Intelligent and Privacy-Preserving Medication Adherence System

Ji Jia*, Jinyang Yu*, Raghavendra Sirigeri Hanumesh*, Stephen Xia*, Peter Wei*
Hyunmi Choi† and Xiaofan Jiang*

*Columbia University, †Columbia University Medical Center

{jj2860,jy2803,rs3603,sx2194,pw2428}@columbia.edu, hc323@cumc.columbia.edu, jiang@ee.columbia.edu

Abstract—We present a novel privacy-preserving pillbox system for helping patients improve medication adherence while maintaining privacy and security. In the proposed system, we protect data that needs to be reported to the doctor by ensuring that the data can only be decrypted by the doctor, authorized by a face-to-face key exchange process through out-of-band communication channels. Our system also gives patients fine-grained control over how their information is transmitted and shared, which is a major privacy concern for many patients. Also, for helping physicians to acquire their patients’ data efficiently and safely, we designed a web interface for physicians. In addition to privacy and security issues, current smart pillboxes typically either use open/close sensors, which do not accurately detect whether pills have been removed, or use weight sensors, which are prone to sensing errors if the pillbox is mobile. The proposed system verifies patient pill intake or medication adherence by using a light-based pill detection mechanism that achieves greater than 98% accuracy. Our user study shows that the system is simple to use and alleviates users’ privacy concerns.

I. INTRODUCTION

Medication adherence is of paramount importance in achieving treatment goals and consequently maintaining quality of life [17], [14], [5]. However, full adherence of medication treatment is frequently difficult for a variety of reasons. One common reason is the difficulty with remembering to take medications, which is particularly prevalent among patients with chronic medical conditions that affect cognitive functions. A recent solution to medication non-adherence is the development of “smart” pillboxes. Recent innovations in cyber-physical systems and the Internet of Things technologies have made it possible to create intelligent systems for medical care such as smart pillboxes [21].

Currently, there are several commercial smart pillbox products available in the market, such as MedMinder [10] and Hero [9]. Existing smart pillboxes have several shortcomings, including inadequate privacy protection and pill detection accuracy. Prior studies have shown that one major concern among patients is the confidentiality and privacy of their electronic health care records (EHR) and web-based communication [7], [16], [6], [20], which has contributed to the lack of widespread adoption of smart pillboxes. Some off-the-shelf smart pillbox products may expose patients’ medication records to unknown sources. As shown in Figure 2, current smart pillboxes send and stores sensitive patients’ pill-taking data to the cloud. This approach poses a potential security risk, and does not give patients control over what and how their information is transmitted or shared. In addition to privacy and security concerns, some pillboxes have pill detection mechanism based on open/close sensors, capacity sensors, weight sensors and light sensors. However, there are some issues with these designs such as accuracy, reliability, and cost efficiency.

Our proposed system is further motivated by experiences from real physicians from the Columbia University Medical Center and their daily interactions and experiences with patients. The first issue expressed by the physicians is the difficulty in obtaining patient dosage history. Even with the use of existing pillboxes, it is often impossible to verify the
patient’s testimony of their own dosage history. The second issue is the patient’s privacy concerns over their electronic health care records.

In this paper, we design, implement, and evaluate a low-cost smart pillbox system (Figure 1) taking into account continuous feedback and suggestions from the physicians at the Columbia University Medical Center. Our goal is not only to make a smart pillbox for patients, but more importantly to develop a system which can help physicians obtain their patients’ dosage history easily.

This system not only accurately detects pills and alerts patients based on prescribed medication regimens, but also ensures the confidentiality and privacy of a patient’s medication records by

- Utilization of the patient’s smartphone for storage of all medication records
- Establishment of a end-to-end secure communication channel between the patient and physician using a public key cryptography
- Acquisition of the physician’s public key by the patient through out-of-band communication channels

The proposed smart pillbox system consists of four connected components: (1) a physical smart pillbox; (2) a mobile application on the patient’s phone; (3) a web application hosted on the hospital’s server; (4) a server for forwarding data from the patient’s phone to the physician’s web application.

Major functions of this system include pill detection, medication reminder, medication history logging, and medication regimen synchronization. The intelligent pillbox uses a light sensor to detect pills inside each container. The smartphone application communicates with the pillbox via Bluetooth Low Energy (BLE) and to the physician’s web application via QR code. All sensitive data regarding pill intake are stored in the pillbox and in the patient’s smartphone instead of the cloud or server and transferred securely to the physician during clinic visits. The security and privacy measures taken to safeguard this data on the phone are described in sections below.

