GNG 1103

Design Project User and Product Manual

The Gask-it

Submitted by:

GASCK, Group 15

Cedric Hoedl, 300363134

Salem Osawere, 300447828

Annie Zhao, 300409935

Keaton Luttrell, 300427663

December 3rd, 2024

University of Ottawa

Table of Contents

1 Introduction

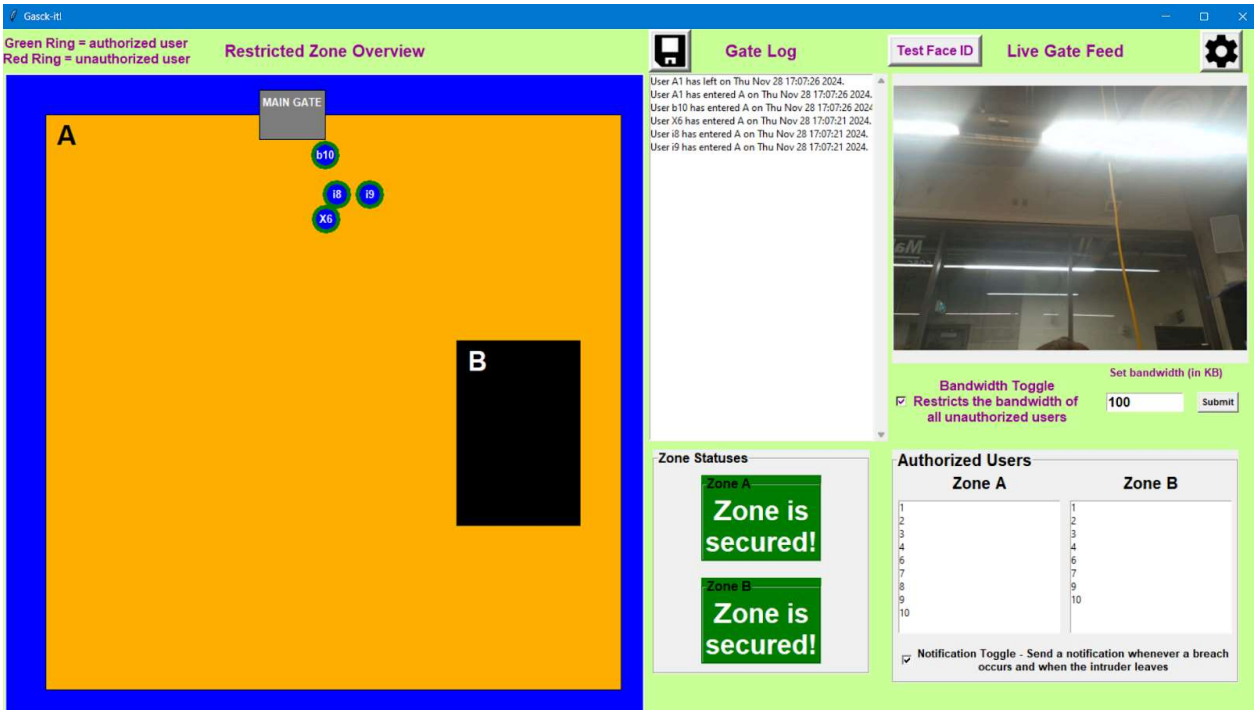
This User and Product Manual (UPM) provides the information necessary for operators to effectively use the Gasck-it and for prototype documentation. This document introduces the problem which this product solves and the various features which the product possesses. The document then provides a general walkthrough of the system and then in greater detail, how to use the system. The following section covers what actions the user should take in the case of an issue or error. Afterwards, product documentation, including how the final prototype was developed and technical calculations and design considerations are stated. The final section includes lessons learned and future additions, if given more time.

2 Overview

The problem is that personnel and machinery are entering spaces where they are unauthorized. This is important because there are safety and privacy risks, ex. physical safety, breach and exposure of data, etc.

The fundamental needs of the user are to use Shabodi's API, specifically the bandwidth API. This is necessary to restrict the bandwidth of unauthorized users within the restricted zone to ensure the security of the data within. The product needs to be able to identify and differentiate users, determining if they are authorized or unauthorized. If the identification system is bypassed, the system needs to be able to send an alert and detect location of the unauthorized user within the zone.

Our product is easy to use and contains a multitude of features with adjustable settings. The product uses two forms of identification, SIM card and face scanning, increasing the level of security and lowering the chance of an undetected bypass. The system records a log of all users who enter and exit the zone(s), including the time of entry and exit. This log can then be converted into a spreadsheet format. The level that the bandwidth is restricted to can be adjusted to as low as 1 KB/s. Users can be easily and quickly added or removed from the list of authorized users.



