IJHSR
ijhighschoolresearch.org

■ RESEARCH ARTICLE

Low-Cost IOT Device Security for Standard Mailboxes

Ansh Maroo

Dougherty Valley High School,10550 Albion Rd, San Ramon, CA 94582, USA; amaroo2006@gmail.com
Mentors: Mr. Sanjay Mehta

ABSTRACT: Communities across America have witnessed increased crimes such as shoplifting, car break-ins, burglaries, home invasion, and even mailbox theft. Mailboxes are easily accessible from curbs, and most have no locks making them accessible and attractive targets for thieves. Additionally, these thieves can empty the mailboxes of entire neighborhoods at a time. Due to stolen mail, many homeowners have been victims of identity theft and other financial crimes. While homeowners have access to various home security devices and systems, their mailboxes remain largely unprotected. This study analyzes the effectiveness of a low-cost device that utilizes home Wi-Fi, the Internet of Things (IoT), and cloud computing to secure standard mailboxes. Once installed in a standard mailbox, the device sends alerts to the homeowner shortly after the mailbox is opened. The possibility of leveraging communication from multiple "secure mailboxes" in a neighborhood to detect in-progress thefts and alert homeowners of possible upcoming thefts is also discussed. Tests indicated that a cloud-connected mailbox sensor was effective when connected to a home Wi-Fi network. A cloud-connected secure mailbox is a reliable, cost-effective solution to address mailbox security.
KEYWORDS: Engineering Mechanics, Internet of Things; Microcontrollers; Sensors; Networking and Data Communications.

■ Introduction

As described by the United States Code 18 Section 1708, mail theft is a felony punishable by up to five years in prison and fines of up to $250,000.[1] Mail theft occurs when one takes mail from mail trucks, delivery bags, mail carriers, and mailboxes. Additionally, state laws punish mail theft with jail time and fines that may be coupled with federal charges. Even with these legal protections, mail theft is on the rise. Data shared by the United States Postal Inspection Service (USPIS) indicates that mail theft reports increased by 600%, from about 25,000 in 2017 to roughly 177,000 through Aug. 24 2020.[2] USPIS data also indicates that approximately 2500 suspects were arrested for the thefts of mail and packages in 2018.[3] However, the magnitude of this problem may be much larger than reported as it has been revealed that mail theft is not being adequately tracked.[3]

Mail theft affects American households directly and indirectly. Stolen packages represent one of the most direct and visible impacts of mail theft, and according to recent research, 49 million Americans have had at least one package stolen from November 2020 to November 2021.[4] This research indicates that the median value of stolen merchandise was $50, amounting to more than $2.4 billion in stolen goods.[4] Another research publication indicated that 73% of its participants have been purchasing more items online since the COVID-19 pandemic amidst rising incidents of package theft.[5] Package theft is a crime of opportunity and convenience and is increasing. Checks are another favorite target of mailbox thieves, who use them to commit check fraud, identity theft, and other crimes.[6] According to a 2021 report by the Bureau of Justice, about 9% of persons age 16 or older had been victims of identity theft during 2018, and the monetary losses across all incidents of identity theft totaled $15.1 billion.[7]

Mail thieves dispose of mail that is of no value to them, but this mail is often valuable to the intended recipient. The mail may contain time-sensitive notices or communication from government agencies, utility providers, employers, other institutions, or individuals. In every case, it may result in failure to respond to opportunities, payments, or some other action. All these result in some form of loss, damage, or inconvenience to the intended recipients and are often never quantified in any research.

Recipients of mail have a few options to physically secure their mail, but these could have been more effective. USPS-approved locking mailboxes are available in the market. However, they come with a variety of issues. USPS letter carriers are not allowed to carry keys to residential mailboxes and instead deposit mail through an unlocked incoming mail door or slot. However, these openings may not be small enough to prevent prying hands from reaching in and fishing out the mail. In addition, USPS-approved locking mailboxes do not protect outgoing mail that needs to be placed in an unlocked compartment available to letter carriers. Thieves have also bypassed the locks on such mailboxes.[8] There are a few USPS-approved smart mailboxes as well, but they also face the same issues mentioned above. Smart mailboxes feature tamper alarms, motion sensors, cameras, and weight monitors and can be secured to the ground. Similar technologies, such as smart doorbells and smart security cameras, have kept porch pirates from stealing packages. However, the adoption of these expensive smart mailboxes needs to be higher as recipients are skeptical of installing them.