The rest of this paper is organized as follows. Section II presents the state-of-the-art on smart medication systems as well as on patient Electronic Health Records (EHR) confidentiality. Section III details the implementation of the pillbox including the hardware architecture with its pill detection technique, the smartphone application, the web application together with their security features. Section IV evaluates the system, including test cases, results, discussions, and future works. Section V concludes the paper by discussing the key contributions.

II. RELATED WORK

Several types of smart adherence solutions have been presented using different methodologies [13]. We describe and compare their approaches to pill detection and data security below.

The MedTracker [8] pillbox tracks the opening and closing motions of pillbox compartment lids to track consumption. This approach is undesirable as patients may open and close the lid, but not actually remove the pills from the pillbox. Sung at al. proposed a mechanism based on a magnetic sensor, a movable plate and two permanent magnets, which are used in each container for detecting pills [18]. If the container has no pill inside, then the magnetic flux generated by the two magnets is relatively close to the magnetic sensor, thus is relatively stronger. While this approach works, the design complexity of the structure is high and it might suffer from mechanical wear and tear over long-term usage.

Salgia et. al. used a capacitive sensing technique as the pill detection mechanism for a smart pillbox system [15]. The presence of a pill which acts as a dielectric produces a change in frequency. However, it works only for tablets that weigh above 10 mg as the accuracy is affected by interference from the surroundings.

Barfield et al. proposed a new light-based sensing mechanism for detecting pills in which the container has an LED on the bottom and a photodiode as a light sensor on the top [3]. In order to maximize the chances of pill detection, a sloped structure is used to aggregate the pills on top of the LED. This method assumes that the LED can be fully blocked by the pill; however, there is a chance that small pills may partially block the LED which leads to false detection. We improve on their pill detection mechanism, by placing the light source on the top and a light diffuser under the light source to further increase the reliability.

Tsai et al. [19] describes an automatic medication dispenser design. The dispenser uses multiple pill sockets to contain different pills, and automatically dispenses pills from these sockets based on the prescription for each dosage. However, this design requires a complex mechanism to dispense pills from each container. The high cost and reliability issues on mechanical parts are characteristics that inhibit widespread adoption.

There also exist many mobile phone-based medication adherence solutions [4], [11], [1], [12], [13] such as OnetimeRX which requires the patient to manually enter the reminder schedule or fill or download a form to fill the reminder schedule [11]. Abbey et al. constructed a pillbox that connects to Wi-Fi and displays medication notifications on a web application directly [1]. AdhereTech introduced smart wireless pill boxes which collect medication records and sends them to a secure proprietary central server, which may use third-party companies or its own infrastructure [2]. However, the storage of such confidential data on third-party servers in the cloud raises privacy and security concerns in patients.

While all of these works have made advances in pill detection and medication adherence, they do not adequately account for privacy considerations of the data involved. Existing commercial solutions store data remotely, which have privacy risks for medical data. And, the current pill detection mechanisms are not robust enough and fail in several real-world scenarios. Some of the methods are also not cost effective for large scale manufacturing. Moreover, few products have considered the pillbox as a system that needs to interact with physicians.
III. System and Implementation

As shown in Figure 3, our system consists of four major components:

- An intelligent pillbox for patients: The pillbox is a stand-alone device using an optical-based reliable pill detection mechanism. The pillbox also collects and communicates data representing the patient’s medication events with the smartphone application, through Bluetooth Low Energy.
- A smartphone that is used to communicate with the pillbox and physicians: Data from the pillbox is directly stored in the internal storage of the patient’s smartphone. Data is securely sent to physicians at the authorization of the patient and is encrypted using the encryption key received from the physician through the QR code displayed on the web application.
- A web application for physicians to review patient medication records and update pill schedules: The web application generates public-private key pairs on the fly to protect every record transmission using asymmetric encryption. Physicians pass the public key face-to-face using a generated QR code.
- A server that establishes a connection between the smartphone and web applications to allow encrypted data to be forwarded from the smartphone to the web application.