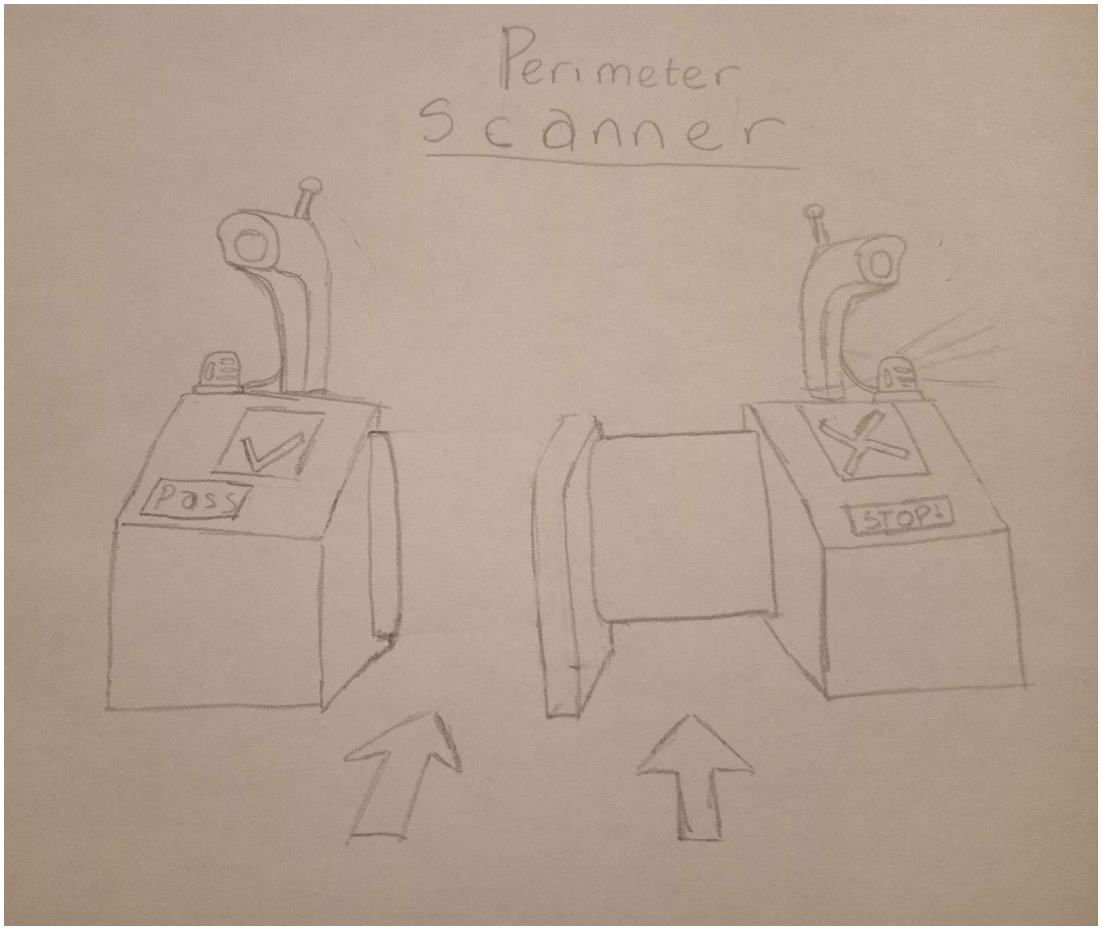
The product will display users within the restricted zone, their location, and whether they are authorized or not. It will include a log of users who have entered and exited the zone, and whether each zone is secured or not. The product includes a live feed of the entrance gate, and a list of authorized users for each zone. The level that the bandwidth is restricted to and the list of authorized users can be changed or adjusted. The log of users can be exported and converted into a spreadsheet form.

2.1 Cautions & Warnings

Users should be aware of the various cooperative and uncooperative systems in the Gasck-it. This would include understanding the functionality/purpose of the gate and the SIM tracking. If/when the system is breached by an individual, a SMS notification will be sent to the operator of the system, which can be further expanded onto sending directly to security or law enforcement. For further explanation on user access considerations consult sections 3.2, 4.6, and 4.9.

