Functional Requirements(uWatch digital forensic tool)

Group Name: MPHETamines

Version: 1.3

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

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

Date: 22/09/2015

Contents

1 Introduction **1**
1.1 Project Background 1
1.2 Project Purpose 1
1.3 Project Scope 2
1.4 Project Assumptions 2

2 Methodology **2**

3 Application requirements and design **2**
3.1 ONW Application Module 3
3.1.1 CapturePDE-Priority:critical 3
3.1.2 UploadPDE-Priority:critical 3
3.1.3 ConfirmPDE-Priority:important 5
3.2 The Administration Module 6
3.2.1 DownloadPDE-Priority:critical 6
3.2.2 ValidatePDE-Priority:critical 7
3.2.3 EncryptPDE-Priority:critical 7
3.2.4 DecryptPDE-Priority:critical 7
3.2.5 ManageAccessAllocation-Priority:critical 8
3.3 Login and Administrative user 9
3.3.1 Login-Priority:critical 9
3.3.2 ViewPDE-Priority:important 11
3.4 Functionalities implemented 14
3.5 References 15

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 too broad and with the time allocated to the team for this project we decided to focus on only one element of the application, users will only upload pictures as evidence for now and disregard the video and audio part of the ONW model. There are three aspects of the system the mobile application side, utilised by a community member; the desktop side where a law enforcement agent logs in and the algorithm which sits in between the mobile and desktop. The algorithm will be used to determine if the photo uploaded is a crime photo. we will focus on human and object detection for now and maybe at a later stage if time permits other media could be uploaded as well.

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.

