Requirements and Design Specification(uWatch digital forensic tool)

Group Name: MPHETamines

Version: 1.2

Taariq Ghoord	10132806
Martha Mohlala	10353403
Phethile Mkhabela	12097561
Sboniso Masilela	10416260
Harrison Maphuti Setati	12310043

Git repository link:
`https://github.com/MPHETamines/MPHETamines/`

October 1, 2015

Contents

1 Introduction

This document sets out the Software Requirements Specification and Technology Neutral Process Design for the COS 301 group project entitled *Online Neighbourhood Watch(ONW aka uWatch)*. The aim for this project is to follow agile software development approach within which the application functionality is developed iteratively. The information provided in this document is presented in such a way as to provide precise and testable requirements. The emphasis is on performing an upfront software architecture engineering for iterative stimulation of the detailed requirements for a use case so that each use case can be built, tested and deployed before the detailed requirements for the next case are added.

1.1 Project Background

Crime is a prominent issue in South Africa as it is all over the world, Many criminal activities go unresolved or even attended to due to the lack of evidence or concrete witnesses. Mobile applications have become increasingly popular all over the world and are used in our everyday and work life for common things such as checking the weather; maps for directions and news feed updates. Digital forensic science hopes to utilise this increasing growth in the use of mobile applications to address the lack of evidence to crime cases in South Africa.

The application is referred to as Online Neighbourhood Watch(ONW) accessible via mobile devices and computers over the internet. The two main users of the ONW model are the uploader (user of the mobile device) and the forensic investigator or law enforcement agent. This tool is to be used by the citizens of South Africa to capture, collect and store potential evidence which can later be viewed and analysed by the Police department and used in the prosecution and detention of criminals.

1.2 Project Purpose

The Online Neighbourhood Watch is aimed to provide a tool that can assist the South African Police Services(SAPS) reduce crime by enabling the members of the community to be part of the judicial system. The ONW application captures and stores potential digital evidence of criminal activities which will then be accessed by law enforcement agents and digital forensic investigators. The goal is to enhance the successful rate of trials and secure a higher number of convictions.
The application can be used in various scenarios, basically it should be used

in any setting where a community member feels like a crime has been committed, it is then up to the ONW model to decide if the uploaded data is a potential crime scene. The application should enable a user to capture digital evidence such as digital photographs, audio and video of a potential crime scene in the domain of the ONW to maintain integrity of the data, the data is then stored into the ONW repository.

1.3 Project Scope

The scope of the ONW is focused on capturing three media types(image,video and audio).Users will capture and upload images,videos and audio as potential digital evidence(PDE). There are two aspects of the system the mobile application side, utilised by South African community members; the desktop side where a law enforcement agent logs in. The PDE is categorised by using tags with drop-down describing the kind of the crimes.Our project has these categories: murder,rape,violence,robbery,drugs and other(relevant crimes). The PDE is tagged with geo-location and time-stamp(that is for making the searching of evidence easier on the law enforcement side) and uploaded to the SAPS server.

1.4 Project Assumptions

The ONW will be tested around Pretoria Hatfield with the local SAPS precinct. If it passes the test then it will be progressed to other cities in Gauteng, eventually to the whole South Africa.

2 Methodology

We will be following agile approach when conducting our project.This incremental approach allows us to test each of the small components of the system independently. Changes in the requirements may be made in this approach so maybe our limitations changing in the implementation phase will not be a problem.

3 Application requirements and design

This section discusses for each module of the uWatch Digital Forensic Tool,the functional requirements as well as the process designs for the use cases.

3.1 ONW Application Module

The Application module will provide services to capture PDE, that is capture images, record videos and record audio to serve as a potential evidence. The user will be notified when an evidence(PDE) is successfully uploaded to the law enforcement server.

3.1.1 CapturePDE-Priority:critical

Service Contract
post-condition: The PDE is captured and added to the database.
Functional Requirement
A user should be able to capture media in any situation they feel that a crime has been committed.

3.1.2 UploadPDE-Priority:critical

Service Contract
pre-condition: The valid PDE was captured.
post-condition: The PDE is encrypted.

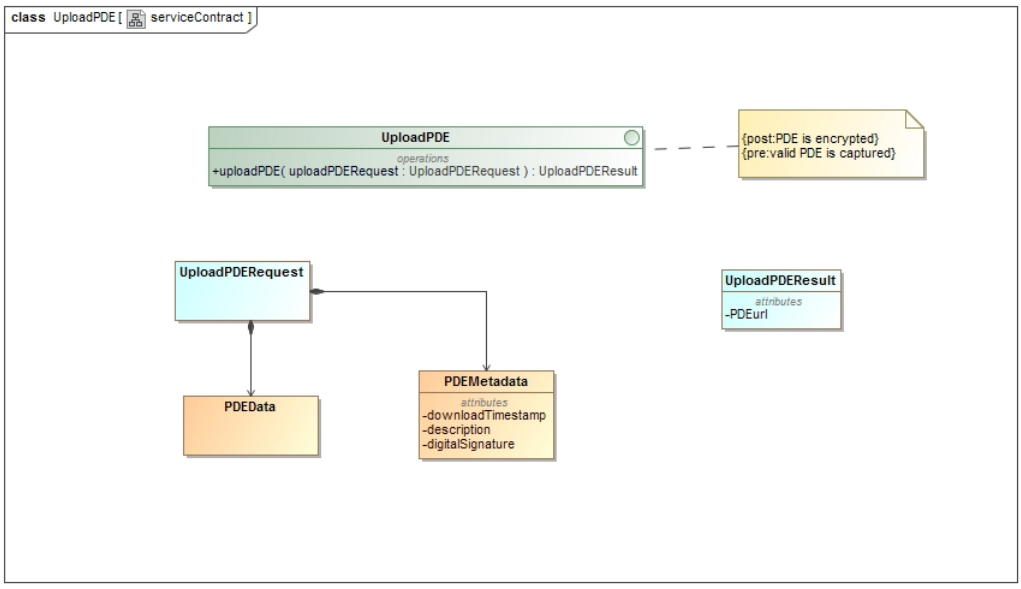

Figure 1: Service Contract: Uploading Potential Digital Evidence

Functional Requirement

A user needs to be able to upload a picture, video or audio whenever and wherever the user is.

