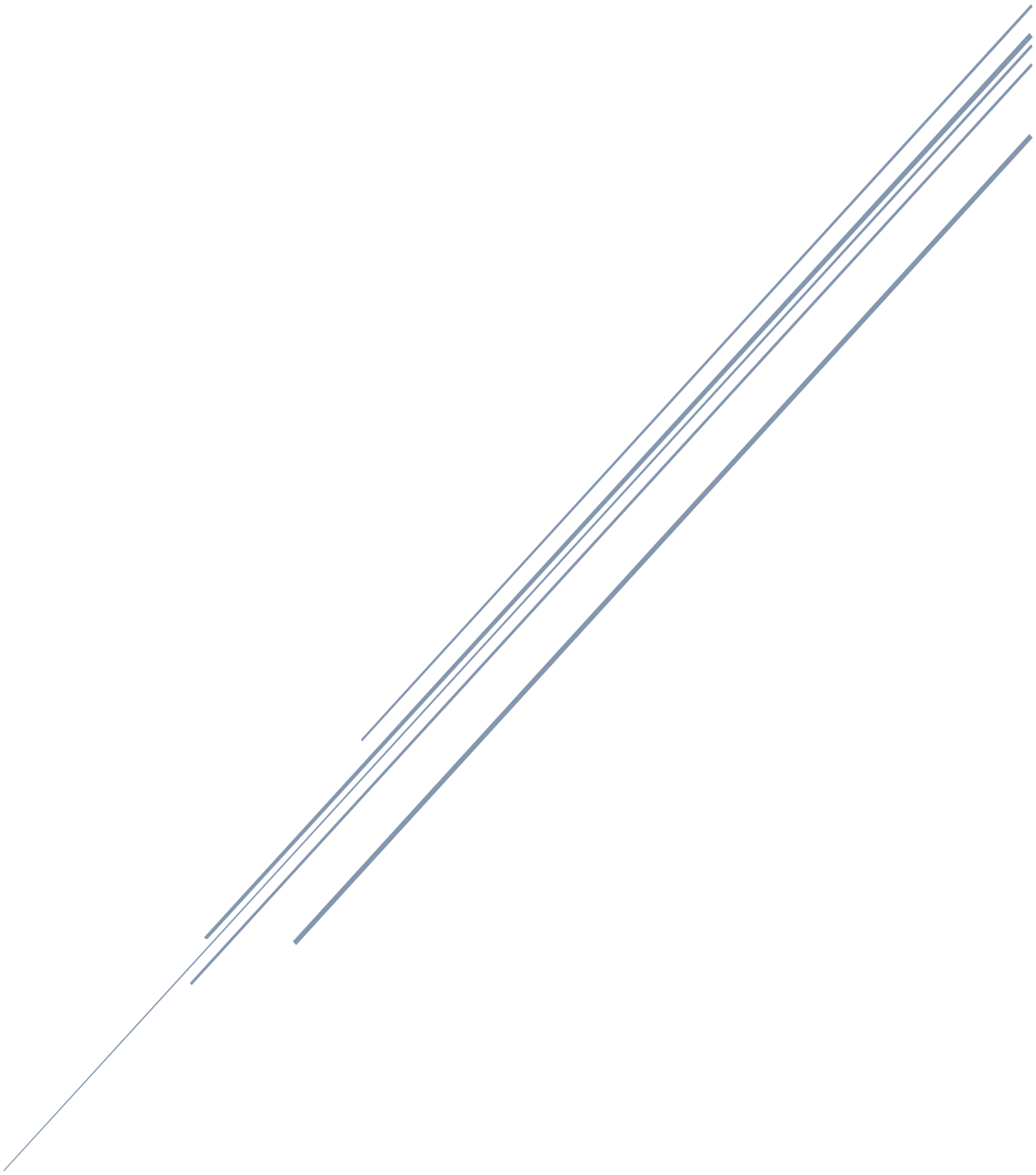
LYNK SOLUTIONS

Demo 1: SRS Document

Watchdog



University of Pretoria
COS 301 Software Engineering

Table of Contents

Introduction 2
User characteristics 2
Domain model 3
Functional requirements 4
Use Cases 4
Requirements 4
Subsystems 5
Main System Diagram 5
Home Control Panel Subsystem 6
Intruder Subsystem 6
Notification Subsystem 7
Storage Subsystem 7
Quality requirements 8
Performance: 8
Reliability: 8
Scalability: 8
Security: 8
Maintainability: 8
Usability: 8
Portability: 9
Cost: 9
Trace-ability matrix 9

