Anti-Theft Package Security System

Team 36 - Nikhil Mehta, Irfan Suzali, Abishek Venkit

ECE445 Project Proposal, Round 2 - Spring 2020

TA: Shuai Tang

Table of Contents

1 Introduction

1.1 Objective

Ordering packages online is extremely commonplace these days, with over 87 billion packages shipped worldwide in 2018 [1]. However, the added convenience can also have drawbacks. One of the risks of ordering a package online is theft. When packages are dropped off outside of an unprotected residence, it is easy for a thief to steal it without being caught. 36% of Americans have experienced package theft, and the average cost to replace a stolen package is $109. This is costly and inconvenient for the customer and supplier [2]. The package delivery industry is incredibly large and growing at a fast pace, which tells us that this problem is significant, and an affordable, reliable, and secure solution would help a lot of people protect their packages from theft.

Our solution will implement computer vision to identify when packages are delivered and when they are picked up. This system will use a camera that is pointed at the location of delivery. The package will be delivered within a general area in the field of view of the camera. Once the package is delivered, the computer vision algorithm will detect its presence, and track it to ensure it stays in full view of the camera. The system will also notify the user via text using WiFi when it detects that a package has arrived. If anyone tries to move it, or if the package becomes obscured from the camera, an alarm will sound, the user is notified, and a short video recording will be taken of the offender. Furthermore, if anyone moves the actual camera system or tries to cover the camera, the alarm will sound as well. In order to disarm the alarm, the actual package recipient must show the camera a unique QR code. This will disable the alarm from triggering for a moment, allowing the user to pick up their package. In order for this system to work at night, there will also be a motion sensored spotlight to illuminate the entryway.

This implementation will use a computer vision object identification algorithm running on the Raspberry Pi. This model will be trained on various standard package shapes and sizes from all angles, to ensure that the system can recognize any package that is delivered. *The Raspberry Pi will only be used for the CV algorithm and storage system, and will transfer data to a separate microcontroller*. This microcontroller will communicate with the Raspberry Pi, and the alarm, WiFi, and spotlight systems. The alarm system will require speaker/audio circuitry, which includes a digital-to-analog converter, amplifier, and speaker. The notification system will require a WiFi module and external server to push text messages to the user. The spotlight system will require a PIR motion sensor, ambient light sensor, and lighting circuitry. The entire device will need a power supply, and voltage regulation.

1.2 Background

Package security is a large industry with several existing solutions on the market. However, despite the growing adoption rate of home security systems, only 17% of homes have some type of security system installed [3]. There are several reasons that people don't use home security systems. This includes the fact that they cost too much, they are difficult to use, and possibly infringe on privacy [4]. Related to the concern over high cost, many

home security systems are fully featured, and serve many purposes beyond just package security. This is great if you want all of these extra features and can afford it, but there are few options if you only want a way to secure your packages. Our system will also be easy to use, with a simple notification system, and an easy way to disarm your system when you want to retrieve your package. The hardware will all be in one package, which will be easy to install and low cost.

Another alternative package delivery solution aimed at reducing theft is choosing to ship your package to a package locker, like a PO box, or the more recent Amazon Locker [5]. This allows you to secure your package in a remote facility until you unlock it and pick it up. This solution is less than ideal as well, because it forces you to travel to a separate destination everytime you want to pick up a package. A more modern and techy solution is using smart locks to allow delivery inside your home, like the Amazon Key [6]. This solution eliminates the risk of package theft after delivery, but introduces a new concern of letting someone into your home to deliver your package. These smart lock systems are also expensive and require installation into your door.

This project is an alternate solution to a problem proposed by Spring 2018 Team 9 [7]. Their original solution detected packages using a doormat with weight sensors, and detected potential thieves through the use of a PIR sensor. Their system would give a warning if someone approached the package and would take a picture of the approaching person. If the package is lifted from the mat, the weight sensors will detect it and trigger an alarm. If an alarm is triggered, the system will notify the user by sending a notification containing the captured photo to an Android app that is connected to this system over WiFi. The system is disabled using the app, or an RFID tag.