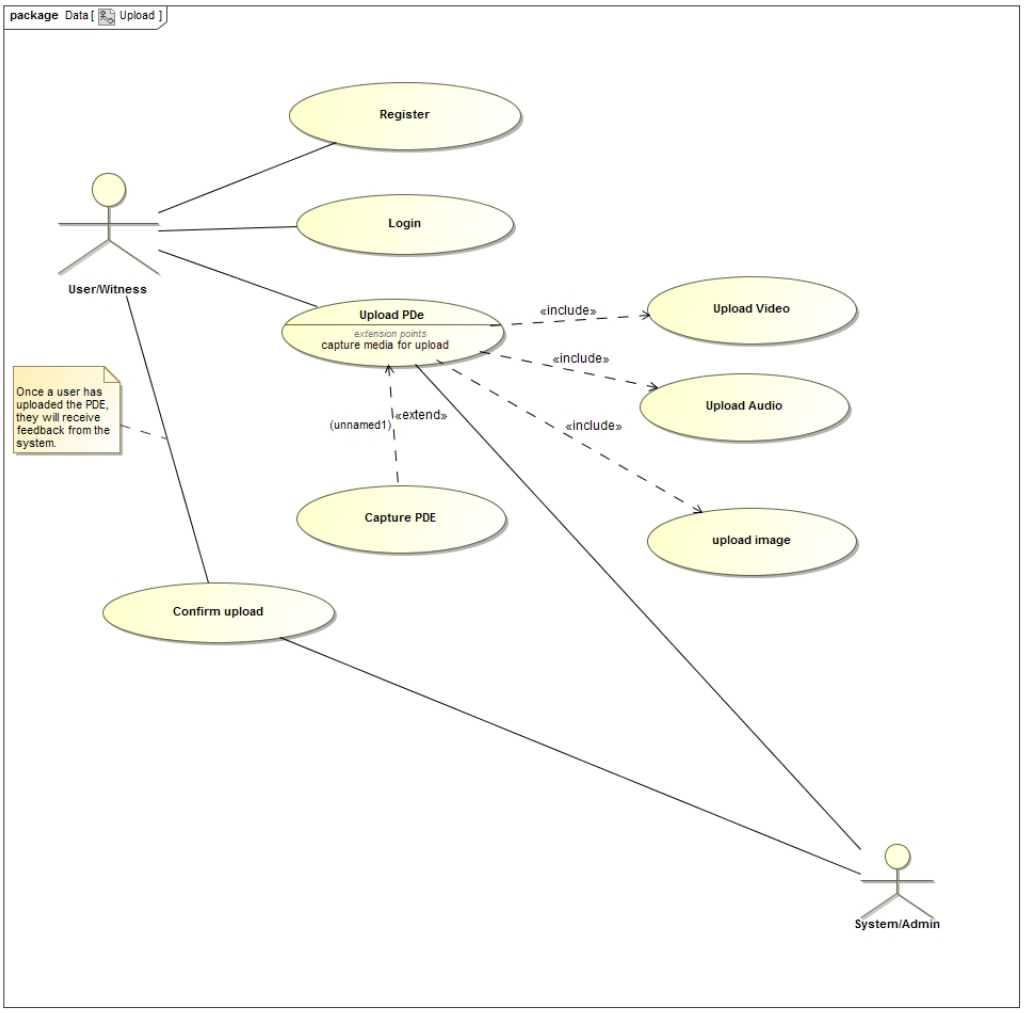

Figure 2: Functional Requirements: Uploading Potential Digital Evidence

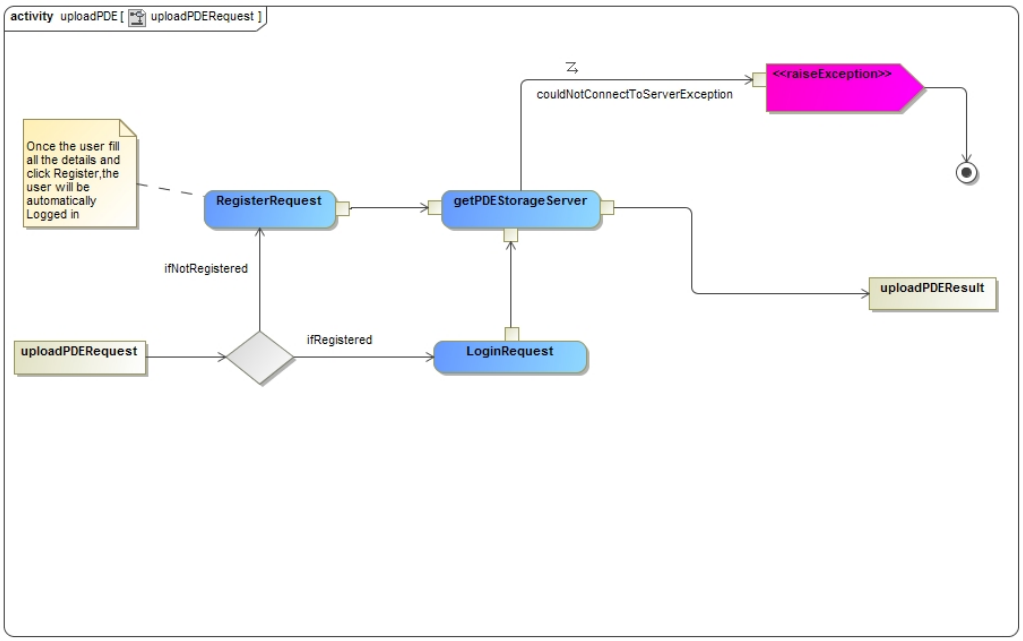

Figure 3: Process Specification: Uploading Potential Digital Evidence

3.1.3 ConfirmPDE-Priority:important

Service Contract
pre-condition: The user must have uploaded something to be confirmed.
post-condition: The user gets a confirmation from the system.
Functional Requirement
The user waits to receive a confirmation from the system telling them if their PDE was accepted or rejected.

3.2 The Administration Module

The functionality provided by the Administration module includes the following:

- It manages access to the web based systems of the model
- It provides means to download the potential digital evidence
- It provides functionality to validate the evidence, whether by location, date and time or digital signature