Introduction

This document aims to provide an outline of the software design decisions made for the Watchdog System. An overview of system design and properties are detailed and serve as an integral artefact in the development cycle..

The Watchdog Security System is a home security system that provides a reliable means of home-intruder detection, as well as a notification service intended for the homeowner and third-party response teams.

The concept for Watchdog stems from the extensive need for home security in South Africa. The Watchdog solution is perfect for the technologically immature market that exists within the country – that being said, the system implements a versatile and easily-deployable design such that the country of use is not a prerequisite consideration in deployment.

User characteristics

The Watchdog system is intended for the use of any person who values their home security or works on the side of security enforcement. It is easily deployable and low-cost, allowing for a widespread user-base.

Expected Users:

Homeowners

With upwards of 15 million households in South Africa, and household break-ins being the most frequently committed crime (5,8% of households are affected), the market for the Watchdog security system is largely untapped, considering the security needs of most homes are unfulfilled. It can be expected that homeowners from low-income to high-income households will be interested in usage of this system, since deployment costs are low, and performance is of a high standard – although the wealth distribution of the country would imply that the most opportune market is in the lower to middle-class income households.

Venue/Building Owners

Separate to the concerns of household break-ins are break-ins that occur at/in commercial venues. The versatile nature of the Watchdog system means that it can be deployed in many different scenarios, namely: restaurants/bars, shops, offices, etc. In the same way that households are defended by third-party security teams, these building owners will be offered a similar level of threat detection and reaction.