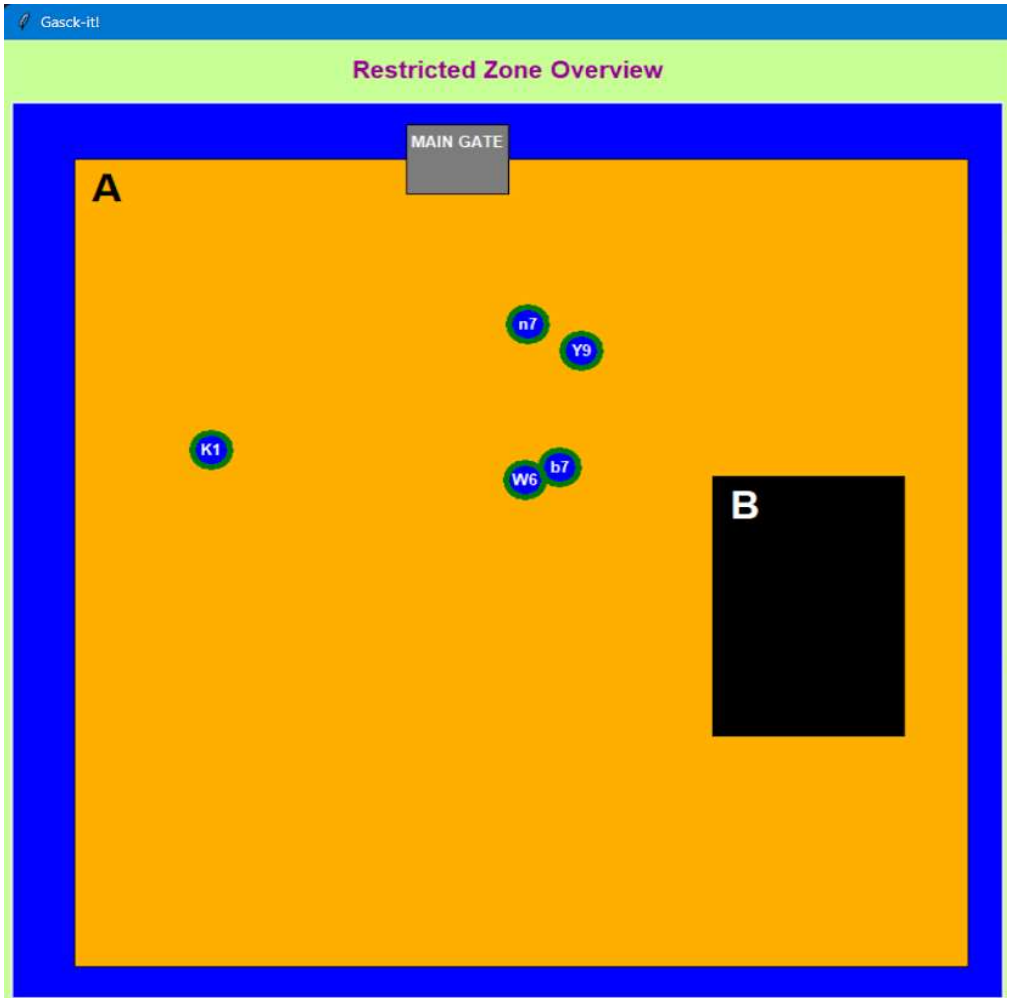
3 Getting started

The Gasck-it's revolutionary design revolves around two main components to provide security to a given area: the entry gate system, and the SIM tracking location system. The former uses facial recognition software to detect whether a user is or is not allowed through.



Prototype of gate-entry system as a part of the Gasck-it.

The latter system uses Shabodi's location API to track users in a given zone-area



Prototype of UI showing restricted zone area

3.1 Configuration Considerations

Inputs and configurations needed are simple, SIM card is needed to have permitted enabled tracking registered with the system. Presenting your face to the camera is required to achieve access based on if the facial scan is recognized. This causes the gate to open. If a breach occurs where an unknown SIM enters an area, the response by the system will be to restrict the user's bandwidth and send a SMS alert to the operator to warn of the breach.

3.2 User Access Considerations

Users permitted into any restricted zone need both a facial scan uploaded into the system, and their phone number to access permission with the SIM tracking function. To easily add a number to the

system, simply type it into the box in the settings bar and click “Add number”.

