send messages to users quickly which is a crucial aspect of any emergency system. It also uses the existing GCM connection on the device to receive the data, saving battery useage as you don't have to open your own connection to the server. XMPP does not however allow broadcast messages to be sent to multiple devices, instead you have to send a new message for each device you wish to contact. This should not present a problem in our system as we will only need to send a message to one device (in this iteration) and even if a later iteration was to require sending to multiple devices, it would be a small number.

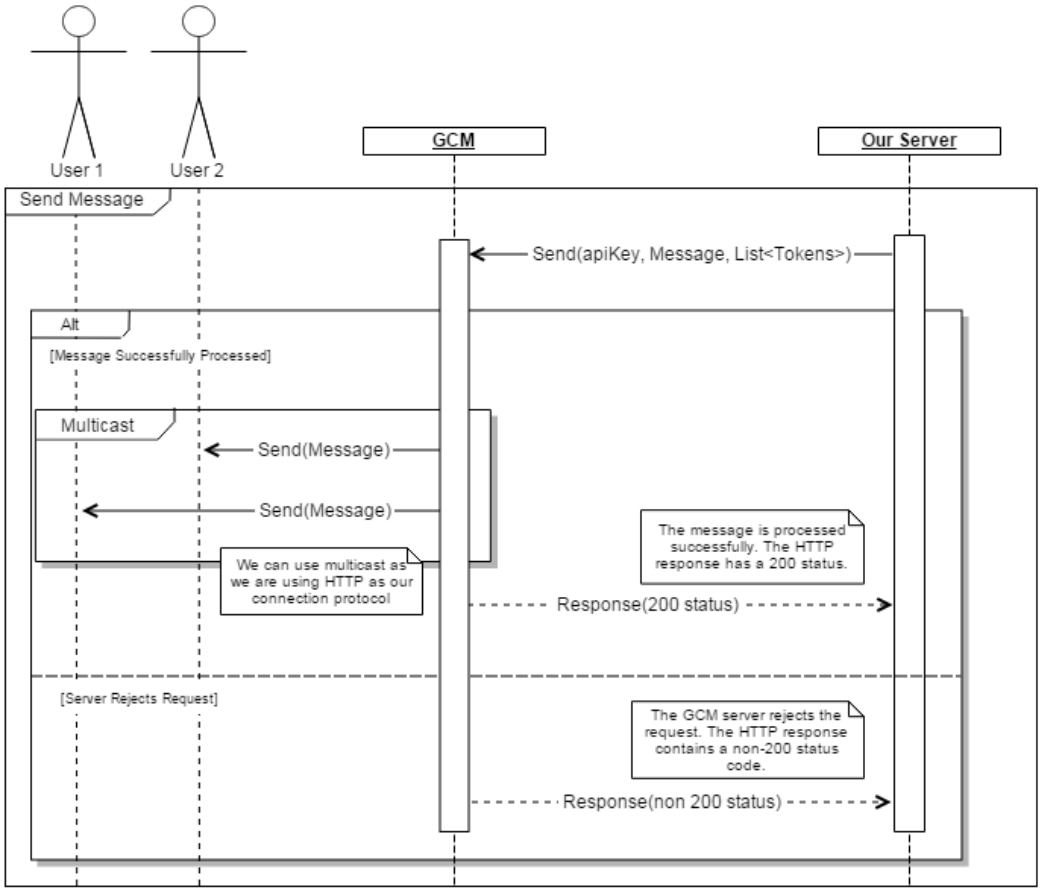

Figure 5: Sequence diagram showing the interactions when sending a message to the client device

Once a XMPP connection is established our server can use normal XMPP ¡message¿ stanzas to send a JSON-encoded message. For this iteration our message will contain five components, the registration ID of the device we are sending the message to, a message ID to uniquely identify this message, a collapse key we can use to overwrite the message later, a time-to-live after which the message with expire and not be sent, and the payload data we wish to send. The format of the message will look like this :

```
<message id="">
  <gcm xmlns="google:mobile:data">
  {
      "to":"REGISTRATION_ID",
      "message_id":"UNIQUE_MESSAGE_ID",
      "collapse_key":"UNIQUE_COLLAPSE_KEY"
      "time_to_live":"TIME_IN_SECONDS",
      "data":
      {
          "KEY":"VALUE",
```

```
    }
  }
  </gcm>
</message>
```

For each device message your app server receives from GCM, it needs to send an ACK message. If you don't send an ACK for a message, GCM will just resend it. GCM also sends an ACK or NACK for each message sent to the server. If you do not receive either, it means that the TCP connection was closed in the middle of the operation and your server needs to resend the messages[10].

These response messages will need to be dealt with according to their responses. The ACK will be sent if the message was successfully delivered however there are two types of error messages (NACK and Stanza error) for situations such as Invalid JSON, bad registration ID or Device Message Rate Exceeded. Each of these messages contains an error ID and message which informs you of what the problem is so that it can be dealt with [15].