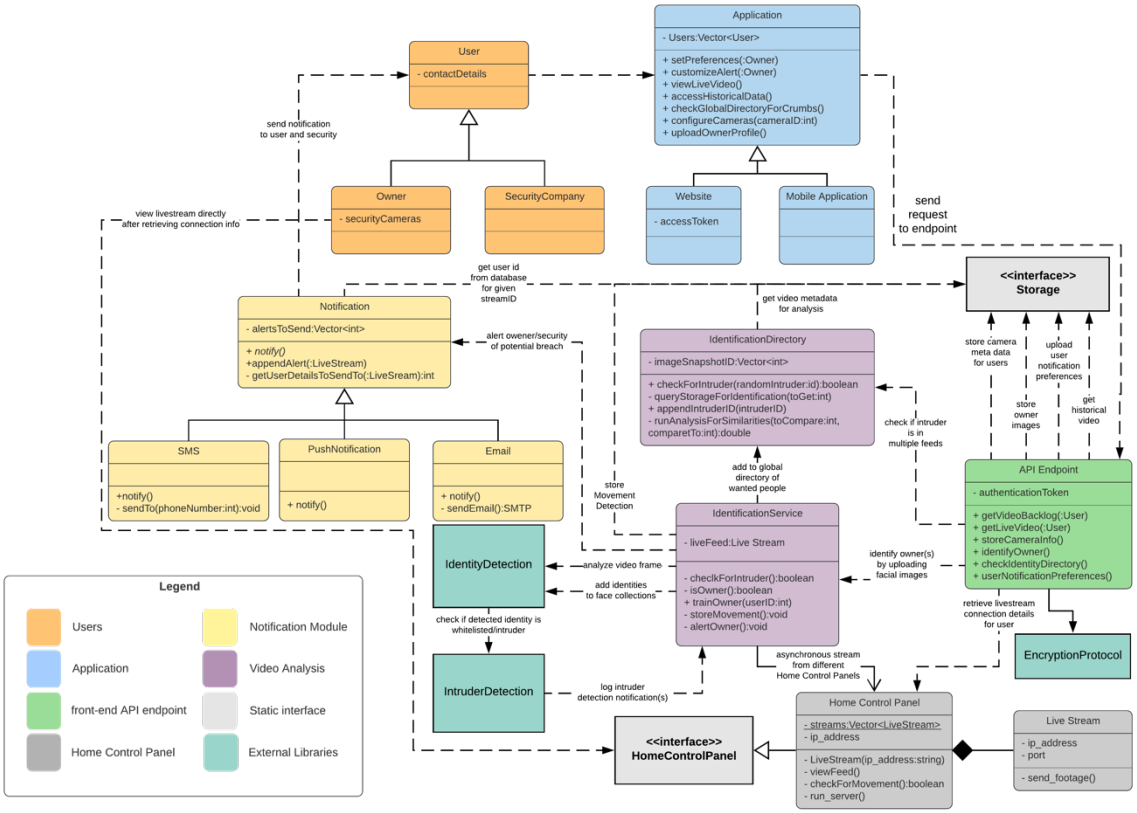
Private Security Companies

The Watchdog system is reliant on third-party security enforcement as first responders to high risk situations, meaning that proper implementation is heavily dependent on the Law/Security enforcement market where the system is deployed. South Africa's private security industry is one of the largest in the world (with over 9000 registered security companies), meaning that it is one of the most accommodating market for the Watchdog System. The first responders will use the system as a means of intrusion detection and notification, allowing for the Security Teams to be stationed.

Law-Enforcement

Public law-enforcement may also be users of the Watchdog system in the way of information collection (potentially in the case of legal action), as well as another layer of third-party security enforcement for the security system (with an expected response slower than that of private security.)

Domain model



The Watchdog system as can be seen in the domain model, will consist of several independent components. This is seen on the domain model where the legend points out the different components. This promotes scalability to grow with an increase of user demand. With separation of concerns, this will allow our team to work on several components independently.

Our system is an event-driven system that encompasses several independent features hosted on Amazon Web-based Services. Using a serverless architecture, we will design our system to be scalable and loosely coupled. This will allow for a more sustainable system that maximizes the resources used at a cost dependent on the usage of resources. The user is the source of truth that controls what events the system will respond to.

Functional requirements

Use Cases

Live Stream:

- User connects to our home control panel subsystem
    - This is done through sockets, and port number

Home control panel – IP Camera:

- User must configure their cameras to this subsystem
- Identify movement
    - Send video frames to Intruder subsystem for further analysis

Intruder Detection:

- Accepts movement detection streams from the home control panel
- Sends off intruder detection to notification module

Notification:

- Relationship between intruder detection and notification subsystem
    - Intruder detection extends to notification if it identifies that there is an intruder
- Send the notification to the owner/security once in notification module
- Can send either: SMS, Email, or Push notification based on user preferences.

Historical Video Streams:

- Accept the video streams to be stored from the intruder detection module or the Home Control panel.
- Owner retrieves the historical video footage from this module

Global Directory of wanted people:

- Send image to this module when an intruder is identified in the Intruder Detection module

User Interface:

- Secure login process
- Push notification are reviewed here
- Notification preferences
    - SMS, Email, and push notifications
- View live streams
- View Historical Streams

Requirements

R1. **Video Footage:** The system shall provide live footage and historical footage captured on owner's respective ip cameras to be accessible for owners.

R1.1. The system shall provide a real-time live stream view of owner's ip cameras for owners to view at any time.

R1.2. The system shall analyse ip camera streams **locally** on the owner's computer machine.

R1.2.1. The system shall use the Open Source library Vidgear coupled with OpenCV in order to identify movement detection.

R1.2.2. The system shall provide a stand-alone executable package that will be installed on the owner's computer machine in order to analyse the ip camera video streams locally.

R1.3. The system shall be able to distinguish between the identities of owners/security and intruders by analysing movement detection streams.

R1.3.1. The system shall utilize Rekognition to achieve this.

R1.3.2. The system shall store images of the owner's in order to add the owner to the face collection that Rekognition will utilise in order to distinguish an owner apart from an intruder.