3.3 System Organization & Navigation

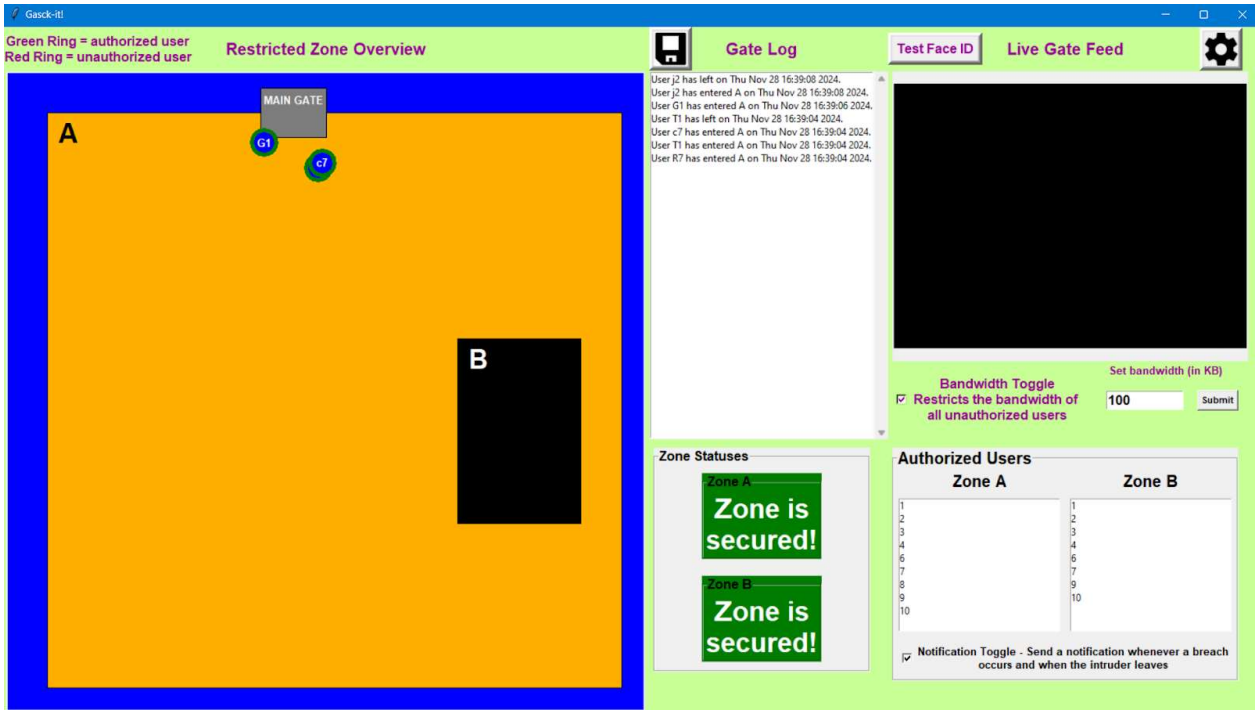
The ‘home page’ of the user interface provides all primary upfront knowledge displayed at all times. In order to access deeper functions such as adding users phone numbers or restricting users access to areas; click the settings cog at the top right. For active facial scan in order to identify as a known or unknown user: click the button labelled “Test Face ID” and present your face.