- It provides encryption and decrypt functionality

3.2.1 DownloadPDE-Priority:critical

Service Contract
pre-condition: For any media to be downloaded, the media must be in the database.
post-condition: The PDE must be persistent
post-condition: The PDE is received

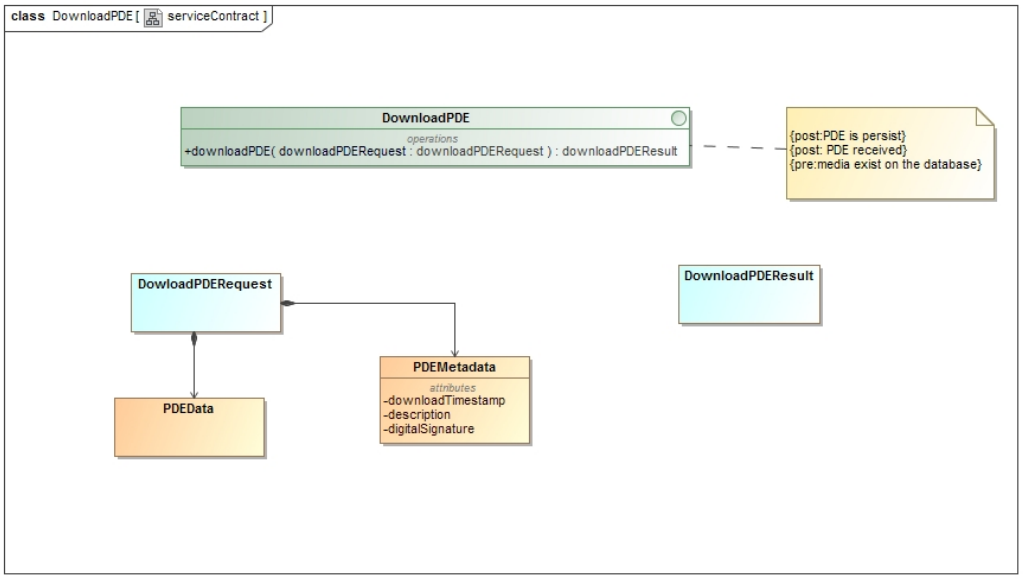

Figure 4: Service Contract: Downloading Potential Digital Evidence

Functional Requirement
The law enforcement agent needs to download the PDE to use it in the court of law.

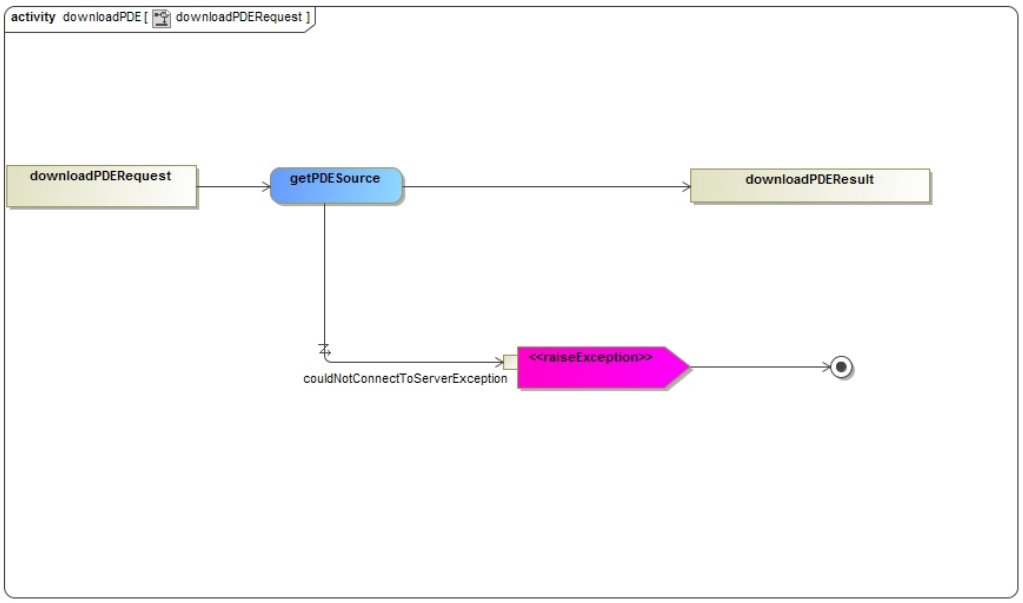

Figure 5: Process Specification: Downloading Potential Digital Evidence

3.2.2 ValidatePDE-Priority:critical

Service Contract
post-condition: The PDE should be checked if it conforms to the standard set for valid evidence
pre-condition: There has to be data to be validated
Functional Requirement
The system needs to validate that the data to ensure it's integrity.