R1.3.3. The system shall only utilize Rekognition once movement detection is identified on the owner's local computer machine.

R1.4. The system shall provide historical video feed for owners to view at any time.

R1.4.1. The following video streams are made accessible for the owner to view: Intruder detection video streams; movement detection streams; and random video streams.

R2. **Notification:** The system shall send notifications to the owner on a potential breach.

R2.1. The system shall notify Owners and security companies when the system identifies that there is an intruder identified on their respective ip cameras.

R2.2. The system shall provide customization of the type of notifications that are sent to the Owners.

R2.2.1. This includes choosing from an SMS, Email, or push notification.

R3. **Interface:** The system shall be accessible both on a web and mobile application.

R3.1. The system shall provide a web and mobile application for the owner to choose from.

R3.2. The system shall provide an easily configurable GUI to seamlessly connect owners' ip cameras to the system.

R3.3. The system shall provide capabilities for owners to view historical and live stream footage from either platform.

R3.4. The system shall provide administrative capabilities on the web application for owners to customize them

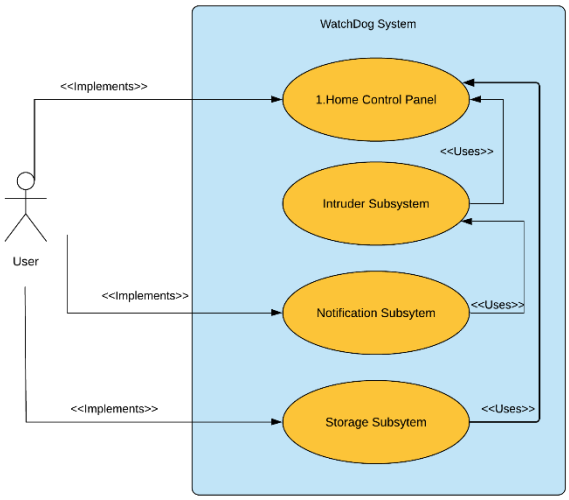
R3.5. The system shall provide a proxy that validates the owner's credentials to prevent the system from any security breaches.

R4. **Global Directory:** The system shall provide a directory of intruders captured by the system.

R4.1. The system shall store intruder image when an intruder is identified by the system into a global directory.

