Requirements

- Hardware

    1. Arduino Uno
    2. Arduino Mega
    3. ESP-32 CAM
    4. R305 Finger Print Module
    5. GSM 800a Module
    6. (16x2) LCD
    7. 12v Solenoid Lock
    8. 5v Relay
    9. 12v Power Supply
    10. UART to USB connector
    11. Push Button
    12. Bread Board
    13. 10KΩ Potentiometer
    14. 10KΩ Resistor
    15. 220Ω Resistor
    16. Jumper Wires

- Software
    1. Windows 10
    2. Apache Tomcat 7 or above
    3. JAVA EE
    4. MySQL 8.0
    5. Arduino IDE
    6. Eclipse or any suitable IDE
    7. jSerialComm-2.6.0.jar
    8. mysql-connector-java-8.0.19.jar
    9. Adafruit Fingerprint Library
    10. ESP-32 CAM library

Design

- **Circuit**

1. Arduino Uno to Arduino Mega Connection

GND pin of Arduino Uno is connected to GND pin of Arduino Mega.
Pin 11 of Arduino Uno is connected to RX2 pin of Arduino Mega. Pin 10 of Arduino Uno is connected to TX2 pin of Arduino Mega. These pins are connected to establish Serial Communication between both the microcontroller.

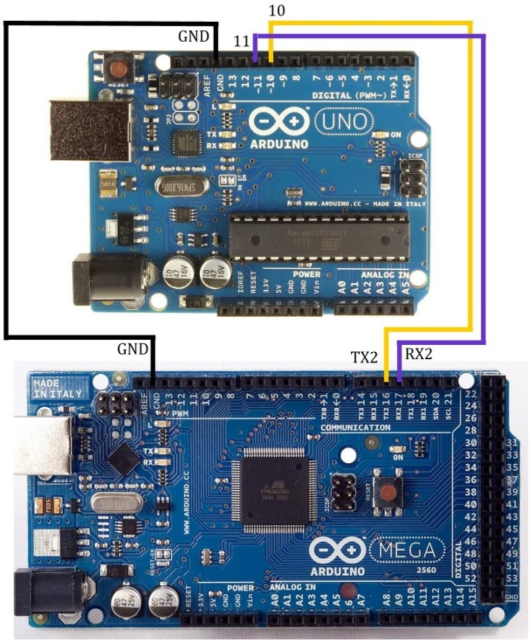


Figure 1. Arduino Uno to Arduino Mega Connection

2. Arduino Mega to R305 Finger Print Module Connection

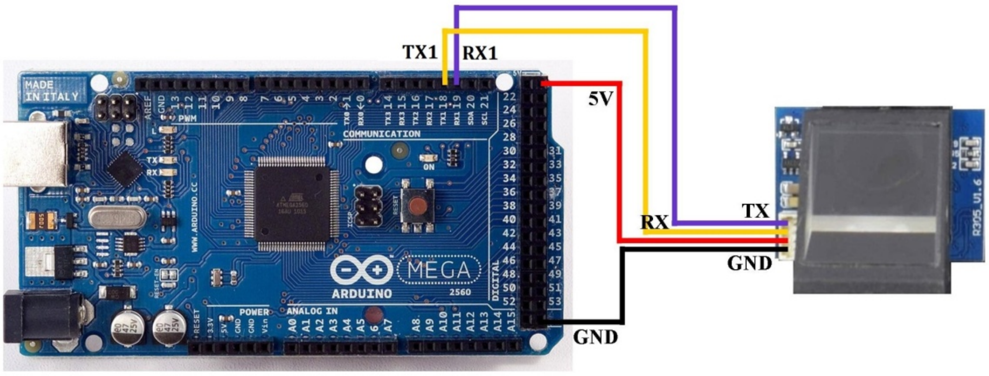


Figure 2. Arduino Mega to R305 Finger Print Module Connection

GND pin of Finger Print module is connected to Arduino Mega. VCC pin of Finger print module is connected to 5V pin of Arduino Mega for power supply. TX pin of Finger Print module is connected to RX1 pin of Arduino Mega. RX pin of Finger Print module is connected to TX1 pin of Arduino Mega. These pins are connected to establish Serial Communication between both the microcontroller.