This study proposes an alternate solution to locked or smart mailboxes. The solution involves using an internet-enabled

DOI: 10.36838/v5i5.6

retrofit device installed in a standard mailbox. The device would connect to the internet using the user's home Wi-Fi. It would detect the opening of the mailbox and send an alert to the cloud. The alert would be processed in the cloud, and the system would notify the user each time the mailbox has been accessed (Figure 1).

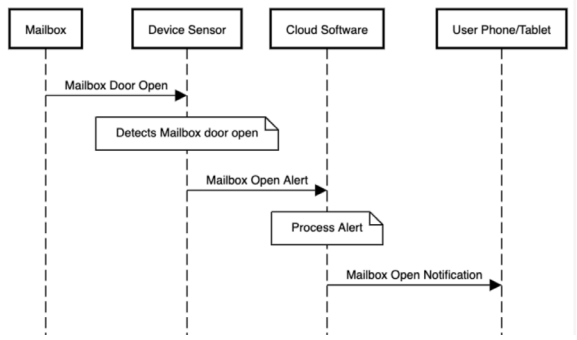

Figure 1: A sequence diagram for the Mailbox SECURE prototype depicting the sequence of events of the solution.

Additionally, as more devices are installed, more and more alerts will be processed in the cloud to infer the mailbox access patterns of each homeowner and highlight any suspicious access by special notifications. Further, the system could scale in the future to identify and alert an entire neighborhood of any suspicious mailbox activity to detect crimes in progress. While the device would be vulnerable to tampering or theft like any other device, such as a security camera, its size would allow it to be installed underneath the mailbox such that it would be concealed and not easily visible.

In this study, a functional prototype of mailbox SECURE was built using commercially available components to demonstrate the feasibility of this solution for a smaller subset of the features envisioned. The objectives for the prototype of this solution were to test if Mailbox SECURE:

1. Can reliably detect the opening and closing of a mailbox.
2. Can quickly notify the user when their mailbox has been accessed.
3. Can be a cost-effective solution for standard mailboxes.

Methods

The prototype for mailbox SECURE involved readily available parts and components (Figure 2).

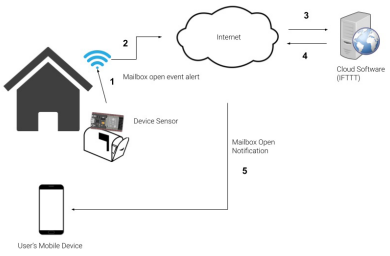

Figure 2: An architecture diagram for the mailbox SECURE prototype depicting all the solution's components.

Existing mailboxes (USPS certified) were used for testing. The prototype included an installable sensor device built with a programmable, internet-enabled ESP32TM microcontroller. A 5-volt, 10,400 milliamp hour power bank and a low-dropout voltage regulator were used to power the microcontroller. In addition, a circuit was designed to act as a physical switch (Figure 3).

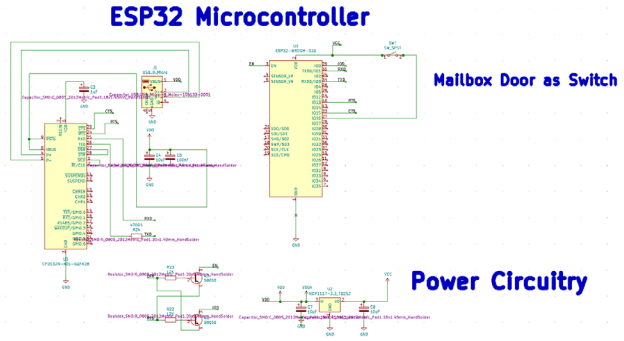

Figure 3: Schematic diagram of the Mailbox SECURE circuit. The microcontroller and supporting circuitry are depicted. A physical switch represents the opening of the mailbox.

This sensor device was installed on the standard mailbox and was connected to a home Wi-Fi network. When the mailbox was opened, the voltage on a pin of the ESP32™ microcontroller changed. Custom software (Appendix) on the microcontroller detected the change in voltage and sent an HTTP request to IFTTT™(If This Then That) servers over the home Wi-Fi network. Software located in the cloud was responsible for receiving alerts and processing them. The prototype solution leveraged a web service and a companion mobile app from the popular automation service IFTTT™. The HTTP request from the sensor device was sent to IFTTT™'s free webhook service, which then sent a notification to the IFTTT™ app on the user's mobile device, informing them that their mailbox was accessed and the time of the event. A video demonstration of the prototype device in use was also created.[9]

The Mailbox SECURE prototype was installed in 3 locations across the San Francisco Bay Area. The installation on each location was configured to send the notification to a unique mobile device. It was tested for:

Reliability: Does the Mailbox Secure prototype send a notification to the user's mobile device when the mailbox is accessed? Reliability was tested by recording whether a notification was received on the mobile device each time the mailbox was accessed. This test was repeated 200 times.