3.2.3 EncryptPDE-Priority:critical

Service Contract
post-condition: The PDE should be encrypted.
Functional Requirement
The system encrypts the PDE for it to be stored in the database.

3.2.4 DecryptPDE-Priority:critical

Service Contract
post-condition: The PDE should be decrypted before it is used in the court of law.

Functional Requirement
The system decrypts the PDE for it to be viewed in the court of law.

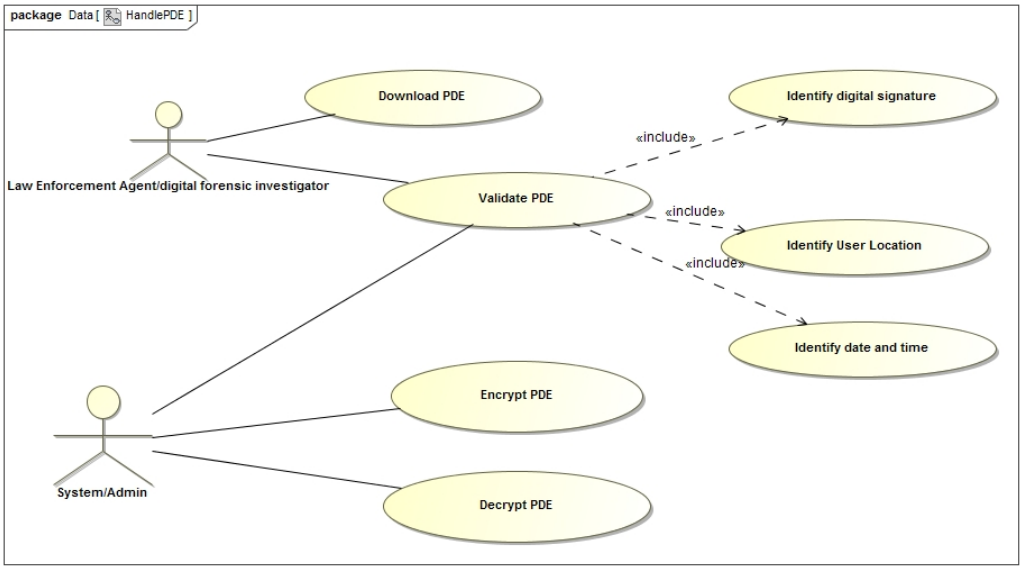

Figure 6: Functional Requirements: Validate,encrypt and decrypt PDE

3.2.5 ManageAccessAllocation-Priority:critical

Service Contract
post-condition: No unauthorised user can log in to the system.
Functional Requirement
The system is suppose to manage who has access to the system, this is a form of security measure. If the user is not authorized, he/she will be given an option to register new account.

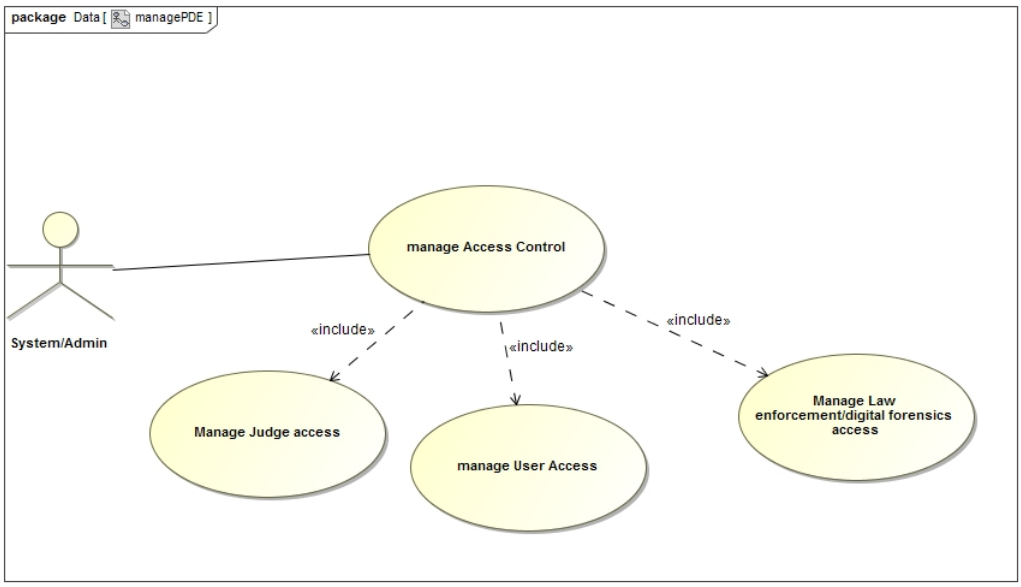

Figure 7: Functional Requirements: Manage Access Allocation

3.3 Login and Administrative user

The system provides a functionality to register new users or to log on already registered users. The system will be running on a remote server and user details are stored in a relation database.
The Login module provides services to log in. Once a user is logged in, the user can view all the files he/she has uploaded to the server without being able to download them.

Administrators on the other end, will also be requested to log in to the system before they could view, download or audit data files send to the server.

3.3.1 Login-Priority:critical

Service Contract
pre-condition: law enforcement agent and jury with provided credentials can login.
pre-condition: Could connect to the SAPS database.
post-condition: UserID on results is populated by user's ID.

