Availability and Reliability Analysis

* Propagate warnings within 6 hours: when a case is reported, it takes 5 hops to go back and forth between user applications and servers to update all the people in the cone
  + Create new servers to allow parallel notifications in the cone
  + Bottleneck in time: time taken for users to grant permission is unforeseeable: user not responding to the system, user not giving permission to use the local storage, user, loss of internet of users for a while
* Lack of Internet connections:
  + - Solution: interaction data is stored on local storage with a cloud backup every regular time intervals, ensuring the lack of Internet won’t cause loss in interaction data.
* 99.99% successful delivery rate: (failure scenarios for medical cases)
  + User not denying permission for sending interaction data to server, cut off the whole branch in the cone
  + Notification of delivery is down due to Internet connection failure/application failure
    - Solution: set up TCP; acknowledgement is required, resend the data if lost
  + User application lost interaction data
    - Solution: cloud to back up

Timeline analysis

* Technology, implementation and execution risk: (???)
* Testing and deployment:
  + technical teams: user application, medical staff application, server, db set-up, CNDS aspects
  + testing: in-house testing 🡪 testing in rural areas and metropolitan area 🡪 launching
* Scaling: (???)

Software/hardware development: building applications, servers and db set-up

1

2

3

4

5

6

7

8

DB and server scaling

CNDS implementation:

Set up TCP/IP

In house testing; target user: 1k

Secondary testing: specific areas

Target user: 100k

Stress testing:

Peak reported/confirmed cases

Privacy and Security Analysis – privacy-functionality-security trade off (innovative approach desired)

* Privacy: minimise data retention
  + Solution: data stored on local storage and only allowed to upload to server and database upon permission by users when the user has suspected/confirmed the infections
  + Solution: data on local storage automatically deleted after 14 days; only backed up data less than 4 days old
* Misreported cases due to malicious actors
  + Suggested: confidence score in the source, every user is given a confidence score (presumably fully trustworthy): for every self-reported case, give a wait-time, after the time-out and it’s not being confirmed by medical staff, change to green status; deduct the person’s confidence score; give people warning in the notification when confidence score is too low

Scale(50-80% penetration of UK mobiles)

Self-reporting:

* Average: 5k to 10k per day
* Peak: 500k
* During outbreaks the geographically distribution of self-reports is likely to vary significantly with the number of correct self-diagnoses accompanied by many incorrect self-assessments due to the known outbreak. (???)

Medical reporting:

* Average: 200k tests
* Peak: 500k tests
* Worst peak confirmed cases: 50k
  + To improve the notification latency; positive cases will be prioritised; update negative cases during non-peak hours; i.e. midnight

Highlighted: not yet resolved