A. Typical Usage Scenario

A patient initially schedules a physician’s appointment. During the appointment, the physician and the patient agree on a treatment regimen consisting of specific pills and schedule. The physician assigns a pillbox to the patient and sets up the intelligent pillbox system with the following steps. First, the patient downloads the smartphone application and pairs with the pillbox via Bluetooth Low Energy. Second, the physician uses the web application to generate a QR code with the patient’s medication schedule embedded inside. Next, the patient scan the QR code to receive the medication schedule on the smartphone. Finally, when the patient’s smartphone comes in range of the pillbox, the medication schedule is transferred from the smartphone to the pillbox through Bluetooth Low Energy. The intelligent pillbox synchronizes medication records to the patient’s smartphone periodically without any actions from the patient.

After using the pillbox for some period of time, the patient returns to the physician for a follow-up appointment. The only item that the patient is required to bring to the appointment is the smartphone that was used to connect to the pillbox. During the appointment, the physician first uses the web application to generate a pair of asymmetric encryption keys, and generates a QR code containing the public key. The patient then scans the QR code, which initiates the transfer of historical pillbox data stored on the smartphone to the physician or hospital’s machine. Finally, based on the results of the checkup, an adjusted medication schedule can be generated and embedded into a new QR code for the patient to scan, receive and synchronize with the pillbox.

B. Pillbox

The pillbox is designed to house 28 containers for storing pills to be typically taken up to 4 times a day for 7 days of the week; or it can be arranged to any schedule up to 28 dosages.

It uses an optical sensing mechanism for pill detection, and logs events such as the opening and closing of lids and presence of containers and pills within the pillbox. The pillbox communicates with the patient’s smartphone using Bluetooth Low Energy (BLE) for control and data transfer when the phone is within range of connectivity. When the connection is lost, the pillbox logs the data in local memory and sends this data to the phone when connection is re-established. The pillbox also obtains the prescribed medication schedules from the phone (explained later in section III-C3). A button is included on the pillbox which is used during the Bluetooth pairing process to prevent unauthorized pairing.

1) Mechanical Design: The pillbox consists of two parts: a base enclosure and pill containers. The base enclosure is rectangular in shape and divided into 28 smaller sections (holders), as shown in Figure 4. Each holder houses a pill container, shown in Figure 5, and has a lid, shown in Figure 6, to hold the pill containers securely. A LED on this lid acts as the light source for the detection mechanism and a indicator for users. The base enclosure also holds the light sensors and related circuitry. The pill containers are small rectangular boxes with the bottom tapering to a small transparent window. Each container holding a single dosage of pills to be taken at a given time. The containers have lids that slide open. The lid also acts as a light diffuser to allow uniform distribution of light within the container for accurate pill detection. These containers can be removed from the holders for refilling or emptying the pills. The light sensors are fixed to the bottom of the base enclosure, such that the sensing region aligns with the window at the bottom of the pill container as described in Figure 7. This setup enables the pill detection mechanism. When all lids are closed, the light from the LED passes through the diffuser, into the container and the intensity of
light received at the opening is measured by the light sensor. The intuition behind the design methodology is three-fold:

- Removable pill containers enable easy refilling and consumption of pills as compared to fixed containers. The containers can be taken out, cleaned, refilled, and put back in any order.
- The pills need to aggregate directly over the sensor for accurate detection. The tapered bottom ensures that there are no stray pills on the sides which might not be positioned directly over the sensor.
- Since only one LED is used per container, ensuring proper distribution and light sensing is necessary. The window and the diffuser ensure this.

2) Pill Detection Mechanism: The pill detection mechanism, visualized in Figure 7, is designed based on optical sensing method. It involves using a light source and a light sensor placed across the top and bottom of the pill container, respectively, as described in the previous section. When the pill container is empty, the light is unobstructed and the intensity of light incident on the sensor is maximum. Conversely, when there is one or more pills present in the container, it obstructs the light, thereby reducing the intensity of light incident on the sensor. The drop in intensity depends on the pill size and the count. Since pill sizes vary, some small pills will not be able to fully block the incident light in other detection methods. In our system, the light sensor effectively detects the presence of pills of common sizes, as described in Section IV. This provides for an inexpensive mechanism for detecting pills with high reliability.

3) Pillbox Calibration: Because of the production error of each electrical component and mechanism structure, the 28 sensors may return inconsistent reading in the same condition. For ensure the accuracy of pill-detection in the 28 containers, the light sensors need to be calibrated before use.