3.4 Exiting the System

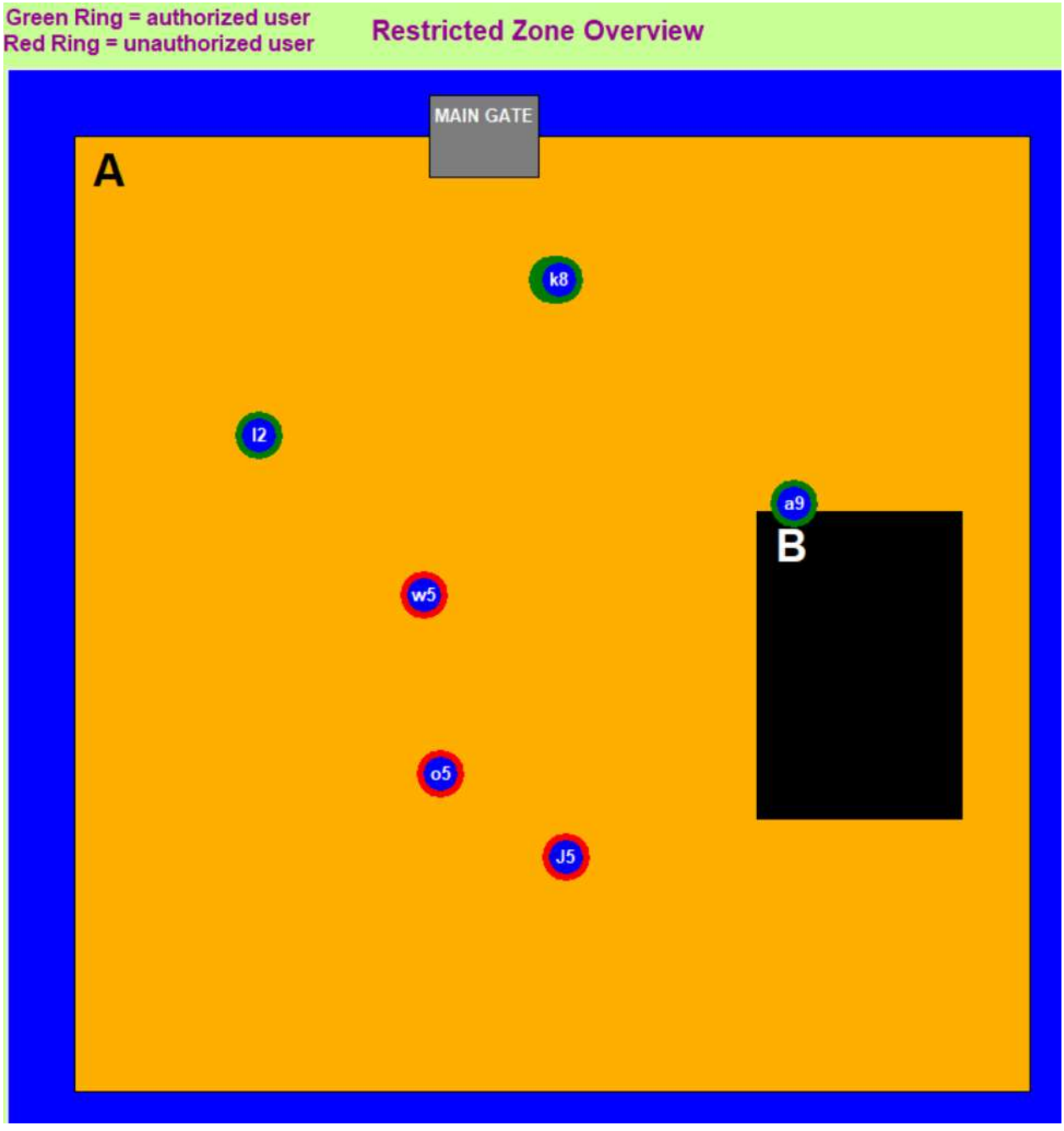
In order to close the system, click the [X] button top right of the program. Make sure to save the entry log data before closing the application if you want the data to be stored.

4 Using the System

The following subsections provide detailed, step-by-step instructions on how to use the various functions and features of the Gasck-it.

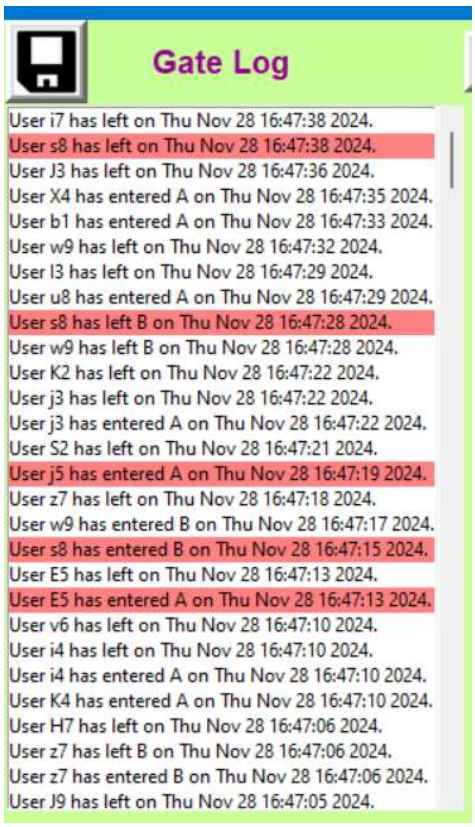


4.1 Zone Overview



This is an overhead view of the restriction zones. Each circle represents a UE where green represents authorized users and red unauthorized users. Each gate will be represented by a gray block and will be labeled. This allows a real time updating system of the users moving within the zone permitting administrators to track the movement of employees or intruders.

4.2 Gate Log



The gate log tracks the entrance and exit of each uE. This marks down the time, the ID and the zone in which the UE traverses. The log highlighted in red represents an unauthorized breach. It will be red when they enter as well as when they leave. The gate log information can be saved into an excel sheet by clicking the save icon represented by the floppy disk.