3. Arduino Mega to GSM 800a Module Connection

GND pin of GSM 800a Module is connected to GND pin of Arduino Mega. TX pin of GSM 800a Module is connected to RX3 pin of Arduino Mega. RX pin of GSM 800a Module is connected to TX3 pin of Arduino Mega. These pins are connected to establish Serial Communication between both the microcontroller.
External 12V DC power supply is provided to GSM 800a Module.

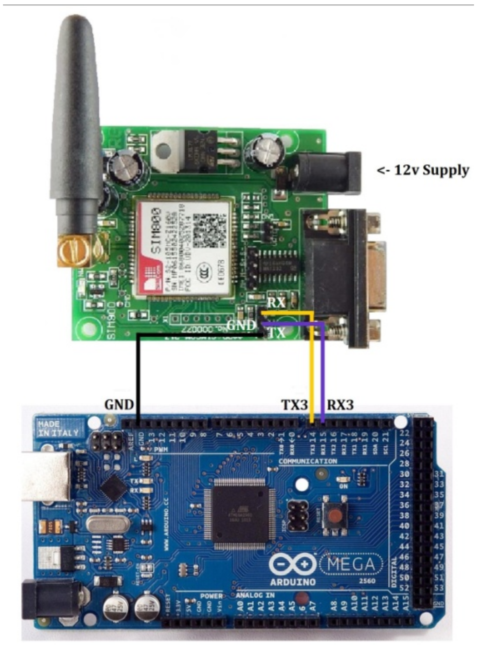


Figure 3. Arduino Mega to GSM 800a Module Connection

4. Arduino Mega to (16x2) LCD Connection

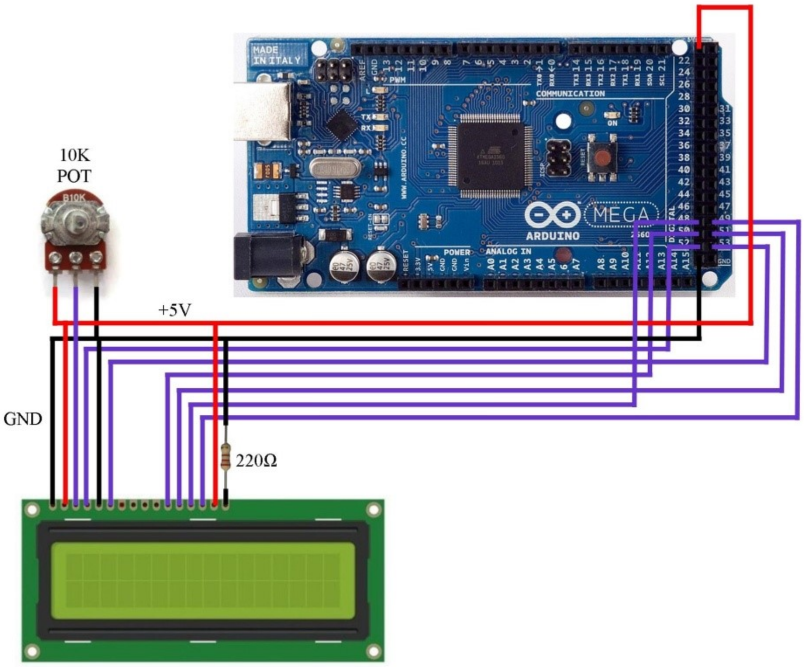


Figure 4. Arduino Mega to (16x2) LCD Connection

VSS pin of (16x2) LCD is connected to GND pin of Arduino Mega. VDD pin of (16x2) LCD is connected to +5v pin of Arduino Mega. VE pin of (16x2) LCD is connected to 10k potentiometer as shown in the figure above. RS pin of (16x2) LCD is connected to pin 52 of Arduino Mega. RW pin of (16x2) LCD is connected to GND. E pin of (16x2) LCD is connected to pin 53 of Arduino Mega. D4 pin of (16x2) LCD is connected to pin 50 of Arduino Mega. D6 pin of (16x2) LCD is connected to pin 51 of Arduino Mega. D6 pin of (16x2) LCD is connected to pin 48 of Arduino Mega. D7 pin of (16x2) LCD is connected to pin 49 of Arduino Mega. BA pin of (16x2) LCD is connected to +5v. BC pin of (16x2) LCD is connected to 220Ω resistor which is connected to GND.