The calibration procedure is as follows. First, readings from all 28 light sensors in the pillbox array are taken in the idle mode without any pills placed inside. We denote this value as $L_{n0}$, where $n$ refers to the container number. The average of these readings is computed, as shown in Equation 1.

$$\text{avg} = \frac{1}{28} \sum_{n=1}^{28} L_{n0}$$

The calibration factor, $a_n$, is obtained by dividing the computed average by every container’s empty idle mode reading, $L_{n0}$, as shown in Equation 2.

$$a_n = \frac{\text{avg}}{L_{n0}}, \forall n = 1, \ldots, 28$$

The final values that are used in the pill detection mechanism, $I_n$, take the sensor readings, $L_n$, and scale the values by the calibration constant. This is shown below.

$$I_n = L_n \times a_n, \forall n = 1, \ldots, 28$$

The modified sensor values, $I_n$, that are used in the pill detection are now much more consistent and take on values at a much smaller range, boosting accuracy and precision in measurements and detection.

4) Pillbox-Patient Interactions: This section describes how the pillbox interacts with patient inputs and actions. As shown in Figure 8 there are two status indicators on the smart pillbox. The pillbox can be in the idle mode, meaning the patient does not need to do anything on the pillbox, or in an active mode, meaning that the patient needs to remove the pills from a specific container. The state diagram is shown in Figure 9.

The pillbox will respond to patients in different statuses and after certain actions.

- In the idle mode, the LED in the container is turned off and the patient is not supposed to take any medication in.
the pillbox, or else an error will result. If the container is opened during this time, the light source LED will begin to blink rapidly to alert the patient of the mistake.

- When the pillbox is in the dosage active mode period, the LED within a specific container starts blinking to notify the patient to remove and take all the pills from that container. The active mode will usually last between one to two hours. This parameter can be set in the schedule. The patient needs to remove the pills, and close the container cap in order to stop the blinking. Once the container LED stops blinking, the pillbox resumes idle mode and waits for the next dosage period before repeating the cycle. If a patient fails to take the specified pills within the dosage window, then an error is recorded in the log.

- If there are any problematic situations that arise, such as excess powder from pills covering the inside of the container or if not all the pills were taken during the dosage period, the LED at the cap of the container will continue to blink until the issue is resolved.

C. Patient Smartphone Application

The smartphone app communicates with the smart pillbox using an established Bluetooth Low Energy (BLE) connection. The app has the following convenient features to make it easy to use:

- The app auto-connects to the smart pillbox, through Bluetooth. When the smartphone comes into the vicinity of the smart pillbox, all pillbox activity data is transferred into the internal storage of the smartphone through the newly established BLE connection.
- The application runs in the background and allows patients to use their phones normally for other activities.
- The data transfer between the pillbox and the smartphone is not severely affected by Bluetooth disconnections; if the smartphone moves out of range of the pillbox and the connection is lost, then data transfer will resume once the smartphone moves back into range of the pillbox and the Bluetooth connection is reestablished.

- Notifications are sent to the user at the beginning, at the end, and throughout the dosage window to remind the user to take the medication.

1) Historical Records: Electronic health records contain sensitive information; thus, we designed several features to preserve patient privacy. The smartphone app stores the historical records in local memory using encryption techniques as described in the Section III-D6. Patients also have ability to view, delete and control the data transfer process, as shown in Figure 10. Before the data is sent to the physician, the patient can select which time durations of the historical data to share with the physicians, as well as which physicians to share the historical data with.

2) Pillbox Status: The smartphone app tracks a real-time status visualization of the pillbox status as shown in Figure 11. The following information is displayed:

- Whether there are any caps or lids on the pillbox containers that are open
- Presence of pills in pillbox containers
- The app indicates whether or not the inner container of a pillbox has been removed
- Indication of whether or not the correct pill was taken by the patient

3) Updating and Synchronizing Medication Schedules: The medication regimen can change at the time of a clinical visit based on changes in the treatment plan. If the number of pills
or frequency of dosages change, physicians can update the medication schedule for the patient and generate a QR code for the medication schedule using the web app. The patient only has to scan the QR code using the smartphone app. When the patient returns home and comes in range of the pillbox, the pillbox schedule gets updated to the new schedule in the smartphone.

4) Privacy and Security Considerations: The smartphone app is protected by a user password. Besides the user password, there are several data security issues concerning the smartphone application. In this section, we discuss three important privacy issues and present solutions for resolving them.

The first issue is the security of the wireless communication between the smartphone and pillbox. Bluetooth version 4.2 (BLE) provides AES-CCM cryptography, a 128-bit encryption standard. This inexpensive encryption is already integrated into our wireless communication protocol of choice (BLE), making it an ideal solution for secure transmission between the pillbox and smartphone.