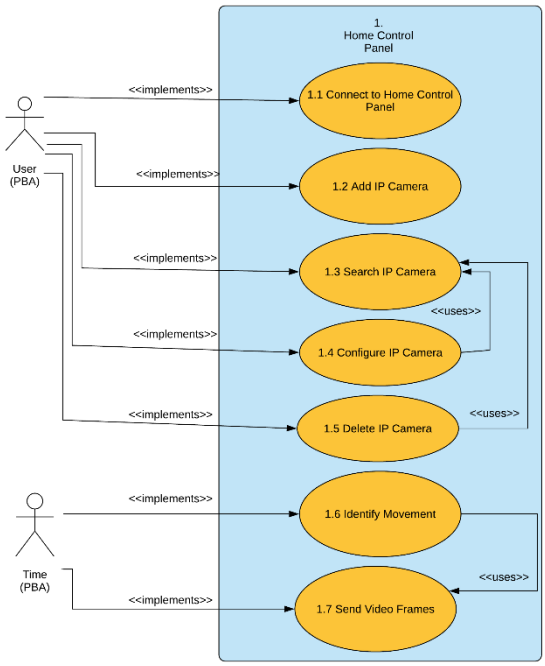
Subsystems

Main System Diagram



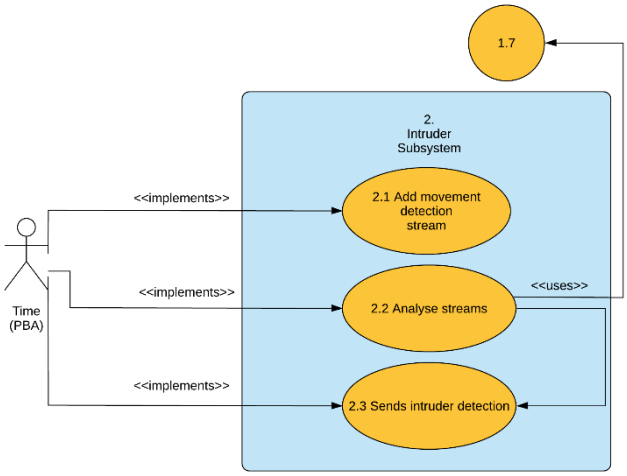
In this simplified main system diagram, we can clearly showcase the core subsystems of the Watchdog system and their interactions with each other (such as the Notification subsystem and Intruder Subsystem when a threat is detected) and how the external user implements the subsystems by performing certain actions (such as configuring IP cameras in the Home Control Panel or accessing the Storage subsystem for historical video streams).

Home Control Panel Subsystem



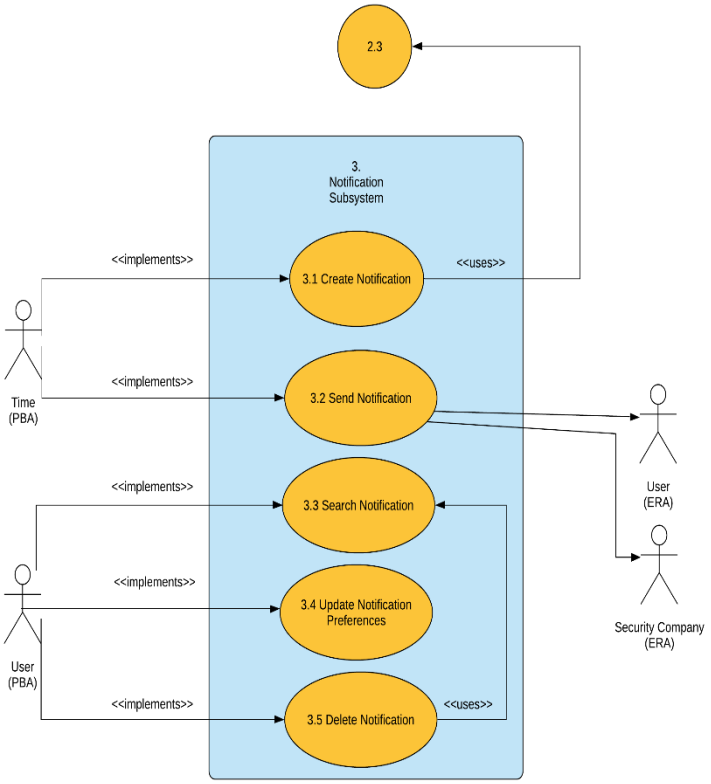
The Home Control Panel subsystem uses the Home Control Panel as an interface and means for the user to interact with the IP camera and set up their home security. It also allows movement to be identified and subsequent video frames to be sent

Intruder Subsystem



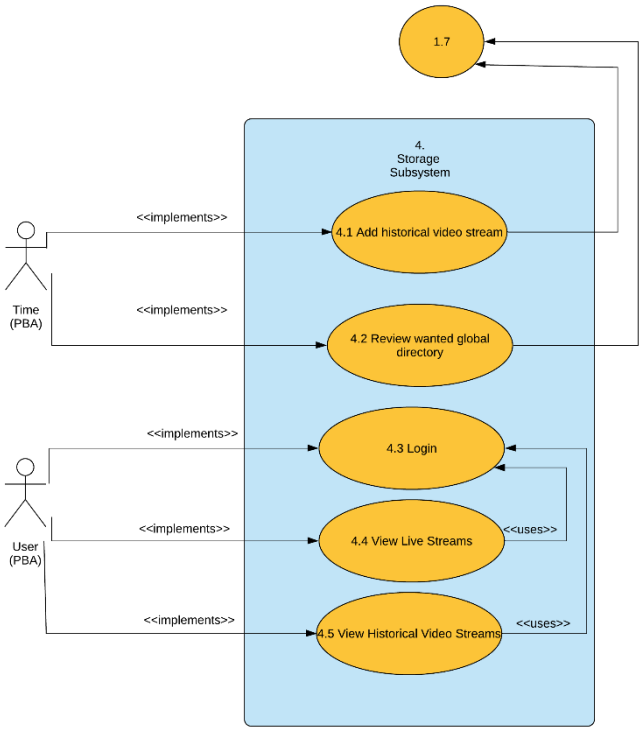
The Intruder subsystem handles intruder activities and analysis. If a video frame sent by the Home Control Panel Subsystem is deemed to contain an intruder, an intruder detection mechanism is sent to the Notification Subsystem.