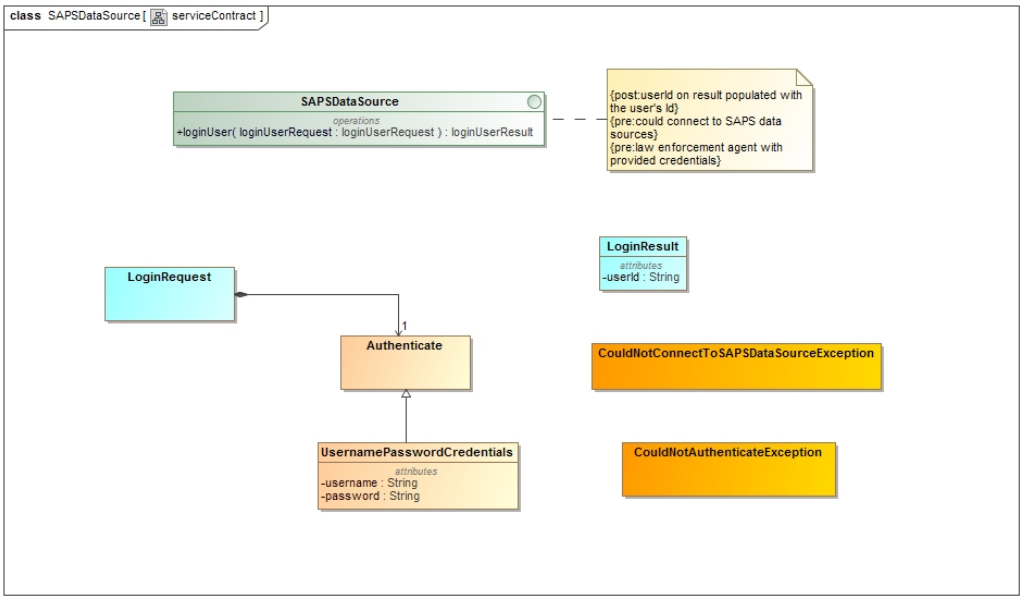

Figure 8: Service Contract: Login for law enforcement and jury

Functional Requirement
The law enforcement agent should be able to log in to the system to search, view and download the PDE.

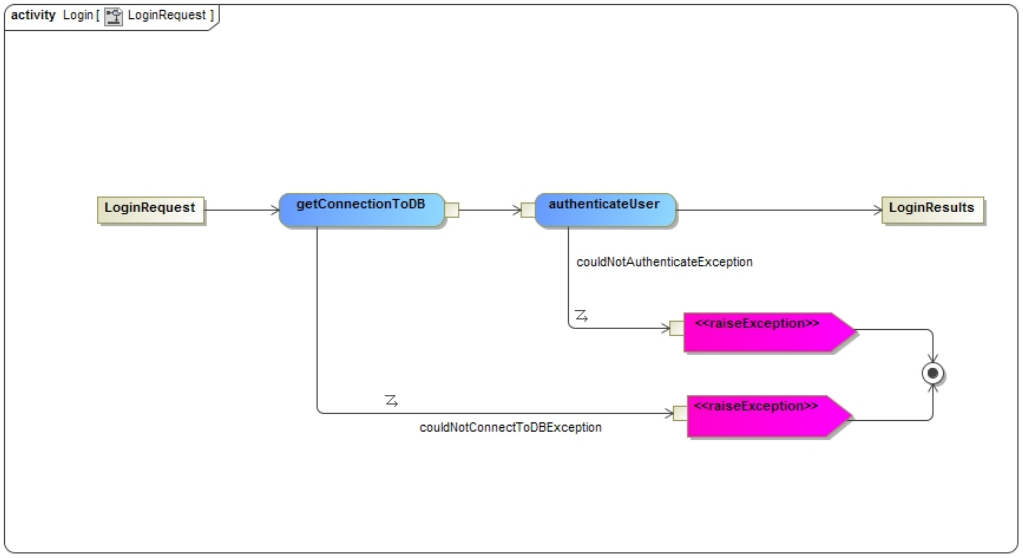

Figure 9: Process Specification: Login for law enforcement and jury

3.3.2 ViewPDE-Priority:important

Service Contract
pre-condition: The PDE is in the database to be viewed.
post-condition: The law enforcement agent can view the PDE.

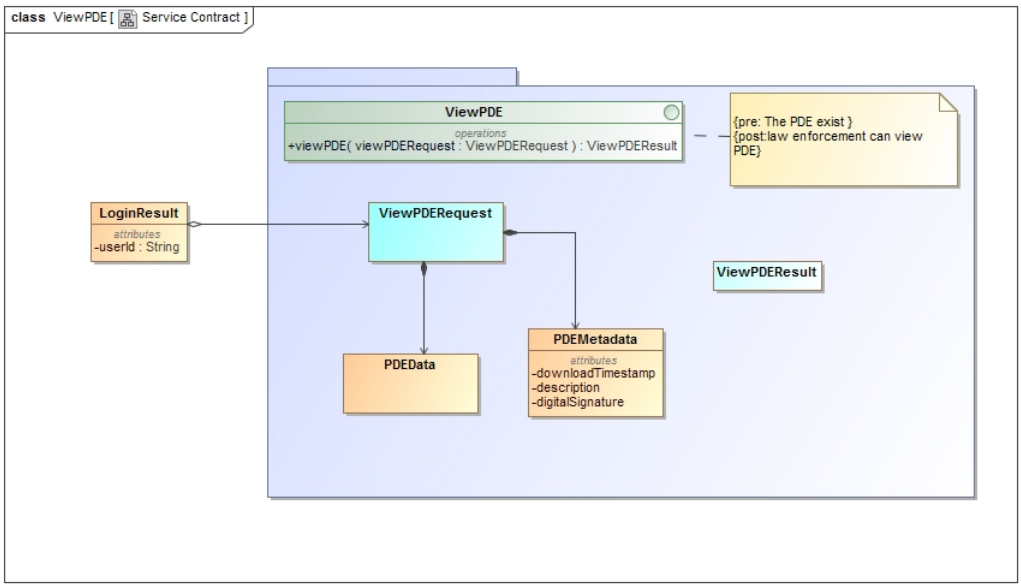

Figure 10: Service Contract: View Potential Digital Evidence.

