Prototype I and Customer Feedback

E Cubed Group (P2)

Deliverable F	Rares Constantin Serban	Emma Belal
November 3rd	Louis-Philippe Keith	

Abstract

Deliverable F will cover our first prototype for the restricted zone net-aware system. Our first prototype is testing the facial recognition capability of OpenCV and the notification capability of Twilio SDK which we will later use along with Shabodi APIs. Next, we will cover the test cases which include User Enrollment, PIN Verification and Access Control, Face Recognition, Unauthorized Access Notification, Notification Reliability and Delivery, Performance and Environmental Tests, and Error Handling and Recovery. We will then go over the analysis of our first prototype, the feedback from the user, and the updated specification. This will be followed by the bill of material and prototyping plan.

Table of contents

Introduction 5
Prototype 5
Overview 8
1. Objective 8
2. Test Scope 8
3. Test Environment 8
4. Test Cases 9
4.1 User Enrollment 9
4.2 PIN Verification and Access Control 10
4.3 Face Recognition 10
4.4 Unauthorized Access Notification 11
4.5 Notification Reliability and Delivery 12
4.6 Performance and Environmental Tests 13
4.7 Error Handling and Recovery 14
5. Acceptance Criteria 14
6. Resources 14
7. Schedule 14
Analysis 15
Comments and Feedback 15
Client Feedback 15
User Feeback 16
Updated Target for Specifications and Detailed Design 16
Updated BOM 17
Prototyping Plan 18
Prototype 2 18
Execution Plan 18
Conclusion 19
References 20

Introduction

In this Deliverable we will detail our first prototype. We will discuss the decisions behind our first prototype. In addition, the critical components of the prototype will be analyzed, and we will see how the prototype matches with the desired metrics. From these factors we will present plans for testing and the prototype.

We have gathered feedback from the client representatives and from prospective clients. We will explain how we will implement the ideas into the next iteration of prototype(s).

From these developments we will update our detailed plans, our Bill of Materials (BOM), and target specifications. Finally, we will present a table of prototyping test planning to show the progression of this project.

Prototype

Our first prototype has a dual focus testing the plausibility of this system working. The first focus is facial recognition abilities and the second being notification system. The prototype has been developed only using a laptop with a camera, VSCode studio, and selected APIs.

The ability to recognize ‘employees’ entered in a database from information received by the camera is being explored in this prototype. We have created a database operated by 1 administrator and containing 1 employee. The employee has been assigned a username and pin code to access a ‘room’. If the employee enters the information correctly and is using the assigned pin, they are granted access.

In this prototype there are two types of notifications being sent. The first being if access has been granted, and the second if there is an unauthorized access attempt. The employee who has been granted access will receive a notification. The administrator will receive a notification about unauthorized access. The notifications are received as a text message (SMS) and an e-mail. The administrator’s notification will also contain a photo of who caused the unauthorized access event.

The below two figures demonstrate the two current outcomes of facial recognition. The black arrows show what the employee must do, and what they see. The gray arrows show what the code generates.