Our solution is different in a few key ways. First, our system uses only one camera to detect and track a package. Team 9's solution contains a camera, but also includes a weight sensor mat. We believe the mat is redundant and unnecessary if the goal is to detect and track a package. This can be done using the camera alone through computer vision. Eliminating the doormat also allows the package to be placed in a wider area in your entryway. The old design will only work if the package is placed upon the doormat, but our solution will function as long as the package is in view of the camera mounted above the door. The field of view of the camera will be much wider than the doormat, making our solution more flexible and robust. Next, our design will be entirely housed in one unit that is mounted above your door, instead of having separate units on the floor and above the door. Having the whole system in one enclosed body reduces the risk of tampering with the system. Another difference is that if motion is detected near the package, our system will record a short video clip instead of just a picture. A video clip will give more context and information surrounding events in which an alarm is triggered. Our system will be disabled using a QR code instead of an RFID tag as well, which further reduces cost because using QR codes does not require any additional hardware, and can simply be loaded onto your phone or printed onto a tag. Finally, our system does not need a dedicated app, and will instead send the user a text when packages are delivered, or if activity is detected. This will make the system more flexible for different users with different types of smartphones.

1.3 High-Level Requirements

In order for this system to be successful, it would need to reduce the risk of package theft from households, and if packages are stolen anyways, the system would need to provide a video record of the thief.

- The video recording system must capture thefts reliably (90% +/- 5% theft detection rate) and must disarm reliably using QR code detection (90% +/- 5% QR code recognition rate)
- The notification system must notify the user reliably (90% +/- 5% notification reception rate)
- The sensor and lighting system must illuminate the scene in the dark reliably, using the PIR and ambient light sensors (90% +/- 5% lighting accuracy)

2 Design

2.1 Block Diagram

Our block diagram displays the distinct different modules in our design. The perception module is composed of the Raspberry Pi and the Raspberry Pi Camera, and will be connected to the control and power supply modules. The control module contains a PIC microcontroller. The motion sensor module will contain a PIR motion sensor, ambient light sensor, and a spotlight, and will interface with the control module to send and receive data. The alarm module will contain a DAC to convert a PWM signal to analog, and a medium sized speaker which will output the alarm signal. The WiFi module will contain a dedicated WiFi chip that will interface with the PIC32 over UART, and a LED status light to indicate transmission. Finally, the power supply module will allow us to convert outlet power (120V) into 5V and 3.3V for usage by the Raspberry Pi, PIC32, LED, speaker, and other components.