Functional Requirement

The law enforcement agents should be able to search, view, download and audit what has been uploaded to the server as evidence. They should also be able to see who has uploaded what and the contact details of the person who uploaded the file(s).

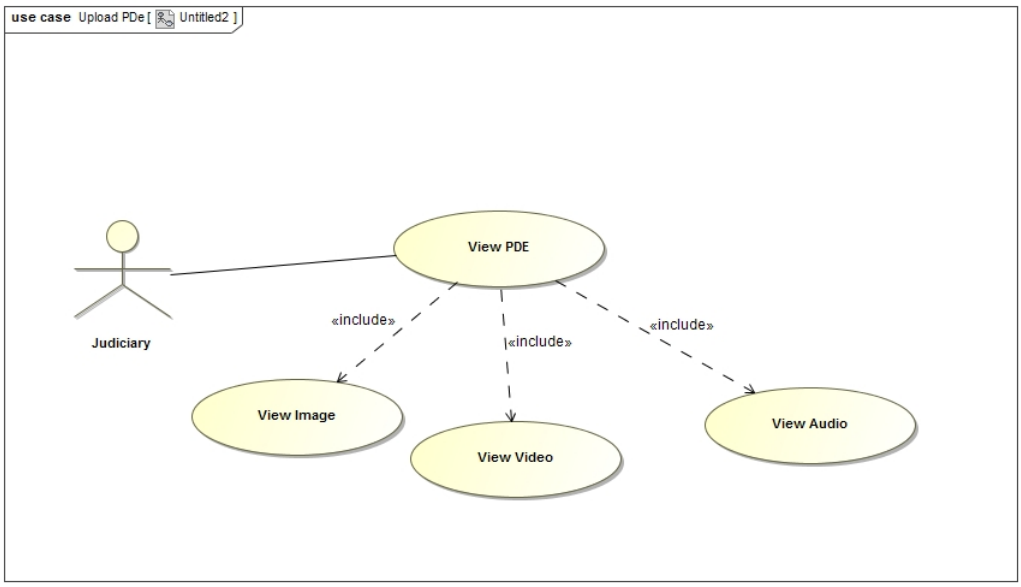

Figure 11: Functional Requirements: View PDE

3.4 Functionalities implemented

list of functionalities implemented from system's use cases:

- Geolocation: ability to detect the system's location at the time the evidence is captured.
- Detect internet connection: ability to tell whether there was internet connection when the evidence was captured.
- Capture PDE: ability to capture images, record audio and video as evidence with our system.
- Upload PDE: ability to send evidence to the database and retrieving it as needed.
- Search: ability for the law enforcement to search PDE file by tags.
- Download PDE: ability for the law enforcement to download pde.
- View PDE: ability for the users and law enforcement to view what has been uploaded
- Login and registration: ability for system users to login or register themselves in order to use the system.
- Access control: law enforcement and users have different rights levels

Newly added functionalities:

- Battery status: This functionality ensures that users upload the evidence before the battery goes flat.
- Tagging: Tag every pde with the geographic location and the time stamp
- Two factor authentication: User get to verify the email address.
- One time password(OTP): user gets a one time password when they register new account.
- Theme: user can choose a theme for the look and feel of the mobile app.

4 Architectural Requirements

4.1 Architectural scope

This system integrate the back-end and the front-end. The front-end of the system is a hybrid mobile app which implements all the front end functionalities required. Functionalitites such as capture videos, audios and images and send those files to a server running on the back end. On the back-end the system runs Apache server, where all the large data files are stored, relational database, where user details and the links to where the files users uploaded. This front-end-back-end integration is made possible by PHP scripts on the server. The app makes RESTful request(http) to send files and user details upon registration to the server.

4.2 Quality requirements

4.2.1 Security(core)

- The system must prevent sql injection
  - The system does string escaping and input validation
- The system must verify user emails
  - Upon registration, the user is send OTP to verify hi/her email address
- The system must implement strong authentication
  - Something user has and something user knows
- The system must detect attacks from unwanted and unauthorized users.
  - Prevent all unauthorized users from accessing the system
- The system must resist attacks from unwanted and unauthorized users.
  - Ensure user's password is longer and strong
- The system must recover from attack from unwanted and unauthorized users.
- The system must minimize access and permissions given to users who do not have the required privileges.

  - Users can only capture and upload, they can not download what the have uploaded.

- All communication of sensitive data must be done securely through encryption and secure channels.
  - Protect user's details and files they have uploaded

- System ensures data integrity
  - Ensure user's details and file are not tempered with

4.2.2 Scalability(core)

- The system operate effectively under a load of registered users.
- The system scales out resources.
- The system manages resource demand.

4.2.3 Reliability(core)

- The system must prevent faults.
- The system must detect faults.
- The system must recover from faults.

4.2.4 Integrability(core)

- The system must integrate with law enforcement server.
- The system integrate with Google maps for Geo-location.

4.2.5 Performance(core)

- Throughput:The rate at which incoming requests are completed.
- The system minimize the responsive time.