The second concern is the accessibility of personal medical records inside of the phone’s storage. To protect this data, we encrypt these records using 128-bit AES-CBC cryptography.

The third privacy concern involves securely transferring medical records as well as keys for encryption between the personal smartphone and care providers. Our system uses RSA 1024-bit cryptography to encrypt the medical records before transferring the data to the care provider. To obtain the key used for encryption to the smartphone application, we do not use an open channel such as the Internet. Instead, we use a side channel, via scanning a QR code. The care provider shares a QR code containing the public key for encryption with the patient. The patient must physically scan the QR code in order to receive the key. By following this process, the key never appears in any public channel. The process of transferring the public key is further illustrated in section 3.4.

D. Physician’s Web App and a Data Forwarding Server

The web application provides an intuitive interface for physicians to control functionalities related to patient records. The web application has two primary functions: generating medication schedules and obtaining medication adherence records from patients. The web app provides a secure means of access for all these functionalities to ensure that the privacy and confidentiality of the patient is not compromised. In some cases, when the phone and physician’s computer don’t have a public IP address, a Data Forwarding Server is implemented between the web app and the smartphone application to forward data transferred from the smartphone to the web app.

1) Single-Use Secured Channel with Time-to-Live: The web app is used by the physician whenever the patient meets him or her during face-to-face sessions. The web app generates a one-time-use RSA encryption key pair locally, and shows a QR code on the physician’s computer which contains the RSA public key. This QR code is scanned by the patient using his smartphone app to initiate the transfer of the adherence records. The smartphone app encrypts the data using the public key and sends the data to the physician’s web app directly via an open channel. The web app can decrypt the data within a predetermined time-to-live (TTL) limit, default 10 minutes, of generating the key. After the TTL has elapsed, the web page refreshes itself, generating a new QR code with a new RSA key-pair. The old key-pair is dropped from the cache to prevent future access permanently. If the physician needs to save the data for future use, the web page can be directly saved.

2) Data Forwarding Server: Because the patient’s smartphone and the physician’s computer usually sit behind NATs, they may not have public IP addresses. Therefore, we need a server for forwarding encrypted data from the smartphone to the web app. In addition to the RSA key-pair, the web app also generates a temporary universally unique identifier (UUID) to identify the message. This UUID is integrated in the QR code scanned by the smartphone app, and is also included with the encrypted data sent by the smartphone to the server. The message can be temporarily stored on the server for a short period of time (TTL set as 10 minutes); within this period, the web app can only query messages with their corresponding UUID. Once this period expires or if the server successfully queries the data once, the data is dropped. With this design, the server never has access to the encryption key, so the data cannot be compromised during the forwarding. Additionally since the UUID is not generated by the server, the server does not have any detailed information about the origin or destination of the data.

3) Advantages of a Non-User Related Design: As the purpose of the web application is only to receive and show the data, we do not need any user-related design. This has some extra advantages. First, there is no static data mapping to any user, which provides extra security to patient data. Even if the data is compromised, an outsider will not be able to associate the data with the original patient and intended physician. Secondly, a simple user interface will allow physicians to learn how to use the application in very little time.
4) **Historical Records Interface:** Once a patient’s data has been sent to the physician’s web application, the physician can view the historical records through an intuitive, responsive interface. Days are marked in red to indicate that the patient forgot to take pills at the prescribed times, or in yellow to indicate that pills were taken at improper times during the day. All days can be moused over to view more details. The interface was designed to be simple and easy to use for physicians. A screenshot of the interface is show in Figure 12.

5) **Generating Medication Schedules:** When the physician prescribes medication, the dosage schedule is entered into the web app and the web app generates a QR code which contains this information. Figure 13 displays the page that physicians will be able to access to create new medication schedules for patients. The patient’s smartphone is used to scan the QR code and the medication regimen is stored on the phone, ready to be transferred to the pillbox upon connection. By using QR code, it reduces the process of establishing a channel on Bluetooth or TCP/IP to just a scan. It is simple for both physicians and patients, also improve the security.