Latency: What is the time in seconds between the mailbox access event and the notification arriving on the user's mobile device? For each mailbox access, the elapsed time from when the mailbox was opened to the time when the notification was received on the mobile device was manually measured with a stopwatch and recorded. This test was repeated 200 times.

Battery Life: How long does the battery for the Installable Sensor Device last under normal usage? Battery life was tested by installing the device in a mailbox and powering it with a 10,400 milliamp-hour power bank. The mailbox was accessed four times daily to trigger the sensor device, simulating normal usage until the power bank could no longer power the device.

DOI: 10.36838/v5i5.6

The battery life was recorded in hours. This test was repeated five times.

Results and Discussion

In 600 trials, the prototype successfully delivered mailbox access notifications 99.66% of the time (Table 1). On further analysis, it was found that the installable sensor device successfully communicated the alert to the IFTTT 100% of the time when the mailbox was accessed.

Table 1: Notifications received on the mobile device after 200 mailbox access events in 3 locations.

Location	Mailbox Access Events	Notifications Received	Success Percentage
1	200	199	99.50%
2	200	200	100.00%
3	200	199	99.50%

In 600 trials, the prototype solution delivered notifications within 5 seconds to the app on the mailbox recipient's device (Table 2). Table 2 shows that 99% of the notifications were received within 4.58 seconds and 90% of the notifications were received within 4.43 seconds of the mailbox being opened. Further analysis indicates that the sensor device takes approximately 500 milliseconds to make the IFTTT™ web service request and the rest of the time is taken by the IFTTT™ web service to process the request and send the notification to the mobile device and that there is further room for improvements both on the installable sensor device and the processing in the cloud.

Table 2: Times to receive notifications on a mobile device after mailbox access.

Location	Percentile Time to Receive Notification (Seconds)		
	Top 99 Percent	Top 90 Percent	Top 50 Percent
1	4.52	4.43	3.99
2	4.58	4.35	3.52
3	4.28	4.06	3.25

A 10,400 milliamp-hour battery powers the prototype solution's sensor device. With four mailbox access events each day, the battery lasted an average of 6.44 days over five trials (Table 3).

Table 3: Average battery life with four access events per day.

Trial	Battery Life in Hours (Days)
1	156(6.5)
2	151(6.3)
3	163(6.8)
4	157(6.5)
5	160(6.7)

Points of Failure:

The prototype solution has some points of failure. Mailbox SECURE uses home Wi-Fi for the installable sensor device to communicate with the cloud software. Any interruption in this Wi-Fi connection will prevent the sensor device from sending mailbox access events to the cloud software. Another point of failure is the availability of the cloud software itself. Any interruption in its availability will affect mailbox events from being processed and notifications from being sent to the recipient's device. However, the likelihood of either of these failures is very low. The cloud software used in the prototype solution is a commercial Internet of Things (IoT) scale service with real-time status tracking and support for its services. Future improvements include a custom cloud software implementation, offering similar or better service availability levels. Additionally, the device circuitry could experience a hardware failure. In this case, the user would not be aware of any failure because the prototype device does not have the ability to signal its health status.

Future Improvements:

While the Mailbox SECURE prototype demonstrates that it is a very promising option to secure mailboxes effectively, the prototype will need some of the following improvements to become a complete solution that the users can adopt.