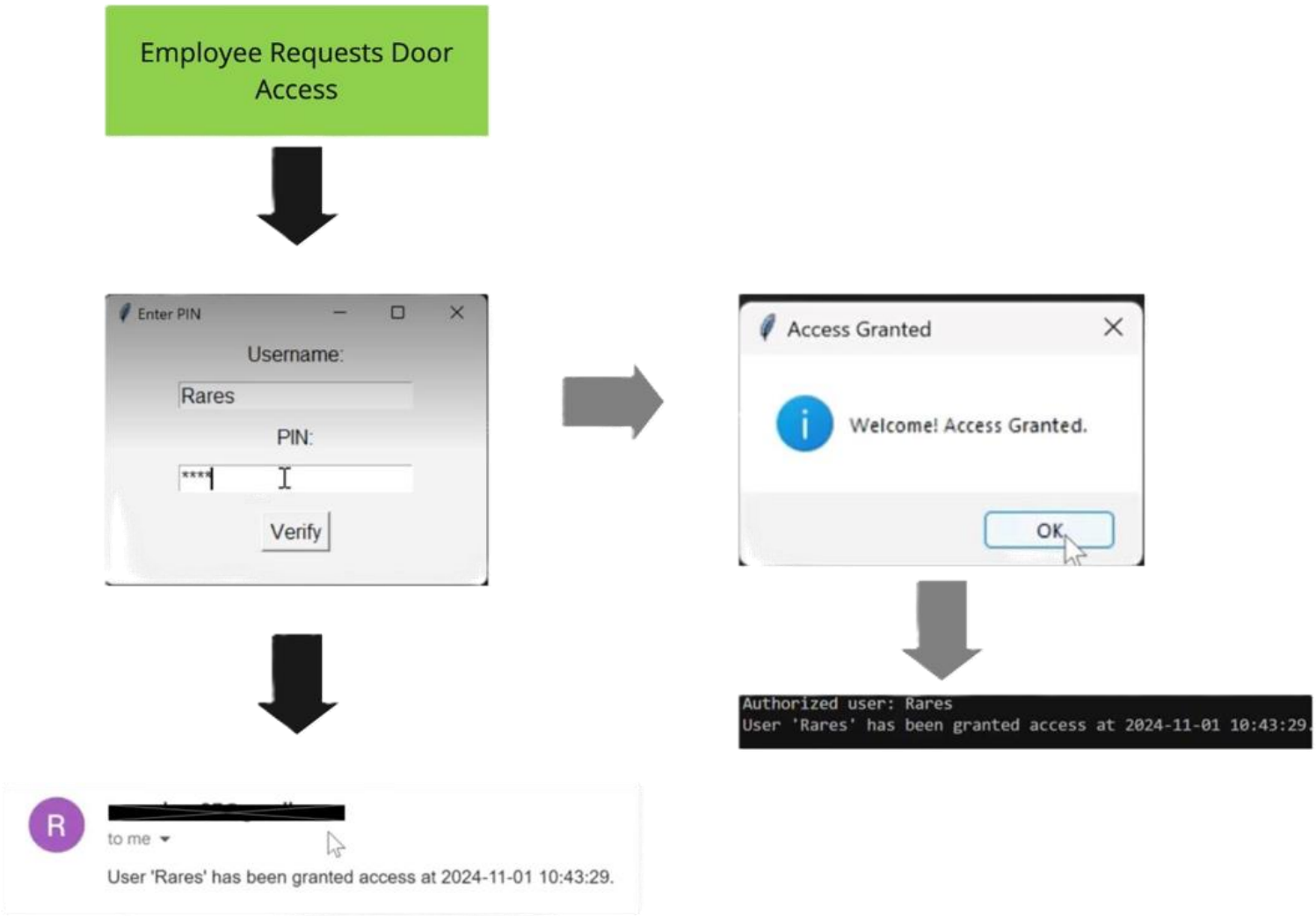

Figure 1: Prototype of When Access is Granted.

Figure 2: Prototype When Access is Denied.

Prototype Test Plan

Overview

This prototype system is a facial recognition-based access control system with PIN verification, which captures video evidence upon unauthorized access and notifies authorized users via SMS and email. The test plan aims to verify functionality, accuracy, performance, and reliability.

1. Objective

The objective of this test plan is to:

- Ensure that the system accurately recognizes authorized users.
- Confirm that unauthorized access triggers the notification system correctly.
- Verify the functionality and reliability of notification mechanisms.
- Validate performance and usability under different environmental conditions and device settings.

2. Test Scope

Testing will cover:

- User enrollment and PIN verification.
- Face recognition accuracy.
- Unauthorized access handling.
- Notification delivery (SMS and email).
- System behavior under various environmental conditions.
- Error handling and recovery.

3. Test Environment

- Hardware: Computer with webcam, supporting required resolution settings.
- Software: Python environment with OpenCV, Twilio SDK, face recognition library, and email handling.
- Accounts: Twilio account for SMS notifications, email server for email notifications.