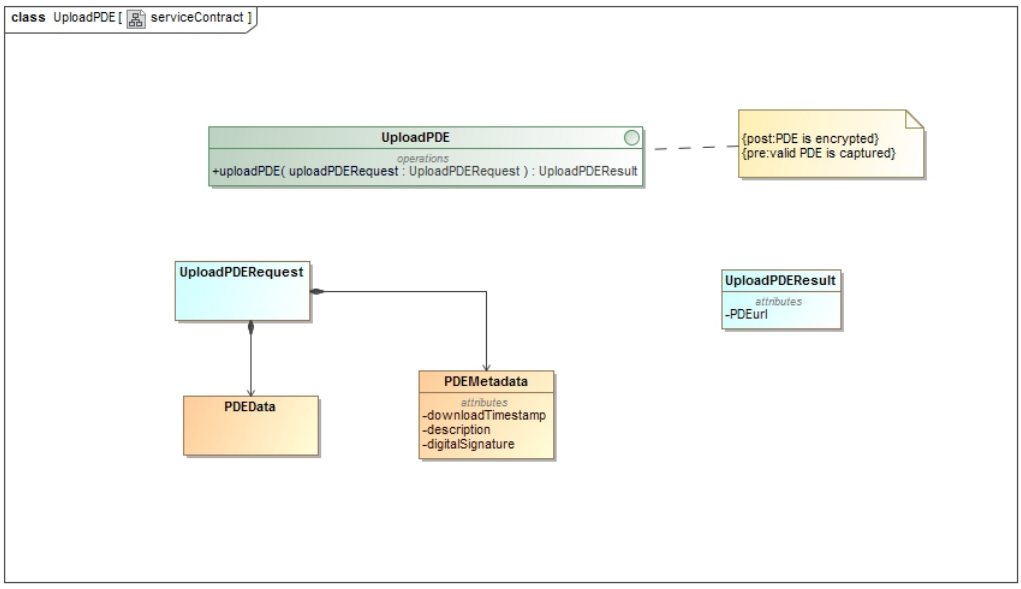

Figure 1: Service Contract: Uploading Potential Digital Evidence

Functional Requirement

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

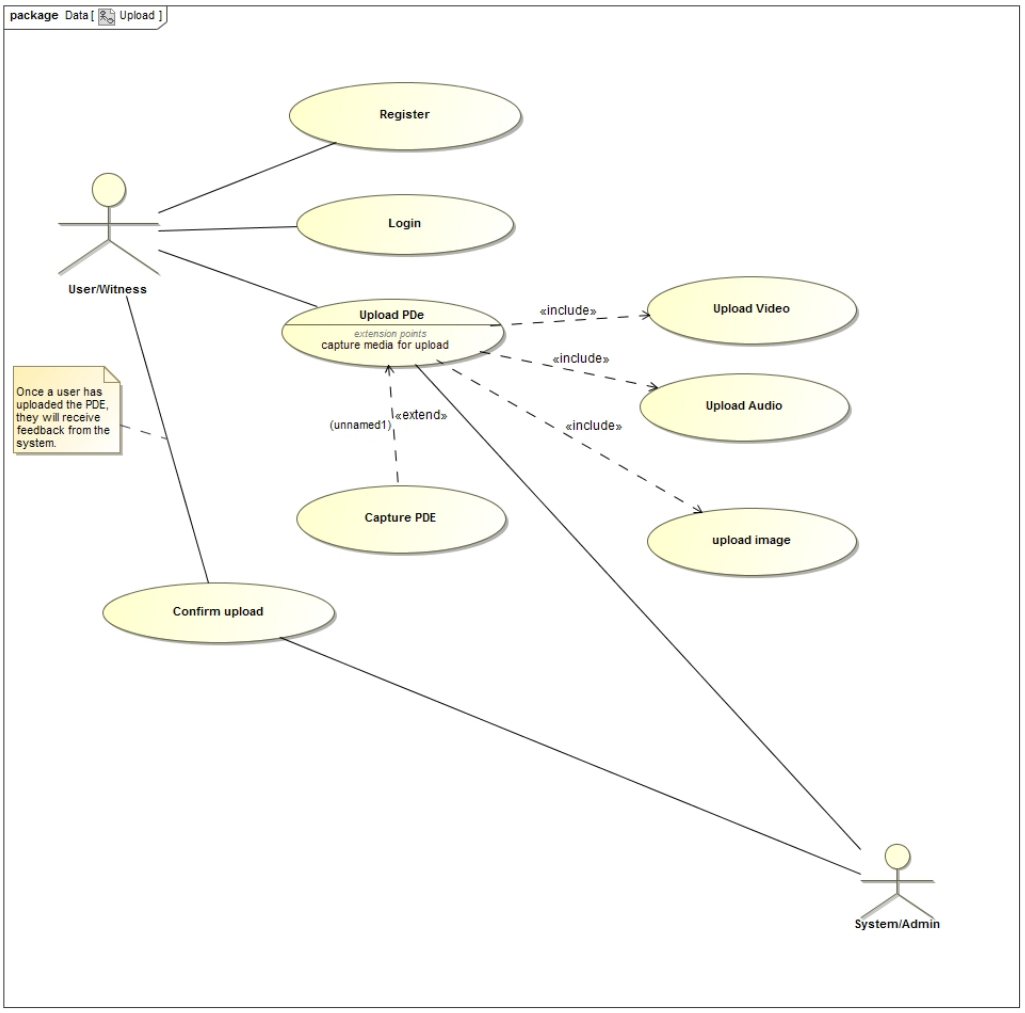

Figure 2: Functional Requirements: Uploading Potential Digital Evidence

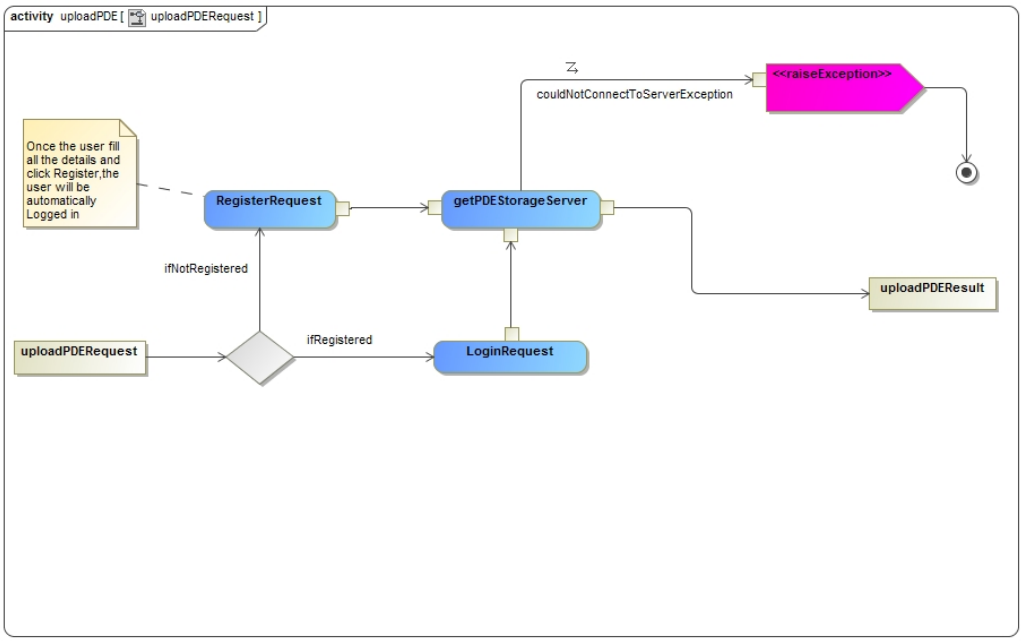

