Functional Specification

Year: 2019 **Semester:** Spring **Team:** 2 **Project:** Guard DAWG System
Creation Date: January 13, 2019 **Last Modified:** January 18, 2019

Member #1: Evan Miller **Email:** mill1576@purdue.edu
Member #2: Yash Nain **Email:** ynain@purdue.edu
Member #3: Ian Sibley **Email:** isibley@purdue.edu
Member #4: Viktoryia Zhuleva **Email:** vzhuleva@purdue.edu

1.0 Functional Description

This is a smart-lock device, meant to recognize registered users and allow them access through a door. This device takes snapshots of a user's face and transmits them over wifi to a server with more computing power, which will run a facial recognition algorithm on the largest face in the frame to determine if the user is authorized to unlock the door. A signal is sent back to the system, where the microcontroller will then determine whether or not to unlock the door.
Should the recognition algorithm fail to meet the required threshold or a secondary user that isn't registered in the system (i.e. a friend of the family that uses the system for their house) want to unlock the door, there is a number pad mounted to the system that will act as a secondary access point.
Finally, in the event of a failure of both systems, such as a power outage, there will be a physical key override.

2.0 Theory of Operation

In its idle state, the device will remain in a low-power mode until the user activates the recognition process, through a button press. When the user activates the system, the embedded camera will begin taking pictures at 4 fps. The device will use the pre-trained facial recognition FaceNet, or similar, to determine if the largest face found in the frame corresponds to an authorized user. The FaceNet network assigns a Euclidean distance score based on 128 feature vectors, comparing stored reference images to the input image. In order to be recognized by the network, roughly 75%* of the images must pass a Euclidean max distance of .52* over several seconds.

After a period of time, the network will determine whether the user is verified or unverified, or if it is indeterminate and the user needs to scan their face again. The Raspberry Pi will then send a signal to the microcontroller over Bluetooth, which will then send (or not send) a signal to the motor MOSFET.
If the network fails to verify an authorized user, or an unauthorized user wants to gain access, an authorized user can grant access by using a numeric password. The lock will have a row-column numeric keypad attached to it, as a secondary point of access. In the event both of these fail, then a physical door key can act as a mechanical override.

When the door is unlocked, it will remain unlocked for a period of time, until it locks again and the user needs to re-scan. Attached to the embedded electronics and door frame will be a Hall effect sensor and magnet, so that the door will not lock while it is still open.

*these values are subject to change due to empirical findings

3.0 Expected Usage Case

The Guard Dawg System will be a door mounted system suitable for residential and commercial properties. Once the system is mounted, it is designed to stay on the door and increase both security and ease of use over traditional lock and key implementations. The resident will be able to use his or her face as a key to unlock their homes eliminating the hassle of carrying around a physical key. The system has components facing the interior and exterior of a home, and as such is designed to be weather resistant.

The system can handle any number of registered users regardless of their age and physical attributes as long as they are in view of the mounted camera. If the camera fails to detect a registered guest, a numeric keypad is also mounted on the door. The key pad allows unregistered users to have access, for example if the resident is having guests over or is expecting a delivery.

Although we are targeting a young, tech-savvy audience interested in the promise of a connected smart home, the Guard DAWG system is a non-invasive product suitable for anyone. The system will require connection to a wireless network, which our target user is expected to have. The most common use case will be the user unlocking their home upon entry, an event which happens a handful of times every day on average.

4.0 Design Constraints

The list of design constraints includes such constraints as computational, electronic, thermal/power, mechanical, and economic.

4.1 Computational Constraints

The main algorithm will be required to find faces within a frame, and identify a previously registered face, while the keypad for the electronic override will rely on the use of a finite state machine. In order to minimize the size of the image to transfer over WiFi, the software will implement a facial cropping functionality from a pre-trained network available in OpenCV. At this moment, it hasn't been determined whether or not this will have a significant effect on the time required to run the algorithm, but this will be confirmed later on in the design process.