6) **Privacy and Security Considerations:** The action of sending medication records to physicians must be a secure operation. Figure 14 illustrates the communication between the patient’s smartphone and the physician or hospital’s web application. An end-to-end secure channel is established for successful transmission of patient records. A public-private key cryptography system is used for this secure transfer. This public key is transmitted via a side-channel (QR code) and used for encrypting the records to be transferred. If the patient fails to use this QR code and send the records within a particular time frame of the QR code creation, the transfer of records fails. This measure ensures that this session is time limited enabling better security. The private key which maintained on the physician’s side ensure that the physician is the only person who can access to the records. In cases when the patient is required to remotely send the records, the physician uses alternative forms of out-of-band communication such as E-Mail to send the QR code to the patient to scan. The patient then scans this QR code with the same TTL. An important aspect of this system is that a new key pair is generated every time a medication record transfer takes place, with a limited time window. The public-private key pairs are generated dynamically by the web app (not stored on the server), and only works for the duration of the TTL.

IV. EVALUATION

We evaluate our system in terms of cost, scalability, accuracy, and robustness of pill detection, as well as the ability for the system to preserve patient’s data privacy.

A. Security

Our system improves the privacy of patient medication records by applying end-to-end encryption using public-key cryptography with keys obtained via out-of-band communication channels. We evaluate the security of the medication record in several aspects.

1) **Key Exchange Process:** The pairing key exchange of BLE happens when the smartphone pairs with the pillbox, which adheres to the Bluetooth standard. Meanwhile, we used a customized key exchange process for transmission between the smartphone app and web app, and here we discuss the security of the exchange between the smartphone and web applications.

   The Man In The Middle (MITM) attack is the most common attack format for a public-private-key encryption system; this occurs when a third party transmits a forged public key for encryption. In our implementation, the key is exchanged in a out-of-band channel (scanning a QR code), which is much more difficult to hack from the network. The data security does not depend on the security of network connection, but rather on the integrity of software and the physical security of the physician’s office (which is out of the scope of this research).

2) **End-to-End Data Security:** To provide full medical data security, we need to ensure the security in the entire pipeline before and after our system.

   The medication adherence data is stored in the patient’s smartphone using AES encryption and is only decrypted when it has to be sent to the physician’s web app. This process prevents data leaks to third parties if the phone’s internal storage is compromised.

   To avoid security breach due to the smartphone being impersonated, the hospital/physician may help the patient install the genuine version of the smartphone app during the deployment process. This is to avoid the distribution of possible fake applications that impersonate the actual application; these fake applications can steal patient data very easily if the patient is
tricked into downloading them. Additionally, a malware scan for the smartphone OS can be required if necessary.

Some of the recent patient records are cached in a hardware buffer inside the chip. The Bluetooth pairing passcode to the pillbox is distributed separately from the pillbox; if the pillbox is lost, there is no way to access the stored data.

The data post-processing should ensure that medication records will not be leaked in the future. Based on the patient’s authorization of medication adherence data, the system makes the data available to the physician for only a limited time as indicated by the patient while sending the data from the smartphone to the physician’s web application. Furthermore, the system uses a new RSA key pair for each transmission which ensures better protection against attacks.

B. Cost and Scalability

In this section, we provide the cost of individual parts that went into building the pillbox. We also compare the cost of our pillbox with that of several commercially available pillboxes. The cost per unit at 3000 numbers per component is listed in Table I. The price of various commercially available smart pillbox are listed in Table II. It is to be noted that most of the commercially available pillboxes do not have any pill detection mechanisms.

<table>
<thead>
<tr>
<th>Class</th>
<th>Component</th>
<th>Price</th>
<th>Quantity</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pill Detection</td>
<td>Light Sensor</td>
<td>0.6</td>
<td>28</td>
<td>16.8</td>
</tr>
<tr>
<td></td>
<td>BH1750</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch</td>
<td>0.2</td>
<td>28</td>
<td>5.6</td>
</tr>
<tr>
<td>IC</td>
<td>NRF51422</td>
<td>2.28</td>
<td>1</td>
<td>2.28</td>
</tr>
<tr>
<td></td>
<td>(256K FLASH)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SN74HC595C</td>
<td>0.17</td>
<td>8</td>
<td>1.36</td>
</tr>
<tr>
<td></td>
<td>IDTQ2526</td>
<td>0.25</td>
<td>4</td>
<td>0.92</td>
</tr>
<tr>
<td>Power Supply</td>
<td>Power Adapter</td>
<td>3.4</td>
<td>1</td>
<td>3.4</td>
</tr>
<tr>
<td>Battery</td>
<td>18650</td>
<td>1.5</td>
<td>2</td>
<td>3.0</td>
</tr>
<tr>
<td>Mechanical</td>
<td>Mode and Plastic</td>
<td>1.5</td>
<td>1</td>
<td>1.5</td>
</tr>
<tr>
<td>Other Components</td>
<td>Components</td>
<td>8</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>SUM</td>
<td>-</td>
<td>-</td>
<td>USD</td>
<td>64.596</td>
</tr>
</tbody>
</table>