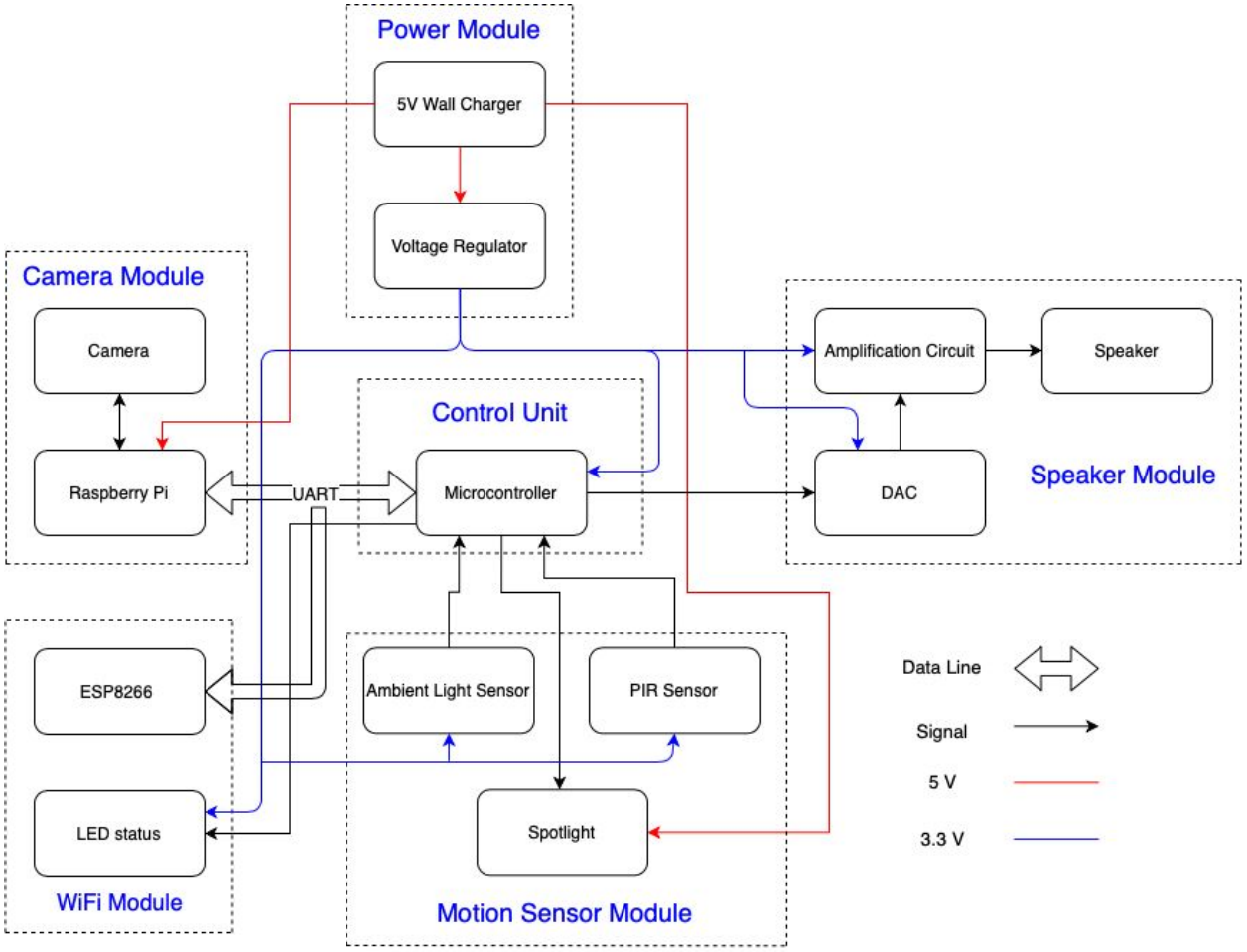

Figure 1. Block Diagram

2.2 Physical Design

The physical design consists of multiple components that will be mounted inside a robust enclosure near the user's entryway. On the front side of the enclosure, the camera, PIR sensor, ambient light sensor, and spotlight will stick out. On the back side of the enclosure, there will be a power cable that should be wired through the wall to be connected inside the user's home.

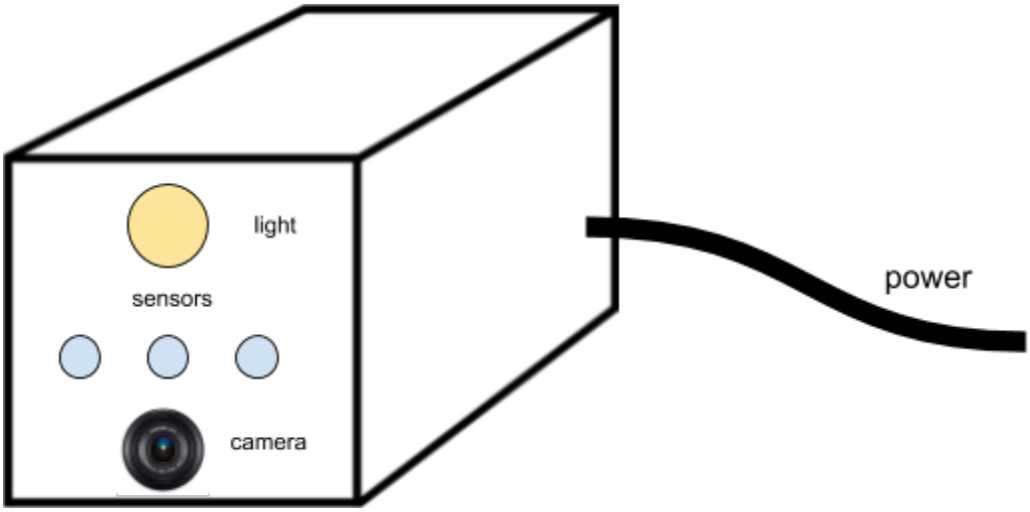

Figure 2. Physical Design

2.3 Power Supply

The power supply is required to allow usage of all components in the device. This includes the Raspberry Pi, microcontroller, camera, LED, speaker, PIR sensor, and WiFi module. The power supply will consist of a 5V wall charger that will step down into 3.3V using a switching voltage regulator (for high efficiency during long periods of energy usage).

2.3.1 5V Wall Charger

The wall charger will be rated for 5V at 3A, which will be sufficient to power all components in the device. It must be able to handle daily usage and current draw from multiple devices (Raspberry Pi, PIC). We will specifically be using the **ALITOVE 5V 3A 15W** supply.