4. Test Cases

4.1 User Enrollment

Test Case ID	Test Case Description	Steps	Outcome
1.1	Add a new authorized user with PIN and photo	Add name, PIN, phone number, email, face photo	User is added to the database successfully
1.2	Add a user without a face photo	Leave the face photo field blank during user enrollment	System prompts user to upload a valid face photo
1.3	Add a user with an invalid phone number format	Input name, PIN, invalid phone number, email, face photo	System rejects invalid phone format
1.4	Re-enroll an existing user	Try adding a user with the same name and details as an existing user	System prevents duplicate entries

4.2 PIN Verification and Access Control

Test Case ID	Test Case Description	Steps	Outcome
2.1	Verify access with correct PIN	Enter correct PIN for a registered user and present their face	Access is granted and user notifications are sent
2.2	Verify access with incorrect PIN	Enter incorrect PIN for a registered user and present their face	Access is denied, no notifications are sent
2.3	Verify access with unregistered user's face	Enter any PIN and present an unregistered user's face	Access is denied, system records a video

4.3 Face Recognition

Test Case ID	Test Case Description	Steps	Outcome
3.1	Recognize a registered user with correct PIN	Present face of an enrolled user after entering the correct PIN	User is recognized, access is granted
3.2	Attempt recognition with incorrect PIN and authorized face	Enter incorrect PIN for a registered user, then present that user's face	Access is denied
3.3	Attempt recognition with an unregistered face	Present an unregistered face with any PIN	System denies access, captures a 3-second video
3.4	Recognize a registered face after 5 seconds	Present the face of an enrolled user after a 5-second delay	Access is denied, unauthorized access is recorded

4.4 Unauthorized Access Notification

Test Case ID	Test Case Description	Steps	Outcome
4.1	Trigger unauthorized access alert via SMS	Enter any PIN with an unregistered face in front of the camera	SMS notification is sent to administration
4.2	Trigger unauthorized access alert via email	Enter any PIN with an unregistered face in front of the camera	Email notification with video attachment is sent
4.3	Test with low-resolution video attachment	Enter any PIN with an unregistered face and set camera to low resolution	Email is sent with low-resolution video
4.4	Test video attachment size limit	Enter any PIN with unregistered face; verify video file size for attachment compatibility	Video file size is within attachment limits

4.5 Notification Reliability and Delivery

Test Case ID	Test Case Description	Steps	Outcome
5.1	Verify SMS notification delivery to registered phone number	Trigger authorized access alert for a user with verified phone number	User receives SMS promptly
5.2	Verify email notification delivery	Trigger authorized access alert and check email delivery	Email is received promptly with correct details
5.3	Test notification failure handling	Disconnect from network and trigger authorized access alert	System logs error and retries
5.4	Notify multiple users	Add multiple users with different contact details, trigger authorized access	All registered users receive notifications

4.6 Performance and Environmental Tests

Test Case ID	Test Case Description	Steps	Outcome
6.1	Test face recognition under varied lighting conditions	Test recognition in bright, dim, and uneven lighting	System performs accurately under all conditions
6.2	Test response time for unauthorized access	Present unregistered face; measure time until notification	Notification is sent within acceptable response time
6.3	Test with high-resolution setting	Set camera to Full HD, trigger unauthorized access	System records video successfully, no lag
6.4	Test system behavior with camera unavailability	Deactivate camera, start recognition attempt	System logs error, alerts user

4.7 Error Handling and Recovery

Test Case ID	Test Case Description	Steps	Outcome
7.1	Handle database connection failure	Simulate database unavailability during recognition	System logs error and denies access
7.2	Handle email server unavailability	Disconnect from email server, trigger notification	System retries sending email or logs error
7.3	Handle Twilio SMS service unavailability	Disconnect from SMS service, trigger notification	System retries sending SMS or logs error
7.4	Handle invalid video format	Modify video format settings to unsupported type, trigger recording	System logs error and alerts user

5. Acceptance Criteria

- The system accurately grants access to registered users and denies access otherwise.
- Notifications are sent reliably within acceptable time frames.
- Video evidence for unauthorized access is recorded clearly.
- The system recovers gracefully from common errors or connectivity issues.