Notification Subsystem



The Notification Subsystem handles and creates all notifications sent to the user and security company affiliated with the system. The notifications can be created, the preferences and nature of the notifications (such as email, SMS or push notifications) can be altered by the user and notification messages removed over time.

Storage Subsystem



The storage subsystem will garner footage from the sent video frames from the Monitoring Subsystem and secure the data with a login authorisation for the user of the system. It will allow the user to view both historical and live video streams from the storage. The video frames are also analysed with images compared to individuals in the global wanted directory for any notices of dangerous felons with a criminal record.

Quality requirements

Performance:

The system is a real-time security system that alerts security and owners of a possible breach. Hence, we need to ensure that the notifications are carried out effectively as the safety of our owners are dependent on the rate of response by the security companies. As such, the analysis of user data streams should be performed with minimal latency and a great degree of accuracy.

Reliability:

The notifications of the system should be timely. When an intruder (or other maleficence) is detected the notification must have a 100% rate of alerting the user. Additionally, the system should be able to adjust to lower latency internet speeds and recover gracefully when internet is unavailable at unforeseen times (such as during "load-shedding").

Scalability:

The system must be highly scalable to grow with an increase of user demand. Additionally, the system must be able to handle an increase in video feeds that could be exponential, as users can have multiple security cameras.

Security:

All data must be encrypted, and access must be used and stored in accordance with the South African POPI act. Access to the system must be controlled and all application settings and data must be available to the Owner. The Owners video camera feed is continuously sent to the servers over the internet; thus, a secure means of data transmission is required by means of end-to-end encryption and safe storage. Watchdog shall securely encrypt all calls made at REST to protect the owner's information. This sensitive data cannot be exposed to outsiders and user verification needs to be strong.

Maintainability:

The system must be modular and allow for a lot of uncoupling of individual subcomponents to allow for easier deployment and maintenance.

Usability:

The Mobile and Web user interface must be functional. This means that a User must be able to watch video streams, configure their settings and potentially get notifications. Accessing the physical application should be separate from configuring the security cameras to allow for a separation of concerns as well as flexibility in how one wants to set up their cameras.

Portability:

The system shall provide Watchdog to be accessible both on a mobile & Web application. This includes having the ability to stream live video on their mobile device and administrators to use a web application. Additionally, we need to ensure that the users may be able to set up their surveillance system in a seamless manner. This means that we need to account for any IP camera such that the user may set it up.

Cost:

Since the Watchdog system uses several Web-based services hosted on AWS, we need to ensure that the cost is minimized to run the different services. This is done such that we will provide a serverless architecture that minimizes the cost of resource usage and provides a cost-effective solution for Amazon.

Trace-ability matrix

Requirements VS Sub-systems

	Website	Mobile	Database (DynamoDB)	Cloud Storage (S3)	AI (Rekognition)	Home Control Panel	Notifications (SNS)
R1				X		X	
R1.1	X	X	X			X	
R1.2				X		X	
R1.2.1						X	
R1.2.2						X	
R1.3					X		
R1.3.1					X		
R1.3.2	X		X	X			
R1.3.3						X	
R1.4				X			
R1.4.1	X	X		X			
R2.1		X					X
R2.2	X	X	X				
R2.2.1	X	X	X				
R3.1	X	X					
R3.2						X	
R3.3	X	X		X			
R3.4	X	X	X				
R3.5	X	X	X				
R4.1				X	X		