Requirement: Must supply 5V at 3A (max) when all devices are connected.
Requirement: Temperature must be below 125F in order to maintain thermal stability and to prevent damage to the charger and enclosure.

2.3.2 Voltage Regulator

This circuit must supply 3.3V to the microcontroller and PCB and must handle 5V input from the wall charger output and 2A peak current draw from the PIC microcontroller and PCB components. We will specifically use the **TPS63070RNMT** switching regulator.

Requirement: Must provide 3.3V +/- %5 from the 5V wall charger.
Requirement: Must have an efficiency of at least 70% for 2A current draw.
Requirement: Must handle 2A current draw from PIC and PCB components.
Requirement: Temperature must be below 125F for stability and safety.

2.4 Perception Module

The camera module will allow the device to take images and process them. The camera will take images and transfer this data to the Raspberry Pi. The CPU on the Raspberry Pi will do the image processing, and send data to the PIC microcontroller. This data will consist of simple directives (eg: “package delivered”, “package stolen”, “QR code recognized”)

2.4.1 Raspberry Pi

The device will use a **Raspberry Pi 3** for image processing using computer vision (openCV) [5]. The Pi will take image input directly from the camera, process this image on the CPU, and send data out. No other portion of the Raspberry Pi will be used.

Requirement: Must be able to read pixel data over CSI interface.
Requirement: Must be reliable when powered by 5V, 3A power supply, and have a max current draw of 2A.
Requirement: Must process preliminary image data in under 3 seconds +/- 2 seconds for scene recognition (eg: “THEFT”, “DELIVERY”, “QR”)
Requirement: Must process more detailed image data in under 30 +/- 5 seconds (eg: QR code number)

2.4.2. Camera

The camera used will be the official **Raspberry Pi camera** (5 MP, 1080p resolution). The camera must take continuous video when motion is detected, and take periodic frames when no motion is detected. It will send this image data to the Raspberry Pi for processing as it takes images.

Requirement: Must take clear, 360p-1080p resolution images (will downsample to improve speed).
Requirement: Must communicate over CSI interface and CSI bus, allowing for fast pixel data transfer.

2.5 Control Module

The control unit needs to process data coming from the Raspberry Pi and the PIR motion sensor, and output audio to the speaker module and string text to the WiFi module. The motion sensor module will alert the control module when motion is detected (within a reasonable threshold), triggering the microcontroller to request information from the Raspberry Pi. The Raspberry Pi will immediately start processing images to detect the current action occurring, and will send data back to the microcontroller. On the receipt of this information, the Control module will take action.

This action can be:

1. Play an alarm sound, request constant video recording from Raspberry Pi for 30 seconds, and send a text message to the WiFi module indicating a theft.
2. Send a text message to the WiFi module to indicate a delivered package.
3. Reset upon the recognition of the correct QR code when a user picks up the package.

2.5.1 Microcontroller

The microcontroller will be a PIC32, specifically the **PIC32MX270F256D,** and will communicate with the Raspberry Pi using UART. It will run software that will recognize commands coming from the Raspberry Pi, as well as send signals out on the PWM output and to the WiFi module.

Requirement: Must communicate over UART at speeds of 4.5Mbps (needs to be fast data transfer with small data packets)
Requirement: Must use 3.3V +/- 5% for power, and draw less than 1A current.

2.6 Sensor Module

The motion sensor module will be required to detect motion, measure ambient light, trigger a spotlight, and communicate to the microcontroller. In order to do this, the PIR sensor will send its data to the microcontroller in real time, which will process this data to detect motion above a certain threshold. If the threshold is passed, the motion sensor light will automatically light up for 30 seconds. This light will also be controlled by the control module. The sensor module will also detect ambient light, and will only trigger the spotlight if the ambient light is below a certain threshold, indicating that there is low visibility in the area.

2.6.1 PIR Sensor

The PIR sensor will be directly connected to the microcontroller, and will output analog data into the PIC analog input pin. The PIR sensor will work in daylight or nighttime, and will need to alert the system if any human movement occurs in the field of view. We will use the **EKMB1101111 PIR Sensor.**

Requirement: Outputs continuous analog readings to PIC microcontroller.
Requirement: False positive and false negative rates of less than 5 +/- 5%, when tested using human and non-human movements.
Requirement: Outputs reliable data in both daylight and nighttime (90 +/- 5% accurate in identifying movement in both lighting conditions).