Figure 3: Process Specification: Uploading Potential Digital Evidence

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

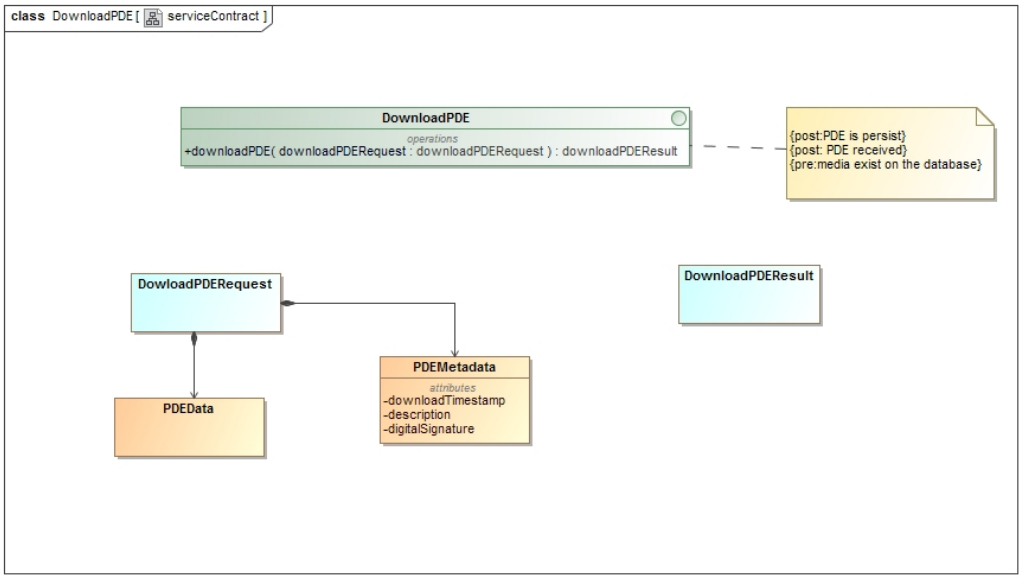

Figure 4: Service Contract: Downloading Potential Digital Evidence

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

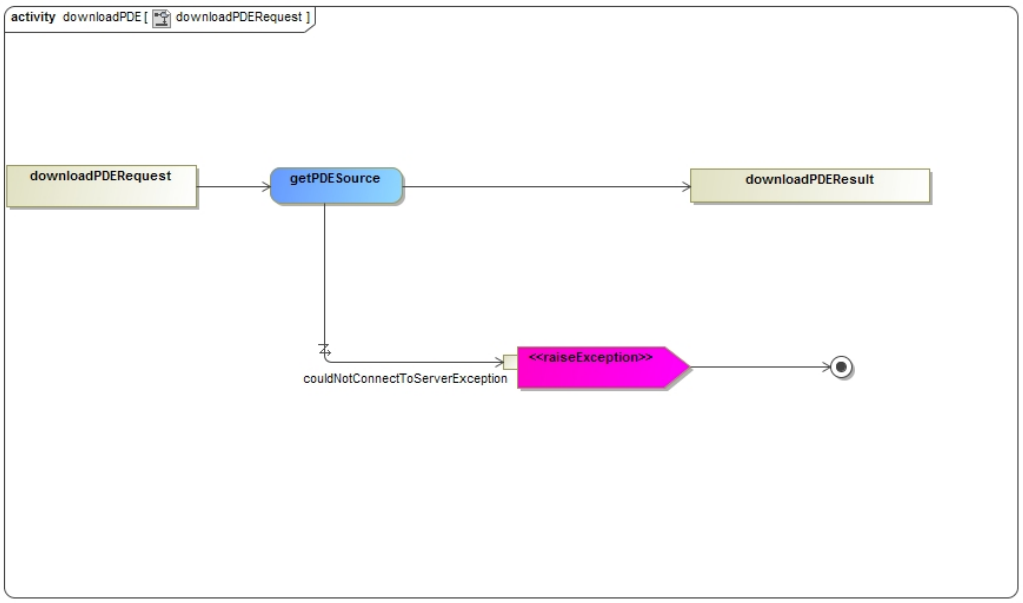

Figure 5: Process Specification: Downloading Potential Digital Evidence