Once saved, the file will be found in the same directory as the Gasck-it software and can then be used independently for archiving.

4.3 Zone Statuses

This gives a quick visual indicator if the zone has been breached or not. If an unauthorized user is within the zone it will turn red to warn the administrator.

Both zones are safe:

Zone A is breached:

4.4 Live Gate Feed

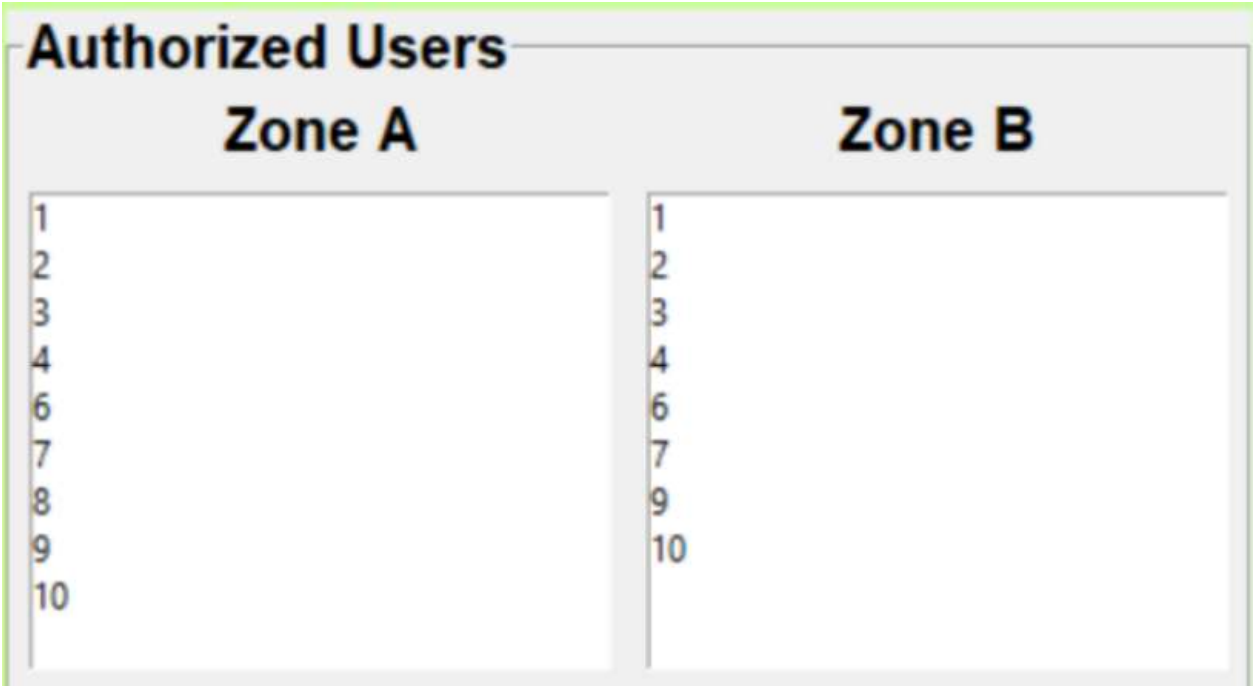
The live gate feed is the camera footage produced from the gate streaming onto the application.

4.5 Bandwidth Toggle

This feature restricted the bandwidth, the internet connection, of unauthorized users within the zone when toggled on. This will prevent them from accessing online resources and to stream or upload documents. You may modify how strict you would like to set the maximum bandwidth for all restricted users or turn it off by toggling the feature off.

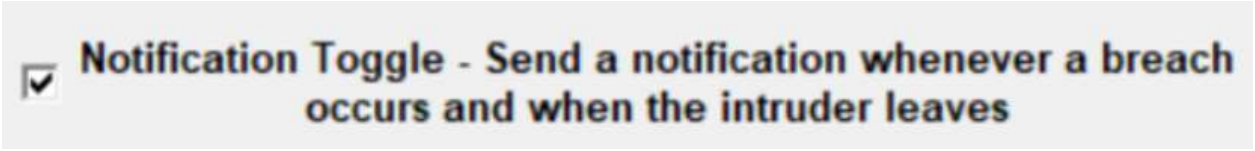
4.6 Authorized User List

This list of all authorized users for the zone. Note that this is not the list of users in the zone but simply who is allowed to access them.