Since running the algorithm is expensive, for now, the process will be offloaded to a more powerful external resource, ideally with a much more powerful GPU. Throughout the initial prototyping phase, we will determine whether or not the Raspberry Pi 3 B+ will be able to run the algorithm itself.

4.2 Electronics Constraints

The design will utilize a Bluetooth transmitter/receiver, Raspberry Pi 3 B+ with heat sinks, a small embedded camera, a hall-effect sensor, some small embedded LED's, a push-button, some power electronic interfaces, and a power door latch handle. The required interfaces for the devices to the microcontroller will be UART, I2C, and SPI, depending on the exact configuration of the components selected for the final design. To protect the low-power microcontroller and Bluetooth modules, the board needs to have a DC-DC converter, since the motor runs on 24Vdc, while the embedded modules require ~5Vdc and very little current. In addition, to protect against feedback current from the motor to the embedded electronics, there will be a voltage regulator in case of an unexpected power surge.

4.3 Thermal/Power Constraints

Since the electronics are a self-contained system, they must be able to run on batteries if necessary. Therefore, the batteries must be able to supply enough current to run the Raspberry Pi (5V/2.5A) and microcontroller through USB. Therefore, to activate the most costly components of the design, the user must press a push-button to turn them on for a few seconds, therefore drastically saving on the overall power requirements needed for the design. To perform the processing of the face for user verification, or to send the image to an external resource for processing, the Raspberry Pi must utilize its GPU, which will require some heatsinks for itself and the CPU to make sure they don't overheat and damage the other components.

4.4 Mechanical Constraints

Since this is a door lock system, the packaging must be able to withstand the normal wear and tear from its environmental surroundings, such as wind, rain, dust, and other natural weather occurrences. In addition, it must be able to withstand a certain amount of mechanical force, in case an unauthorized user is attempting to break the lock in order to gain access behind the door. Therefore, the mechanical packaging standards must meet at least an IP65 rating, meaning that it should be able to protect against low pressure water jets (to simulate storm conditions).

4.5 Economic Constraints

The cost of the entire system is calculated based on the cost of individual components that go into it. Such components include the camera, keypad, microcontroller, Wi-Fi chip, motor and system-compatible lock. The motor has 24V DC operating voltage, while the microcontroller requires 5V and the rest of electronics range between 5V and 3.3V operating voltage. The system (without the motor) needs a 5V power supply. The motor would need to be powered with a separate 25V~ power supply. Assuming the maximum current requirement to be 100 mA, the maximum power consumption is going to be 2.5W. According to the Nest smart lock spec sheet, it "requires 4 AA batteries (included). Battery last for 1 year. If batteries become depleted, user can unlock the door using a 9V battery for power" (Nest). Our system would need a similar power supply approach which will require battery recharging/change with the same frequency as Nest system - 4 AA batteries a year.

4.6 Other Constraints

N/A

5.0 Sources Cited:

Keras Documentation. [Online]. Available: https://keras.io/applications/#vgg16. [Accessed: 18-Jan-2019].

K. Simonyan and A. Zisserman, *VGGFace2*, 08-Oct-2014. [Online]. Available: http://www.robots.ox.ac.uk/~vgg/research/very_deep/. [Accessed: 18-Jan-2019].

D. Sandberg, "FaceNet," *GitHub*, 16-Apr-2018. [Online]. Available: https://github.com/davidsandberg/facenet. [Accessed: 18-Jan-2019].

F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," *[astro-ph/0005112] A Determination of the Hubble Constant from Cepheid Distances and a Model of the Local Peculiar Velocity Field*, 17-Jun-2015. [Online]. Available: https://arxiv.org/abs/1503.03832. [Accessed: 18-Jan-2019].