4.2.6 Usability(core)

- The system must be efficient.
- The system must be easy to use.
- The user must be satisfied by the system.

4.2.7 Maintainability

- System must be easy to be tested, updated and changed if needed.

4.2.8 Deployability(important)

- The system is deployed into cross platforms.

4.3 How we intend to achieve Quality requirements

4.3.1 Security

- Access control: We have our own access control where registering users have different level of privileges. First of all,user has to login to view what he/she has uploaded and users can only view what they have uploaded. Law enforcement on the other hand, has privileges to view and download any pde uploaded by any user.

- 2 factor authentication - Every user has to confirm hi/her email address for him/her to be successfully registered.

- Hashing: We implement sha256 hash algorithm were we hash users passwords and links to pde before they are send to a cloud.

- Encryption: We implement AES encryption algorithm. We encrypt users passwords and links to pde before the pde is sent to a cloud.

- SSL: we use secure layers to connect to the database to ensure extra communication security when sending data and receiving it from the cloud and database.

4.3.2 Scalability

- Data storage: We use both the database and the cloud to even up the load. We store users information in the database and user's pde files in the cloud and save the link of those large files in the database. This simplifies database structure and increases performance since the large data files are not queried to/from the database but only the partial link of the file is stored in the database and the file itself is stored in cloud. Every user has a related to a list of links of pde files he/she uploaded on our system.

4.3.3 Reliability

- Testing: We are using tested plugins from ngCordova repository to access device's camera, audio and video options. The plugins have been tested and we also do our own integration tests to ensure that the plugins work well with no conflicts.
- Exception handling: We catch all our exceptions to ensure that the system behaves as intended.
- Fault tolerance: A copy of the pde file is kept in our system cache until it is successfully uploaded to the cloud, in case there is a connection error while a user tries to upload the pde file. If there is an error, the cached pde file will be resend.

4.3.4 Integrability

- Our system is integrated with google map api to decode the longitude and latitude values we get from user's device location to human-readable address.
- Server: We integrate mysql database with Apache server to save large files on the server and store the link to the files on the database.
- Plugins: We integrate media plugins to access device's camera, audio and video controls with encryption and hashing algorithms.

4.3.5 Performance

- Cloud and Database: We separated user details from large files users upload to increase performance and to structure our data well.

4.3.6 Usability

- Ionic framework build hybrid apps that uses native device's controls, meaning users enjoy the feel of using an app that is build with native language on any device the user will be using our system on. The button, forms and checkboxes feel as if they were build from native languages on both android and ios devices, meaning users will ship their knowledge of using the device and making it easier for users to adapt and learn to use the system quicker.
- Icon: We use visuals such as icons for users who can not even read to be able to still use the system because of the visuals on the buttons.

- Colors: We use colors to show users the quality and strength of their passwords, making them to enter the right secure password from the start.

4.3.7 Maintainability

- MVC: We use MVC design pattern to separate the view from the controller and the model. This helps us modularize our system and make it easy to maintain and test it.

- State pattern: Every view has it's state and depending on the state, a relevant page loads, this simplifies page linking and makes it easy to load any page dynamically depending on the stage of the current page or on which button pressed.

4.3.8 Deployability

- We are building a hybrid system that can be deployed in almost all the platforms. We are focusing on Android, Ios and windows mobile devices because of the higher percentage in the use of these devices. This also reduces the quirks of different devices and ensures reliability on every device and high performance.

4.4 Integration and access channel requirements

The system will be accessed using Mobile/Android Applications clients through the use of ngCordova, browser clients which is where ionic's web based framework comes in and web services clients.

4.5 Architectural constraints

- There are multiple factors that may place constraints on the architecture that is being developed for the uWatch System

- This is developed under ionic framework which is simply web based, thus it put constraints on certain programming languages Compliance with existing standards

5 Architectural pattern or styles

5.1 MVC(Model-View-Controller)

- Ionic framework is build from this pattern, where the view is the template HTML pages, the model is the JSON object to and from the database and the controller is the JavaScript functions to implement the system's functionality.

5.2 Pipes and Filters

- We will be tagging images, videos and audio files being uploaded to the server and using this architectural pattern to allow us to easily search and filter by tags and categorize the PDE being uploaded.

5.3 Client/Server

- uWatch allows multiple clients to access the system using N-tier architectural style.The benefit of using N-tier architectural style is that it improves the scalability of the system.

- The server side is the back-end of the system which manages the centralized data and access to the database from the server. The aim of having the back-end manages the data is to achieve higher security.

6 Architectural tactics or strategies

6.1 Security:

We do not cache user credentials nor keep them in history. This forces users to login everytime they need to login to the our system. Users have a limited amount of tries to login.

6.2 Maintainability and Flexibility:

Our views are templated, separating the view from the templates. Since our system relies on AngulaJS, we inject dependencies and as such the is Inversion of control (IoC).

6.3 Perfomance:

We catch users' retried PDE so that the system can respond faster especially on slow internet connection. Localstorage caches data in case the relational DB goes down and once it goes up again, it synchronizes the cached data with the data in the DB.

6.4 Scalability:

Our server is not tightly coupled with the system. The serve can be hosted any where, locally or remotely. Links to files stored on the server are send to a relation database.

We use local storage to store any PDE that the user chooses to upload later in case the user did not have internet connection at the time the PDE was captured.

6.5 Reliability and Availability:

caching and local storage as explained above.

6.6 Auditability :

Users login before they can upload a PDE. We use date, time-stamps and Geo-location.Data that is send to and from the serve is encrypted.

6.7 Testing:

we will implement unit testing and integration tests to see if the pre and post condition are/were met.