TABLE I
SYSTEM COST COMPARISON TO DIFFERENT PILLBOX SYSTEMS (USD)

<table>
<thead>
<tr>
<th>Name</th>
<th>Cost (USD)</th>
<th>Pill Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tricella</td>
<td>74.99</td>
<td>no</td>
</tr>
<tr>
<td>My uBox</td>
<td>25/month</td>
<td>no</td>
</tr>
<tr>
<td>MedMinder Jon</td>
<td>55.99/month</td>
<td>no</td>
</tr>
<tr>
<td>Hero Pill Dispenser</td>
<td>599</td>
<td>appearance of container</td>
</tr>
<tr>
<td>Our Pillbox</td>
<td>64.596</td>
<td>yes</td>
</tr>
</tbody>
</table>

TABLE II
COMPARISON TO DIFFERENT PILLBOX SYSTEMS

C. Pill Detection

To evaluate the robustness of our pill detection mechanism, we conducted 3 different tests. The test was done using 10 pills of different sizes, as shown in Figure 15. The first test was done by putting one pill at a time of each size and verifying the detection rate over 15 trials. In the second test, 2 pills of the same size were simultaneously placed in the containers and the detection rate was again noted for 15 trials. The third test was conducted by mixing different sized pills. For each test, the pills were placed in random containers. The pill detection mechanism achieves an accuracy of 99.7% on uniform pills and 98.3% on mixed pills as shown in Table III and Table IV, respectively.

<table>
<thead>
<tr>
<th>Pill</th>
<th>One Pill Test</th>
<th>Two Pill Test</th>
<th>Total Trials</th>
<th>Success Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>15</td>
<td>15</td>
<td>30</td>
<td>100%</td>
</tr>
<tr>
<td>2</td>
<td>15</td>
<td>15</td>
<td>30</td>
<td>100%</td>
</tr>
<tr>
<td>3</td>
<td>15</td>
<td>15</td>
<td>30</td>
<td>100%</td>
</tr>
<tr>
<td>4</td>
<td>15</td>
<td>15</td>
<td>30</td>
<td>100%</td>
</tr>
<tr>
<td>5</td>
<td>15</td>
<td>15</td>
<td>30</td>
<td>100%</td>
</tr>
<tr>
<td>6</td>
<td>15</td>
<td>15</td>
<td>30</td>
<td>100%</td>
</tr>
<tr>
<td>7</td>
<td>15</td>
<td>15</td>
<td>30</td>
<td>100%</td>
</tr>
<tr>
<td>8</td>
<td>15</td>
<td>14</td>
<td>30</td>
<td>96.7%</td>
</tr>
<tr>
<td>9</td>
<td>15</td>
<td>15</td>
<td>30</td>
<td>100%</td>
</tr>
<tr>
<td>10</td>
<td>15</td>
<td>15</td>
<td>30</td>
<td>100%</td>
</tr>
<tr>
<td>Total</td>
<td>150</td>
<td>149</td>
<td>300</td>
<td>99.7%</td>
</tr>
</tbody>
</table>

TABLE III
UNIFORM PILL DETECTION ACCURACY

<table>
<thead>
<tr>
<th>Number of Different Pills</th>
<th>Pill Detected</th>
<th>Total Trials</th>
<th>Success Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>14</td>
<td>15</td>
<td>93.3%</td>
</tr>
<tr>
<td>3</td>
<td>14</td>
<td>15</td>
<td>100%</td>
</tr>
<tr>
<td>4</td>
<td>15</td>
<td>15</td>
<td>100%</td>
</tr>
<tr>
<td>5</td>
<td>15</td>
<td>15</td>
<td>100%</td>
</tr>
<tr>
<td>Total</td>
<td>59</td>
<td>60</td>
<td>98.3%</td>
</tr>
</tbody>
</table>

TABLE IV
MIXED PILL DETECTION ACCURACY

D. User Studies

To evaluate the efficiency of interaction, 9 people of different ages, backgrounds, and occupations were invited to test the system, as either a physician or as a patient. They are officers, security guards, engineers, students, and the ages are in the range of 25 to 55.