1. Redesigned Sensor Device: The installable sensor device should be further optimized with a custom circuit and printed circuit board. This can help bring the following improvements:

a. Power and Batteries: The battery powers the prototype device for approximately six days on a single charge. Improvements to power regulation circuitry and other design enhancements will allow the battery life to be comparable with that of commercially available IoT devices. The device could also be improved with circuitry to detect low battery levels and alert the user when the battery needs recharging, at which point the user would recharge the battery manually. All batteries discharge faster at cold temperatures, reducing battery life. To mitigate this, the device could include lithium batteries that are less severely affected by colder temperatures. Additionally, solar power could be implemented. This would reduce or eliminate the need to recharge batteries manually.

b. Cost reduction: A custom-designed and printed circuit board, especially at scale, can significantly reduce the cost profile of the Mailbox SECURE solution and make it more attractive to users.

c. A compact form factor that will also make installation easy for users

d. Optionally, more sensors, such as cameras, could be added to disambiguate suspicious mailbox access events and record suspicious activity to track down bad actors. Additional hardware like alarms could also be added to deter bad actors, especially if suspicious activity is detected on other mailbox SECURE-enabled mailboxes in the immediate neighborhood.

e. Alternative wireless communication: While the prototype device used a direct Wi-Fi connection, alternative wireless communication methods were considered for future improvements. Protocols such as Zigbee, ESP-NOW, and other alternatives to a direct Wi-Fi connection could provide improvements to battery life, notification latency, and reliability. If such protocols are used, an additional device would be needed to receive messages from the mailbox sensor and relay them to cloud servers.

f. Device health: Device health could be indicated through periodic signals sent by the device. Failure to send or receive such a signal would indicate a device failure.

2. Custom cloud software: By using a custom-designed cloud software interface instead of the IFTTT platform, the following improvements can be brought to the solution:

a. More reliable and faster notifications: A custom-developed cloud interface can provide much faster, near-real-time notifications with higher reliability. Notification latency under 2 seconds and 99.99% notification reliability are realistically achievable.

b. Machine learning and Artificial intelligence: By learning from the patterns of mailbox access for each home, a neural network can disambiguate suspicious mailbox access and thereby alert the user only when there is suspicious access to reduce notification fatigue.

c. Community alerts: The cloud software could alert an entire community when it detects a pattern of serial mailbox access events in the immediate neighborhood. Such events could alert users even before a thief nearby accesses their mailbox.

3. A Mailbox SECURE app: a dedicated mobile application would be necessary to deliver some of the abovementioned features, especially any community alert features and custom notification events. Such an app could also help users easily set up the device, specify their notification preferences, and receive notifications on multiple devices.

Conclusion

Tests of the prototype indicate that a fully functional Mailbox SECURE solution could be an effective mail security system. It provides a 99.66% notification success rate, notifications under 5 seconds, and a nearly week-long battery life. However, improvements such as longer battery life, an improved form factor, custom cloud software, and a dedicated mobile application will be necessary for more feasibility in the real world. Additionally, the Mailbox SECURE sensor device also offers a working prototype for similar IoT devices that can be paired with other sensors and software integrations to serve a variety of use cases.

Acknowledgments

I appreciate all those who supported me while envisioning and completing this prototype. I thank my parents and Mr. Sanjay Mehta, who motivated me to complete this project.

References

1. 18 U.S.C. 1708 - Theft or Receipt of Stolen Mail Matter Generally; 2021; Vol. 1708.
2. Schapiro, R. Is mail theft surging in the U.S.? Postal inspectors don't know http://www.nbcnews.com/news/us-news/mail-theft-surging-u-s-postal-service-inspectors-don-t-n1241179 (accessed 2022-08-05).
3. Mail Theft | USPIS https://www.uspis.gov/tips-prevention/mail-theft (accessed 2022-08-07).
4. 2022 Package Theft Annual Report https://www.security.org/package-theft/annual-report (accessed 2022-08-08).
5. 2021 Package Theft Statistics Report – C+R Research https://www.crresearch.com/blog/2021-package-theft-statistics-report (accessed 2022-08-19).
6. Davis, W.; Keith, T. Check fraud is on the rise. Here's what you need to know and how to avoid it https://www.npr.org/2022/02/03/1077766541/usps-checks-mail-fraud-bank (accessed 2022-08-20)
7. Harrell, E. Victims of Identity Theft, 2018 https://bjs.ojp.gov/library/publications/victims-identity-theft-2018 (accessed 2022-08-20).
8. Miller, M. Mail thieves aggressively target locked metal boxes https://komonews.com/news/local/mail-thieves-aggressively-target-locked-metal-boxes (accessed 2022-08-27).
9. Maroo A. Mailbox SECURE Demonstration https://youtu.be/SYZww4Sz-Qw (accessed 2023-04-01).

Author

Ansh Maroo is a senior at Dougherty Valley High School in San Ramon, California. He has an avid interest in software programming, computer hardware, and electronics.

DOI: 10.36838/v5i5.6