6.8 Usability:

We use nice icon and buttons and less text and encourage users who can not read to be able to use our system. Since it is a web base, we develop our system in away that blind and visual impaired users will be able to use screen readers to access our services.

6.9 Integrability:

Our system is integratable since it is decoupled form the cloud/database, it can work with any database or a cloud for that matters or simply a local storage.

6.10 Deployability:

The system is cross platform, it will be deployable on IOS, Android, Windows, Amazon and blackberry platforms.

7 Use of reference architecture and frameworks

- We are using Ionic framework to implement our mobile application. Ionic framework is a mobile base framework build on the following frameworks:
  - ngCordova An Apache cordova framework which packages HTML, css and js files in to respective platform such as Android, IOS, Blackberry, Windows mobile etc.
  - AngulaJS Is a Google JavaScript framework that helps implement controllers and services for our project.
  - Bower and Node package manager (NPM) to help install dependencies and plugins into our project in order for us to extend functionality beyond your normal JS capabilities.
  - UI-Routes we use routes to changes from one view to the other and from one state to another, this framework help us achieve exactly that.
  - Gulp js for simplifying our project and stripping out all unnecessary comments on our codes so that it can compile faster and respond quicker. Furthermore, the packaged final project file is relatively smaller and making it easy to deploy, share or to store.
  - SASS this is the framework that deals with the look and feel of our application. SASS is described as css on steroid on the sass website.
- Reasons for choosing ionic framework:
  - Since it is a web based, it leverages our web development skills and the knowledge we have of the web based languages such as js, HTML and css.
  - It is cross platform, one project will be deployed on every platform. Meaning we do not need to write special code to accommodate a specific platform or learn the native language that each platform

uses. This speeds up production and is convenient since we can not assume that users will be using one specific platform.

- It is pretty powerful. We use ngCordovas plugins to access native device camera, video camera, audio recording, media file, local storage etc All this is done effortless.
- Our app has to access ones Geo-location and it is relatively easy to that with ionic than will a native language.
- Is easy to implement security features in javascript
- Is easier to debug, you can also debug in a browsers console.
- It uses less resources, you do not need an emulator to test features such as Geo-location or encryption
- There are many encryption js libraries. For example forgejs, cryptojs and they both implement AES cryptography.
- It's easy to work with JSON object.
- It has a great community and up to date plugins.

8 Access and integration channels

- Integration channels that we using:
- We using a REST API which uses the Library cURL(which is a computer software project providing a library and command-line tool for transferring data using various protocols)
- This REST API uses :
  - HTTPS (Hypertext Transfer Protocol Secure) is a protocol that allows safe and secure transfer of data over a network.
  - HTTP PUT for retrieving, writing and updating of data.
- API specifications used in the integration of the systems
  - Authentication API - We have our own access control were users are required to verify their email address by OTP
  - Security API - which an API that specifies rules(read,write and validate),what the client can be able to access and what restricted to them and it provides encryption strategies,for example Forge(which is an encryption method).

- Quality requirements that can be achieved through the implementation of the access channels mentioned.
  - Reliability so that the system is online as much as possible and that data transfer isnt easily corruptible and that the transfer is fast. We use localstorage to back up the file before it is send to the server, if the file transfer fails or the file gets corrupted, then the local copy is tried until the file is successfully uploaded.
  - Security of user data being transferred.
  - Scalable so that a large amount of users data can be transferred to and from the systems.
  - Maintainable, the integration with the system must be easily maintained. (because for example security rules are all defined in one place.

9 Technologies

Technologies Used in the development of our Application are stated below along with why the choice was made and it's benefits.

9.1 Ionic framework

- Ionic framework is a great framework that supports hybrid application which has many benefits, specifically in terms of access to third party code , speed development and platform support.
- It is an Model-View-Controller framework which separates concerns, allowing re-use of the business logic; it enables parallel development by separate teams which is ideal when working in a project such as this one. The MVC framework uses AngularJS for controllers and services, HTML for view and JSON for the model which are all popular and easy to learn languages.

9.2 ngCordova

- ngCordova is a collection of 63+ AngularJS extension on top of the cordova API that make it easy to build, test and deploy Cordova applications with AngularJS, ngCordova uses packages and libraries, compiles source code and deploys the source code to Apk (android), Xap (windows mobile) and ipa (ios).

Security provided by the serve includes:

- Authentication API-who the user is.
- Support SSL on all clients
- Uses Bcrypt for password storage
- Uses the JSON Web Token for standard credentials
- Generate Server-Signed Tokens
- All security Logic is put in one pace

The benefits of using PHP and MYSQL:

- PHP has many libraries for encryption and hashing
- Is easier to send email with php than with many server side language
- PHP works well with session and tokens
- MYSQL is easy to work with
- Is easier to manage user details and writing sql queries

10 Unit testing

Unit testing are done using karma and grunt. They support the following frameworks:

- Jasmine
- Mocha

They support dependency injection and use angular-mocks for mock-up data.

11 Integration testing

Integration testing are done using grunt. Here no mocks are used.

12 References

- All About Ionic (author and date unknown) Available from:http://ionicframework.com/docs [Accessed: 31 july 2015]
- Why use ngcordova (author and date unknown) Available from:http://stackoverflow.com/qu [Accessed: 31 july 2015]
- Features (author and date unknown) [Accessed: 31 july 2015]
- S.Omeleze,H.S.Venter, Toward a model for acquiring digital evidence using mobile devices. Information and Computer Security Architecture (ICSA) Research Group, University of Pretoria.
- AGILE METHODOLOGY (author and date unknown) Available from: http://agilemethodology.org/ [Accessed: 15 May 2015]