4.7 Notification Toggle

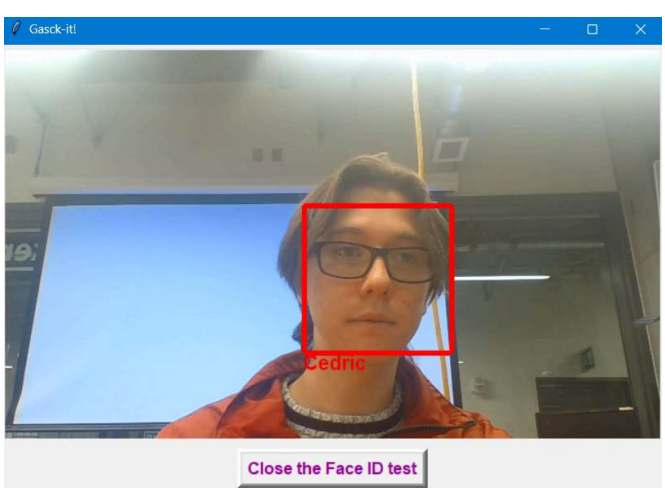
When turned on, a notification will be sent to the registered phone number (see section 4.9.3 for more details) whenever a breach occurs and when the unauthorized user leaves the zone. When toggled off, these notifications will not be sent.

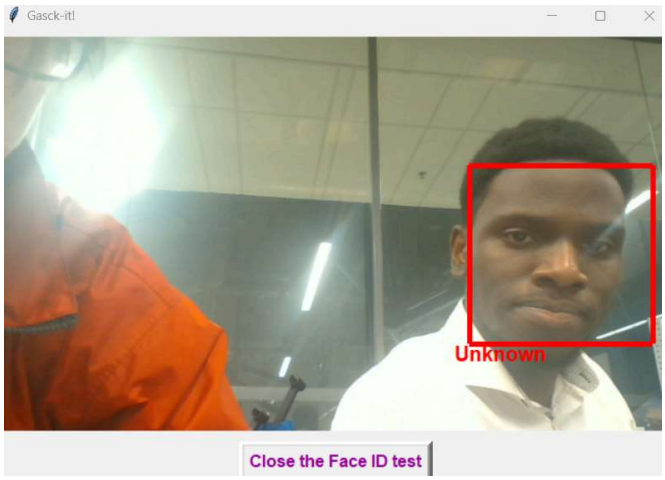


4.8 Face Recognition Test

By clicking the “Test Face ID” button top right of the program, it will open a separate window with working face recognition. All unauthorized users will be seen as “Unknown” while registered users will have their name displayed. The program only scans the closest face. To add a user to the registered list you must take a clear picture of the face, add the image in the same directory as the software, in the CAMERA AND FACE RECOGNITION section of the code in the faceReco class, add the name of the user and make sure the file name is correctly written as shown below. Restart the program and the user will now be registered.

```
cedric_image = face_recognition.load_image_file("cedric.jpg")
cedric_face_encoding = face_recognition.face_encodings(cedric_image)[0]
```





4.9 Settings Menu

To access the settings menu you must click the cog wheel icon top right of the screen which will open the settings menu.

4.9.1 Adding Users

Select the zone you would like to change by clicking “Change A” or “Change B” button then enter the user ID you would like to add and then click the “add ID” button. The user will then be added to the authorized user list of the zone you selected.

4.9.2 Removing Users

Select the zone you would like to change by clicking “Change A” or “Change B” button then enter the user ID you would like to add and then click the “Remove ID” button. The user will then be removed from the authorized user list of the zone you selected.

4.9.3 Changing Registered Number

In the entry box above the “Add number” button, you can add your phone number. A confirmation will be sent to that number to register it. Once added, click on the drop down menu, the phone number list, and select the desired number. Notification alarms will now be sent to that number.

5 Troubleshooting & Support

5.1 Error Messages or Behaviors

For display errors, we are aware of an issue if you authorize a user to a zone which he is already in and marked unauthorized, his icon will remain “red” until he leaves. He will still be treated as an authorized user but since he was initially taken as an intruder, the program does not update his color settings until after he leaves.

For program error, if you repeatedly click the “Test Face ID” button, the program will stop responding as this will make many duplicates of this high demanding window.

For errors regarding the bandwidth restriction or location detection, make sure you are connected to the shabodi’s virtual private network (VPN) and that your provider has not blocked the port 2222 for them to work.

For errors within the program, the best approach is to do a quick restart of the program to reset it. If it is an unknown library error make sure to write “pip install” followed by the name of the library to download it. You may also need to write “py -m pip install” followed by the name of the library if the previous method does not work. If a different display error occurs please consult section 5.3 Support to inform Gasck of this error.