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.

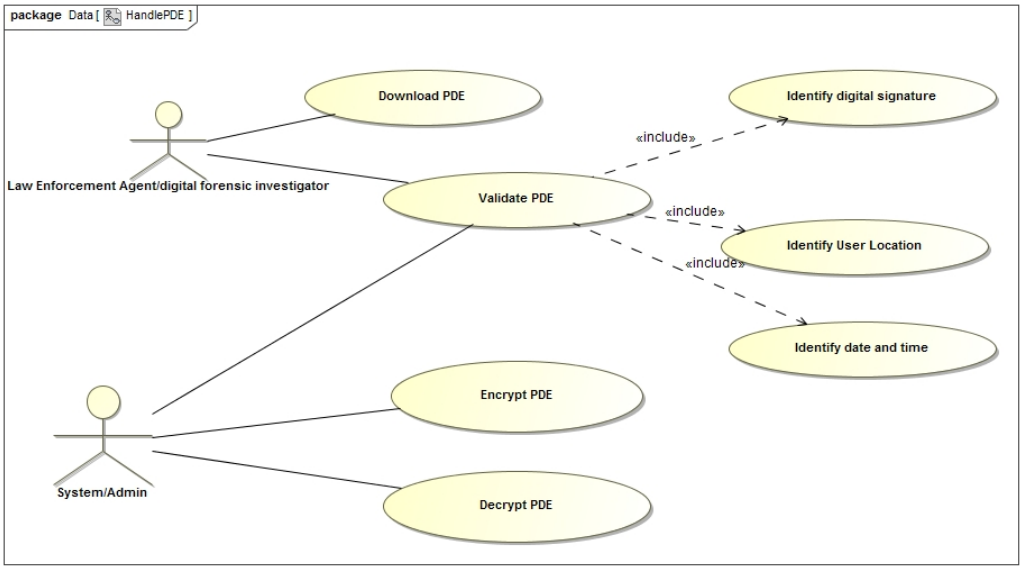

Figure 6: Functional Requirements: Validate,encrypt and decrypt PDE

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.

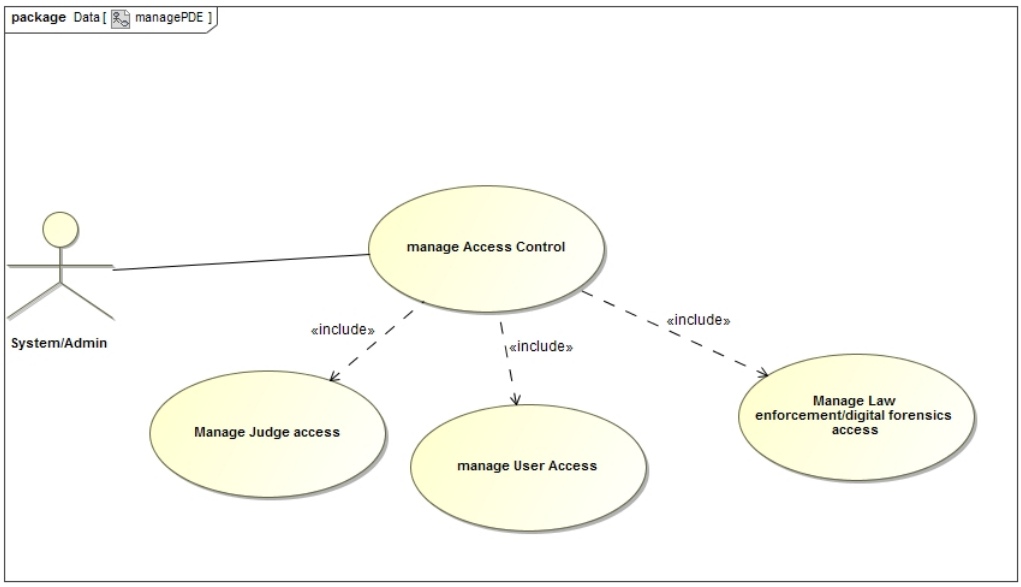

Figure 7: Functional Requirements: Manage Access Allocation

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.