2.6.2 Ambient Light Sensor

The ambient light sensor will be directly connected to the microcontroller as well, and will constantly measure the amount of ambient light in the package drop-off area. If the ambient light is above the threshold, there is high visibility which means the spotlight is not needed. Above this threshold, the camera should be able to

capture potential thieves and detect the package easily. Once the ambient light drops below this threshold, visibility will start to decrease, making it harder for the camera to detect the package and capture thieves. Once the ambient light drops below this threshold, the spotlight will begin to be triggered when the PIR sensor detects motion. We will use the **APDS-9007-020 Light Sensor.**

Requirement: Accurately detects ambient light (90% +/- 5% accuracy), and provides consistent and reliable readings.
Requirement: When the threshold is crossed, the spotlight should be enabled (90% +/- 5% reliability).

2.6.3 Spotlight

The spotlight will be powered by the main power supply, and will be turned ON and OFF by the microcontroller. The microcontroller will control an external switch, which will be ON when it is nighttime and motion is detected (PIR sensor and Ambient Light Sensor). We will use a disassembled flashlight, specifically a **Maglite LED Flashlight.**

Requirement: Must illuminate the scene such that the camera can identify objects, persons, and labels clearly.
Requirement: Must operate under 5V, and 200mA, using system power supply.
Requirement: Temperature must be below 125F for stability and safety.

2.7 WiFi Module

The WiFi module is responsible for receiving data from the microcontroller and sending SMS messages to the user's cellphone using the 802.11b/g/n protocol. During the operation, a status LED will indicate transmission is occuring.

2.7.1 WiFi Transmission Module

The WiFi module will be used to transmit messages to the user in real time. It will be connected to the microcontroller, and will receive a message to transmit an SMS to the user's cellphone. The specific WiFi module that will be used is the **ESP8266.**

Requirement: Must communicate with user device over 802.11b/g/n protocol.
Requirement: Must receive data signals from microcontroller on UART I/O pins.
Requirement: Must execute signal transmission within 5 +/- 5 seconds of receiving an alert signal from the microcontroller.

2.7.2 Status LED

The status LED will indicate when the transmission process is occuring by flashing ON and OFF. This will be used for debugging purposes, and can also be useful to deter thieves from stealing packages after being detected. LED model: **C512A-WNN-CZ0B0151**.

Requirement: Must be visible from 2-3 meters away.
Requirement: Must draw 10mA current.

2.8 Alarm Module

The alarm module is responsible for our alert system, intended to scare off potential thieves. It will be triggered by the microcontroller, and will need to create a 30 second alarm signal at 70-90 dBA. In order to achieve this loudness, it will require a dedicated amplification circuit.

2.8.1 Output Speaker

The output speaker will be a single, medium-sized, lightweight tweeter. This will allow the suspect to clearly hear the alarm, and become deterred from stealing the package. We will use the **CMS-40558N-L152.**

Requirement: Must output 70-90 dBA (a-weighted decibels) for appropriate loudness.
Requirement: Must be relatively lightweight, less than 100 grams, to be easily mounted.

2.8.2 DAC Filter

The IC DAC will take as input the PWM output from the PIC microcontroller, and output an analog signal for amplification by the amplification circuit. It will be implemented using the **LTC2644IMS-L12#PBF** IC DAC.

Requirement: Must convert PWM square wave into analog signal for amplification circuit input.
Requirement: Must operate under 3.3V input and draw less than 100mA during operation.
Requirement: Temperature must be below 125F for stability and safety.

2.8.3 Amplification Circuit

The amplification circuit will consist of an opAmp (**LM2904DR)** and variable resistors to amplify the signal, such that the output speaker signal is measured at 70-90 dBA (a-weighted decibels).

Requirement: Must amplify audio signal enough so the user can hear it clearly (70-90 dBA)
Requirement: Must remain below 125F in order to maintain safety of the user and device circuitry.

2.9 Risk Analysis

The success of the project is determined mainly by our ability to detect the presence of objects within a scene during different lighting conditions. Our system must be able to detect and label packages of various sizes and shapes. To do so, we will train our model to recognise a variety of packages. This will play a pivotal role in determining how efficient our system will be in tracking objects. We will need to also ensure that a package can

be tracked during nighttime conditions. To account for this, we will implement a sensor system that will detect movement and illuminate the scene. In any case, we would want our system to be able to track a package and its status at all times. Failure to recognize an object will ultimately render our system useless. Establishing a system with reliable object detection will be the greatest challenge of the project.