5.2 Maintenance

Check for regular updates from Gasck to make sure you have the latest model and to make sure your device meets required specifications to run the program.

5.3 Support

If errors persist, contact GASCK call 1-800-123-4567 or email gasck.support@gmail.com for additional help or clarification. If there is an error with the API’s, please contact developer.support@shabodi.com. For Gasck related emails, start the email with “ PROBLEM: “ and within the email include the version of the software you are using as well as an image of the error obtained.

6 Product Documentation

The program was created using python 3.11.5 and the Tkinter interface. The main logic of the simulation is described below.

The program randomly generates users at the appointed gate and logs the time of entry. If you are testing the program without the location API, the movements are semi-randomly generated. The gate will react to the user according to its list of authorized users sending a notification if breached and allowing authorized users in. For each user in the zone, a respective User object is created and stored in the inZone list to be used in other sections of the code. Every 0.05 seconds, the location and time of the user gets updated. Depending on the new location, the program checks if they are still in the zone if they have entered a new one and reacts accordingly. This simulation runs continuously without break since a new user has a 1/65 chance to generate every 0.05 seconds.

For further information on each function described in section 4 of the manual and more detail in the back end code of this program, please refer to the code documentation. This documentation separates each section of code to their respective part describing what it does and how it does it. This will allow for a more in-depth code based understanding of the software in the needs to modify, improve or add features.

7 Conclusions and Recommendations for Future Work

Lessons Learned

1. **Understanding User Requirements:** A clear alignment with Shabodi's sandbox and API usage emphasized the importance of focusing on functional and demonstrable network-aware applications. The ability to deliver practical utility aligning with the clients' needs.
2. **Technical Integration Challenges:** Encountering API integration issues highlighted the need for robust testing environments and early troubleshooting to avoid delays.
3. **Importance of Simplification:** Keeping the project within feasible and comprehensible will give us clearer goals to shoot for and save more time.

Prototype Work Summary

1. **Prototype 1:** Focused on validating logic and the ability to identify and track users using simulated IDs. Key success was storing user information and demonstrating basic functionality.
2. **Prototype 2:** Tested breach detection and notification systems, shows alert reliability and response time.
3. **Prototype 3:** Integrated location tracking, real-time alerting, and comprehensive breach logging. Final tests ensured detection accuracy and system reliability.

Future Work Recommendations

1. **Expand API Integration:** Incorporate more of Shabodi's APIs to explore additional capabilities, such as location and jitter reduction.
2. **Enhance Realism:** Shift from simulations to hardware integration (e.g., actual SIM cards, a physical gate) to validate the systems ability under real-world conditions.
3. **Improve User Interface:** Create a more intuitive dashboard or GUI for administrators to interact with the system efficiently.
4. **Optimize for Scalability:** Develop methods to handle larger datasets, multiple restricted zones, and diverse user profiles to cater to enterprise-level requirements.
5. **Conduct Long-Term Testing:** Simulate extended operation scenarios to test durability, reliability, and system adaptability under varying conditions.

If Given More Time

- **Integrate Physical Hardware:** Build a working prototype with live facial recognition and physical gates for more practical demonstration.
- **Expand Testing Scenarios:** Explore edge cases such as system responses under network congestion or hardware failures.

- **Include Advanced Features:** Add real-time data visualization, integration with enterprise management systems, or advanced reporting tools.
- **Focus on Security Enhancements:** Implement encryption protocols to protect sensitive data transmitted via APIs and the system.

8 Bibliography:

1. Stack Overflow. (2018, January 25). *Python threading: How to repeatedly execute a function in a separate thread*. Stack Overflow. https://stackoverflow.com/questions/48049861/python-threading-how-to-repeatedly-execute-a-function-in-a-separate-thread

2. Geitgey, A. (n.d.). *facerec_from_webcam_faster.py*. GitHub. https://github.com/ageitgey/face_recognition/blob/master/examples/facerec_from_webcam_faster.py

3. OpenCV Forum. (2020, October 23). *Display video camera in two tkinter windows*. OpenCV Forum. https://forum.opencv.org/t/display-video-camera-in-two-tkinter-windows/2590

4. Canva. (n.d.). *Canva: Visual suite for everyone*. Canva. https://www.canva.com

   *For creation of GASCK logo

9 APPENDIX I: Design Images

Figure 1: The image used to access the settings.

Figure 2: The image used to save the gate log into an excel sheet.

Figure 3: The Gasck logo