6. Resources

- Personnel: Team members, peers from other teams (for feedback).
- Tools: Twilio API for SMS, email server configuration, webcam with configurable resolution.
- Test Data: Sample face images, valid/invalid phone numbers, email addresses, and PINs.

7. Schedule

Testing will proceed over a span of 1-2 weeks:

- **Days 1-3**: User enrollment and PIN verification.
- **Days 4-6**: Face recognition accuracy and notification tests.
- **Days 7-10**: Performance, environmental, and error-handling tests.

Analysis

This prototype currently has two critical systems, the first being the facial recognition system, and the second being the notification system. Both systems are necessary to fulfil the basics of our restricted security alerting system. Specific aspects of each system are needed to work optimally.

The facial recognition system needs to operate with high levels of accuracy. It needs to be able to process the face and correctly assign it to the correct employee. This is required to make sure there is a way to verify the other information coming enter the network, such as a pin being entered. If this system fails there is no way to verify the information, preventing the ability to restrict specific areas of the enterprise. Additionally, if this system is lagging it can increase the chances of people entering restricted areas. Since the system will have delays and the person can enter during the lagging periods. We tested this system to ensure accuracy by running the camera multiple times with a variety of people using the same pin.

The notification system needs to operate efficiently. The notification must be sent to the administrator in a timely manner, along with the necessary information. The notification system is responsible for collecting the employee pin and face identification data. If this system were to fail, there would be no way for the administration to prevent restricted access attempts. There would be a serious concern for safety in the enterprise. Having the system send a photo and time stamp to the administrator makes more informed decisions in responding to these events.

Comments and Feedback

Client Feedback

During Client Meeting 2 we presented our final project idea. The client, Shabodi, provided feedback that helped us develop our first prototype. Their feedback included reducing the number of systems needed to define entrance (example: removing card access). As well as focusing on using face recognition as an authentication system paired with Subscriber Identity Module (SIM) card location. The client also noted how a phone can do most of what we are aiming to do, and recommended we consider using SIM cards to open doors as proof of access. They emphasized the importance of using NetAware and how they would like a product to demonstrate their network capabilities. The client also stated it could be advantageous to send a photo from the cameras to the administrator when there is a restricted access attempt.

User Feeback

Keeping the client's recommendations in mind we produced our first prototype, as discussed above. We presented our prototype to prospective users to gather more feedback on the design and utility. The users mentioned how they would like to have the location displayed as information for the administrator in the notification. The users also brought up concerns about multiple people entering a room at once but only using one person’s access information.

Updated Target for Specifications and Detailed Design

1. Facial recognition

- When the face recognition camera can't recognize a face, it will take a video and send it to admin.
- Use Shabodi latency and bandwidth API to improve video quality of security camera signal.
- Being able to recognize multiple faces that are in a directory (expand database)
- Being able to send the location when the camera does not recognize a face.
- Improve camera resolution (up to 1920x1080p)
- Add external(s) camera(s)

2. Tracking

- Make sure that SIM card tracking is accurate to the meter
- SIM tracking must update location every 10 seconds.
- Code must work 90% of the time.
- Uses location API from Shabodi

3. Additional Safety Measures

- Add a log system with a log rotation mechanism

Updated BOM

To reflect the change in direction of the project we have updated the BOM. The testing for the project will be done on a laptop or a phone. The product itself will only require a camera to be fully operational for the inquiring Enterprises.

PART NUMBER	PART NAME	DESCRIPTION	LINK	QUANTITY	UNITS	SUPPLIER / MANUFACTURER	UNIT COST	TOTAL PART COST
1	OpenCV	Face Recognition API	OpenCV	1	NA	OpenCV	$0	$0
2	PIP libraries	Library for python	Pip	1	NA	PIP	$0	$0
3	Shabodi	Sandbox	Shabodi	1	NA	Shabodi	$0	$0
4	Twilio	Notification API	Twilio	1	milliseconds	Twilio	$0	$0
5	Shabodi Location	API	Shabodi	1	coordinates	Shabodi	$0	$0
6	Shabodi Bandwidth	API	Shabodi	1	bits per second	Shabodi	$0	$0
7	Shabodi Latency	API	Shabodi	1	milliseconds	Shabodi	$0	$0
			TOTAL PARTS	7			**TOTAL**	$0.00