In some situations, we will include a payload of data that will be sent (in the message) to the clients device. This payload is easily incorporated into the message and forms part of the JSON-encoded message string. This payload data has no limit to the number of key-value pairs however there is a total limit of 4kb maximum message size. String values are recommended to all other data types would need to be converted to strings before sending them to the device [15].

0.1.1.4 Sending Upstream Messages We can also use GCM to send upstream messages from the clients device to the server via Googles CCM (Cloud Connection Service). This works by embedding the servers registration ID (obtained when registering for the GCM service) into the clients software and passing this ID along with a message to the GCM service to be forwarded to the server.

Figure 6: Diagram showing the sending of a message from the client device to the server

This will once again use the XMPP protocol for the reasons stated in Sending Downstream Messages and then we can use normal XMPP ¡message¿ stanzas to send a JSON-encoded message in the following format[25] :

```
<message id="">
  <gcm xmlns="google:mobile:data">
  {
      "category":"com.example.yourapp", // to know which app sent it
```

```
      "data":
      {
          "KEY":"VALUE"
      },
      "message_id":"UNIQUE_MESSAGE_ID",
      "from":"DEVICE_REGISTRATION_ID"
  }
  </gcm>
</message>
```

This message is then forwarded by GCM to our server and the message is parsed for its data. The device uses the send() method from the GCM API to construct and send the message. This takes the following format:

```
gcm.send(GCM_SENDER_ID + "@gcm.googleapis.com", id, ttl, data);
```

Where `GCM_SENDER_ID` is the stored GCM ID number of the server, id is the unique message ID, ttl is the time to live of the message (seconds) after which the message will expire and not be sent and finally the data to be sent [25]. This will produce a stanza in the format described above and send it to the server ID specified.

After the message is received from CSS by our server we are expected to send an ACK message back to google. This should be in the following format [25]:

```
<message id="">
  <gcm xmlns="google:mobile:data">
  {
      "to":"DEVICE_REGISTRATION_ID",
      "message_id":"MESSAGE_ID_OF_RECIEVED_MESSAGE"
      "message_type":"ack"
  }
  </gcm>
</message>
```

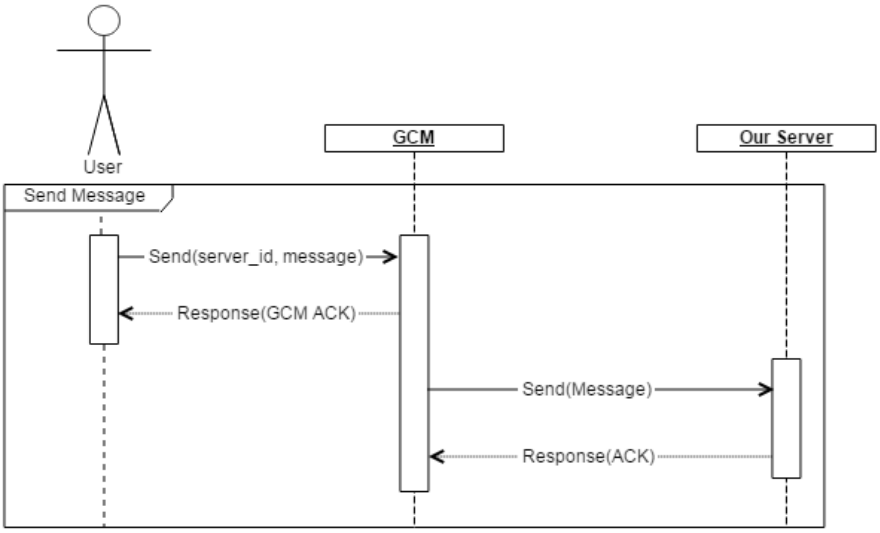

Figure 7: Sequence diagram showing the interactions when sending a message to the server from a client device

0.1.2 Database

It was immediately apparent that both the Emergency App and CPR System would need a database backend. To ensure we chose the best system, we investigated the three most prolific database management systems (DBMSs): MySQL, Oracle, and SQL Server.

Almost immediately, we discounted MySQL as being immature compared to Oracle and SQL Server. Transactions and stored procedures are a relatively recent addition to the system, and both are technologies that we will rely on heavily to ensure data is consistent and intact. It also has far fewer features relevant in enterprise environments, lacking fine-grained access control, table partitioning and disaster recovery.

Next, we scrutinised the remaining contenders. Ultimately, there isnt a lot of difference between them; SQL Server has a marginal advantage with in-memory tables and better performance in write-intensive environments, while Oracle is supposedly more suited to applications with equal read and write traffic due to its locking system.

In the end, we decided to go for SQL Server due to its Spatial Data extensions, which would be used particularly heavily in the CPR System. This functionality allows us to do accurate geometric calculations, like finding the distance between two sets of coordinates, within the database itself. In addition, SQL Server is renowned for its stability, with a transaction and journaling system that detects and automatically fixes errors, preventing corruption and increasing uptime - all of which are desirable traits in such life-critical applications.