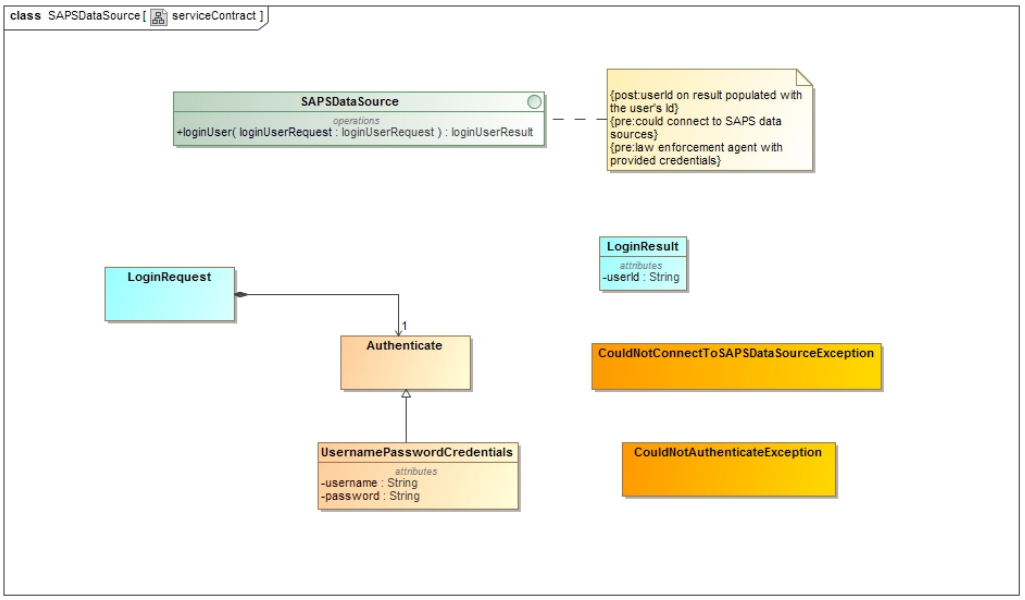

Figure 8: Service Contract: Login for law enforcement and jury

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

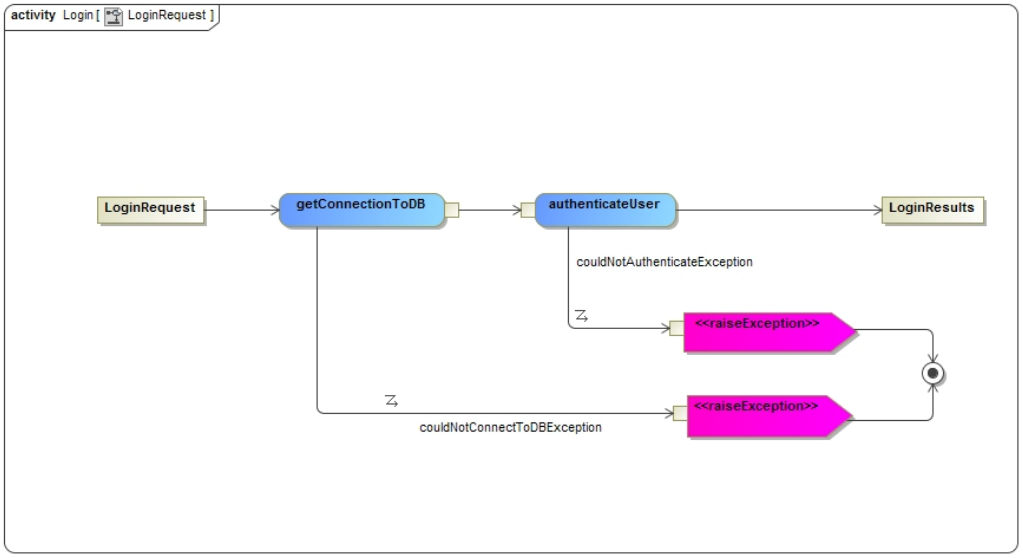

Figure 9: Process Specification: Login for law enforcement and jury

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.