3 Ethics and Safety

We have an obligation to our profession to uphold the highest level of ethical and professional conduct. We stand to follow and commit ourselves to the guidelines stated by the IEEE Code of Ethics. Safety of the user is of utmost importance especially since there are significant hardware components situated on the body of the user. There is a potential danger of hardware components short circuiting and overheating after prolonged usage that could cause harm to the user. We intend to design our product with these risks in mind in accordance to the IEEE Code of Ethics #1 - "To hold public safety first and to disclose factors of our project that might endanger the public" [8]. Mitigating these risks are our main priority. To avoid overheating, we will ensure that all components operate in low power mode when not in use. Additionally, hardware components will be spaced out accordingly within our designed enclosure so that electrical contact is avoided risking a short circuit and ultimately device malfunction. The enclosure should uphold OSHA provision standards 1910.303(b)(7)(i) stating "Unless identified for use in the operating environment, no conductors or equipment shall be located in damp or wet locations; where exposed to gases, fumes, vapors, liquids, or other agents that have a deteriorating effect on the conductors or equipment; or where exposed to excessive temperatures."[9] to provide protection against any case of exposure to liquids that could cause a short circuit. This is critical as the device will most likely be placed outdoors where it will be exposed to the elements.

We acknowledge that there is a certain degree of error that can arise from object identification. The core of the project depends on users being able to trust our system to identify and label an object in its scene with a high level of accuracy. To adhere to the IEEE Code of Ethics #3 - "To be honest and realistic in stating claims or estimates based on the available data."[8], it is our duty to be honest of the estimates provided from the available data provided to us. To uphold this, we will ensure that our system has a reliable output and is able to verify and identify a variety of packages with different sizes and shapes.

Finally, our product would not be possible without the advances in computer vision algorithms developed by pioneers before us. In accordance to the IEEE Code of Ethics #7 - "To seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others." [8], we would like to formally acknowledge and give due credit to those who have contributed to the open source software, OpenCV.

References

[1] K. Buchholz and F. Richter, "Infographic: 87 Billion Parcels Were Shipped in 2018," *Statista Infographics*, 08-Nov-2019. [Online]. Available: https://www.statista.com/chart/10922/parcel-shipping-volume-and-parcel-spend-in-selected-countries/. [Accessed: 03-Apr-2020].

[2] Kaza, "6 Shocking Stats about Package Theft," *Smiota*, 17-Feb-2020. [Online]. Available: https://smiota.com/resources/6-shocking-stats-package-theft/. [Accessed: 03-Apr-2020].

[3] "Burglary Statistics: The Hard Numbers," *National Council For Home Safety and Security*, 19-Dec-2019. [Online]. Available: https://www.alarms.org/burglary-statistics/. [Accessed: 03-Apr-2020].

[4] "5 Reasons Why Homeowners Don't Have Home Security Systems," *ADT Home Security and Alarm Systems | ProtectYourHome.com*. [Online]. Available: https://www.protectyourhome.com/blog/articles/2014/march/5-reasons-why-homeowners-dont-have-home-security-systems. [Accessed: 03-Apr-2020].

[5] H. Blodget, "Here's A Picture Of Amazon Locker, The New Delivery Box Amazon Is Using To Take Over The World," *Business Insider*, 24-Aug-2012. [Online]. Available: https://www.businessinsider.com/amazon-locker-2012-8. [Accessed: 03-Apr-2020].

[6] T. Haselton, "Amazon Key changes how packages are delivered - just beware of your dog," *CNBC*, 16-Nov-2017. [Online]. Available: https://www.cnbc.com/2017/11/16/amazon-key-in-home-delivery-review.html. [Accessed: 03-Apr-2020].

[7] J. Bianco, J. Graft, and J. Simonaitis, "Package Anti-Theft System," Feb. 2018. [Online]. Available: https://courses.engr.illinois.edu/ece445/getfile.asp?id=12482. [Accessed: 03-April-2020].

[8] "IEEE Code of Ethics," *IEEE*. [Online]. Available: https://www.ieee.org/about/corporate/governance/p7-8.html. [Accessed: 03-Apr-2020].

[9] Osha.gov. (2020). *1910.303 - General. | Occupational Safety and Health Administration*. [online] Available at: https://www.osha.gov/laws-regs/regulations/standardnumber/1910/1910.303 [Accessed 28 Feb. 2020].