Prototyping Plan

Prototype 2

From the feedback we have outlined a set of goals for our next prototype. These goals are:

- Adding multiple people to the directory
- Sending a video (~ 3 seconds) with the unauthorized user to the administrator
- Adding SIM card location tracking
- Add SIM card door opening abilities
- Sending location of the SIM card to the administrator
- Add audible alert

We plan to use prototype 1 as the basis for these modifications. Aiming for a more well-rounded product that provides the maximal amount of information to the administration. Each of these new additions can be tested by test methods from the previous deliverable, such as speed in milliseconds and accuracy in terms of image recognition and centimeters.

Execution Plan

<table>
<tr><th></th><th>Week of October 28th</th><th>Week of November 4th</th><th>Week of November 11th</th><th>Week of November 18th</th><th>Week of November 25th</th></tr>
<tr><td>Louis-Philippe</td><td rowspan="2">Access Shabodi APIs to do the phone tracking.</td><td rowspan="2">Tracking case with boundary definition must be roughly coded. With at least 1-2 API’s.</td><td rowspan="3">Finish up both Tracking case with boundary definition And Security camera subsystems to combine for the door access sub-system</td><td rowspan="3">Door access should be roughly coded.</td><td rowspan="3">All systems must work perfectly for design day.</td></tr>
<tr><td>Emma</td></tr>
<tr><td>Rares</td><td>Security camera prototype is done</td><td>Security camera should incorporate at least 2-3 API from Shabodi</td></tr>
</table>

Conclusion

In conclusion, our first prototype uses python code on visual studio to simulate are facial recognition part of our final solution. The testing of the prototype worked as intended and helped us learn what needs to be changed. For instance, the notification can receive a video instead of a photo to better depict the unauthorized user. Additionally, as a team we agreed on the final BOM, and prototyping schedule. With the first prototype done and our plan complete we are one step closer to our final design.

References

1. ISO/IEC. *ISO/IEC 19795-1:2006: Information technology — Biometric performance testing and reporting — Part 1: Principles and framework*. International Organization for Standardization, 2006.

2. Zhao, W., Chellappa, R., Phillips, P.J., & Rosenfeld, A. *Face Recognition: A Literature Survey*. ACM Computing Surveys (CSUR), 2003, vol. 35, no. 4, pp. 399–458.

3. OpenCV. *OpenCV Documentation*. Available at: https://docs.opencv.org/. https://docs.opencv.org/.

4. National Institute of Standards and Technology (NIST). *Special Publication 800-63B: Digital Identity Guidelines – Authentication and Lifecycle Management*. U.S. Department of Commerce, 2017.

5. OWASP Foundation. *OWASP Testing Guide v4*. Available at: https://owasp.org/www-project-web-security-testing-guide/v4/.

6. Twilio Inc. *Twilio API Documentation*. Available at: https://www.twilio.com/docs.

7. Klensin, J. *RFC 5321 - Simple Mail Transfer Protocol*. Internet Engineering Task Force, 2008. Available at: https://www.rfc-editor.org/rfc/rfc5321.html.

8. Naik, K., & Tripathy, P. *Software Testing and Quality Assurance: Theory and Practice*. Wiley, 2008.

9. Kaner, C., Falk, J., & Nguyen, H.Q. *Testing Computer Software*. Wiley, 1999.

10. National Institute of Standards and Technology (NIST). *NIST IR 7822: Performance of Face Recognition Algorithms*. U.S. Department of Commerce, 2012.

11. IEEE. *IEEE 2410-2021 - IEEE Standard for Biometric Open Protocol Standard (BOPS)*. IEEE Standards Association, 2021.

12. IEEE. *IEEE 829-2008 - IEEE Standard for Software and System Test Documentation*. IEEE Standards Association, 2008.

13. International Software Testing Qualifications Board (ISTQB). *ISTQB Foundation Level Syllabus*. Available at: https://www.istqb.org/.