S. Skúli, "Making your own Face Recognition System – freeCodeCamp.org," *freeCodeCamp.org*, 11-Jan-2018. [Online]. Available: https://medium.freecodecamp.org/making-your-own-face-recognition-system-29a8e728107c. [Accessed: 18-Jan-2019].

"IP Ratings (Ingress Protection)," *IP rating table*. [Online]. Available: https://www.mpl.ch/info/IPratings.html. [Accessed: 18-Jan-2019].

"Nest x Yale Lock Spec Sheey," *HomeDepot*. [Online]. Available: https://images.homedepot-static.com/catalog/pdfImages/b1/b108b63a-28e2-41fb-9ed7-7578668f9598.pdf. [Accessed: 18-Jan-2019].

5.0 Appendix

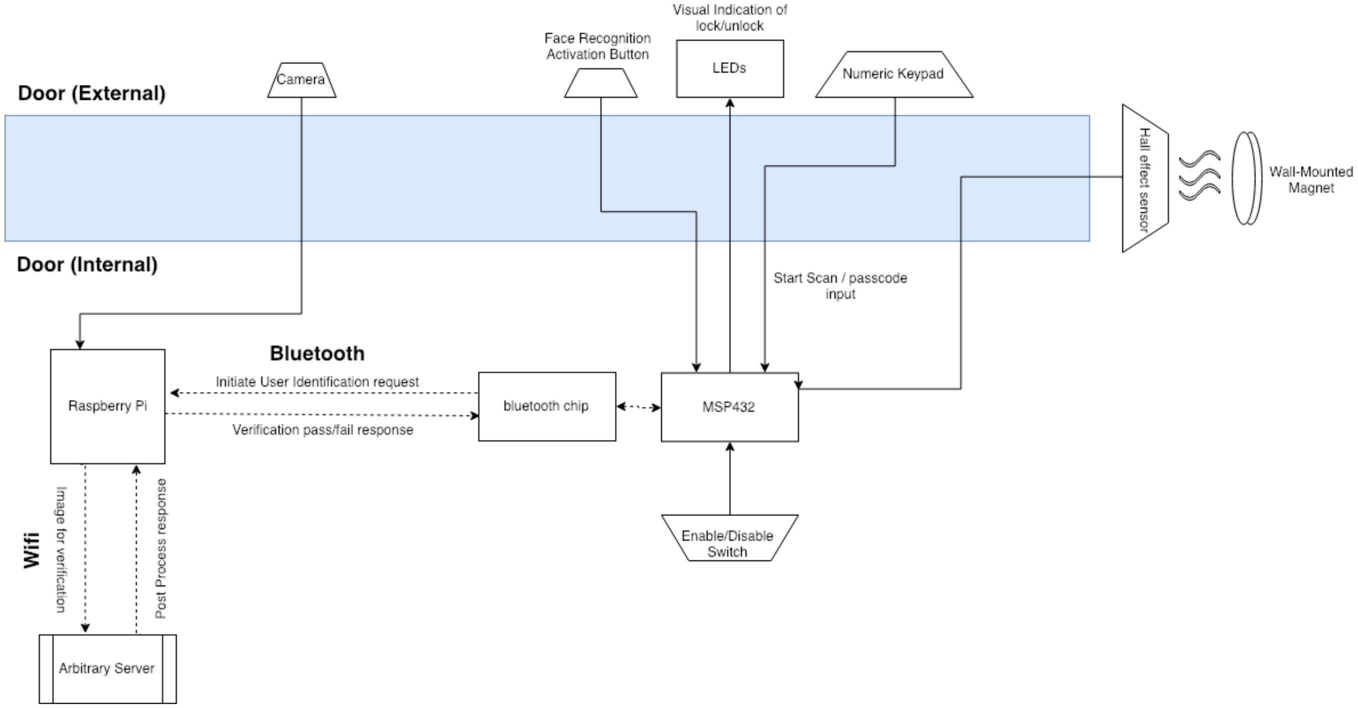

Figure 1: Functional Block Diagram