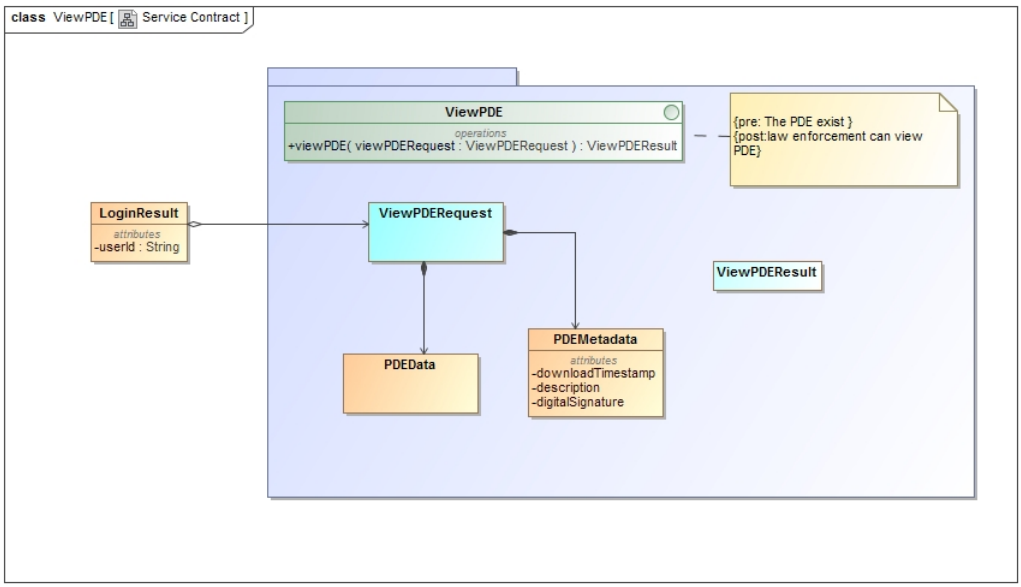

Figure 10: Service Contract: View Potential Digital Evidence.

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).

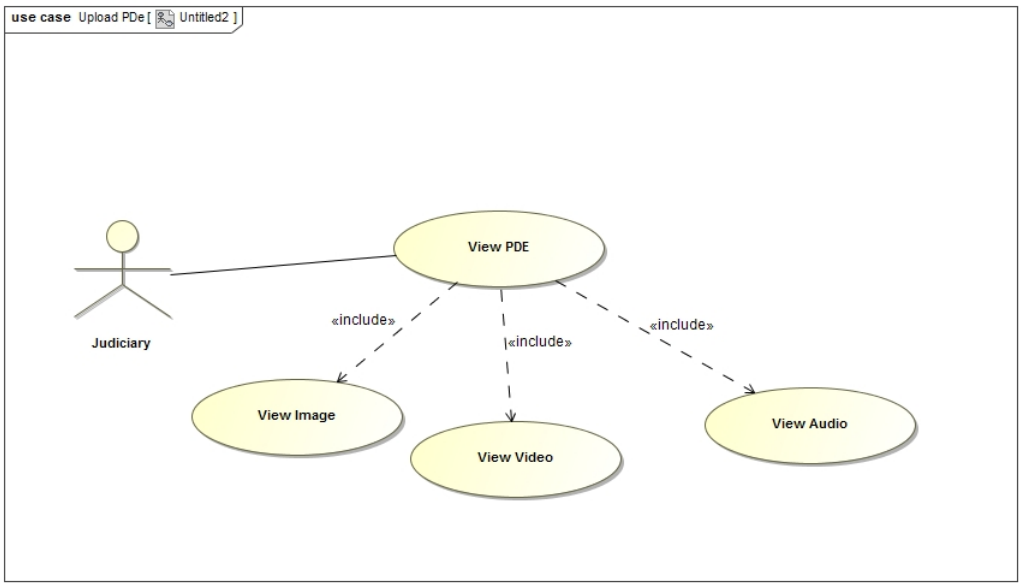

Figure 11: Functional Requirements: View PDE

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.

3.5 References

- 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]