Each patient is assigned 4 dosages over a time span of 6 hours. To simulate the experiences of patients with forgetfulness, the participants were not informed of the dosage schedule beforehand; thus, the participants remain unaware of
the actual dosage time until they are given a system alert. In each dosage time window, participants are given 3 notifications at 10 minute intervals, they are a blinking LED on the pillbox, a text alert from the participant’s smartphone, and a final sound alarm. The aim of the experiment is to determine which notifications elicit a response, and when a participant takes the dosage. During the experiment, the pillbox is put on the table in the participant’s work area or office, and the participants are asked to focus on their work. After the participants get he notification from the pillbox, participants need to manually record the time when the dosage is taken, and which notification triggered the response. Other participant actions outside of the dosage schedule are also recorded, such as opening and closing pill containers without removing the pills. After completing the 4 dosage schedule, the participants are asked to upload their historical data and to give feedback about the procedure.

Each physician is first shown how to update dosage schedules and upload historical data. They are then given a preset schedule, asked to update the schedule on a patient’s smartphone, and to upload the historical dosage record to the web app. The time to finish the two tasks are recorded, and the participants are asked for feedback about the procedure.

For feedback, the patients and physicians were asked four questions:

- On a scale from 0 to 5 points, How simple is the system to use?
- Which functions could be added to improve the system?
- Which currently implemented system function has the best design?
- What privacy concerns do you have when using the system?

1) Patient Response: On average, the test patients respond within 248 seconds of the first notification, and interact with the pillbox for 19 seconds; this data is shown in Table VII. From feedback gathered from the participants, lack of response to the LED notification can be attributed to the participant not being in close physical proximity to the pillbox. However, from the data in Table VII, the LED notification is often sufficient for alerting the patient.

2) Physician Task Time: The average time the physician spends on the "Update Schedule" and "Transfer Historical Record" procedures are 55.7 seconds and 37.5 seconds respectively, as shown in Table IX. After learning the procedure, the physicians expressed confidence in being able to replicate the procedure. Additionally, each physician was able to easily assist patients in transferring data, and to find abnormal events in the historical record.

3) User Experience and Privacy: All participants gave a positive experience rating, with patients and physicians giving
average ratings of 4.8 and 4.0 respectively, see Table VI and Table VIII. The main concerns of the physicians come from their experiences with the web application user interface, and is discussed below.

In terms of privacy, the participants were largely concerned with the lack of a login mechanism. After learning of the security design of the pillbox system and the system architecture, however, the participants expressed confidence in the system and believed that the security design would help to alleviate patient privacy concerns.

4) User Feedback: After the experiment, participants were asked to give feedback about the system from the patients’ and physicians’ perspectives. Participants commented that the LED and text-based notifications, as well as the automatic data transfer improved convenience for users who may forget their medication schedules. Some suggestions for improving the system include a subsystem for easier refilling of pills, and a vibration motor for additional notifications.

Some participants were more critical of the physicians interface, stating that the web application user interface could be improved for ease of use. In particular, additional visualizations of the data, such as a historical summary, would aid the physicians in understanding the patient’s records more efficiently. However, some commented that the system is an improvement over existing solutions.

V. CONCLUSION AND FUTURE WORK

In this paper, we present an intelligent pillbox system with an emphasis on protecting the privacy of patient data and ensuring confidentiality. This system also features a reliable pill detection mechanism at low cost. The privacy of the medication adherence and medication regimen is maintained through four key components in the smart pillbox system: secure storage of pillbox activity records on the patient’s smartphone; key-pair generation by the doctor’s browser which are inaccessible to the server; transfer of the public key to the patient during face-to-face meetings with the doctor using out-of-band communication channels; and secure transfer of these records to the doctor using public key cryptography.

The tests performed in Section IV indicate the high reliability of the pill detection mechanism offered by the proposed system. Dissemination of a reliable, low-cost and secure end-to-end system will facilitate medication adherence, provide security of patient data, and has the potential to impact medical outcomes. It will not only prove to be highly beneficial for the patients and physicians, but will also instill a sense of comfort and confidence in their minds as the system ensures that their privacy is not being compromised.

In future versions of the pillbox, we propose the following improvements: a smaller and lighter version of the pillbox that is easier for patients to carry and use; a method for automatically refilling the pillbox; and a pill detection mechanism able to determine an exact number of pills in each compartment.

In addition to improving the existing system, we are in the process of conducting additional focus group studies with doctors and patients at the Columbia University Medical Center. We plan to commercialize our prototype into a real product to be sold and used by many patients and physicians to improve medication adherence.

REFERENCES