5. Miscellaneous

GND pin of 5V Relay is connected to GND pin of Arduino Mega. VCC pin of 5v Relay is connected to +5v of Arduino Mega. IN pin of 5v Relay is connected to pin 45 of Arduino Mega. COM of 5v Relay is connected to +ve terminal of 12v power supply. NO of 5v Relay is connected to Solenoid Lock. –ve terminal of 12v power supply is connected to Solenoid Lock.
Push Button is Connected to Arduino Mega with help of 10KΩ resistor as shown in the figure.

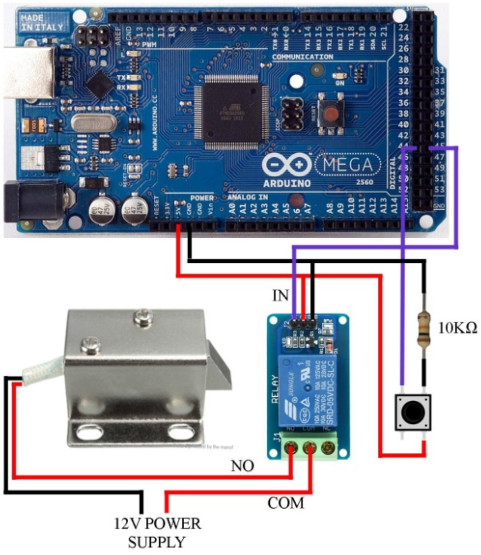


Figure 5. Arduino Mega, Solenoid Lock, 5V Relay, Push Button Connection

Both Arduino Uno and Arduino Mega is to be connected to a Computer in which Server is running.
A valid SIM is to be inserted into GSM 800a Module.
+5v /+3.3v and GND of ESP-32 CAM is to be provided either by any of the Arduinos or through an external power supply.

- **Code**

Complete code for the project is available at-
https://github.com/abhradipg/IOT_home_security/
Code for database:
https://github.com/abhradipg/IOT_home_security/blob/master/Databasecode.txt
Code for Uno: https://github.com/abhradipg/IOT_home_security/tree/master/uno
Code for Mega: https://github.com/abhradipg/IOT_home_security/tree/master/mega
Code for Web Server:
https://github.com/abhradipg/IOT_home_security/tree/master/iot_lock1
Code for ESP-32 cam : https://github.com/easytarget/esp32-cam-webserver

Result & Analysis

1. Login Page:

Login Page is shown in the adjacent figure. Here a user can login using a valid Username and Password. Someone having OTP to access the lock can open the lock by entering OTP which can be generated for any mobile number by an authorised user. If OTP is correct then it opens the lock and welcome message is displayed in LCD. And if mobile notification is turned on it sends notification to registered mobile number as shown in figure 18 and logs the time and username in database in server. After the user is logged in Main Menu is displayed.

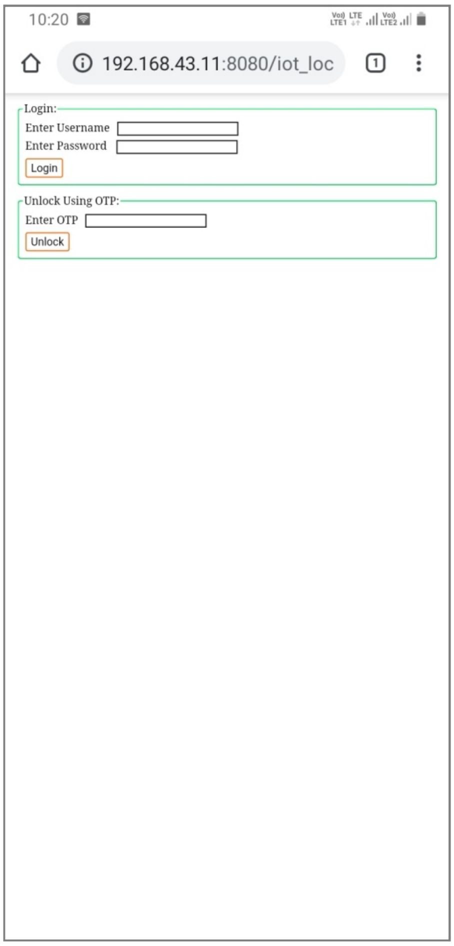


Figure 6. Login Page

2. Main Menu

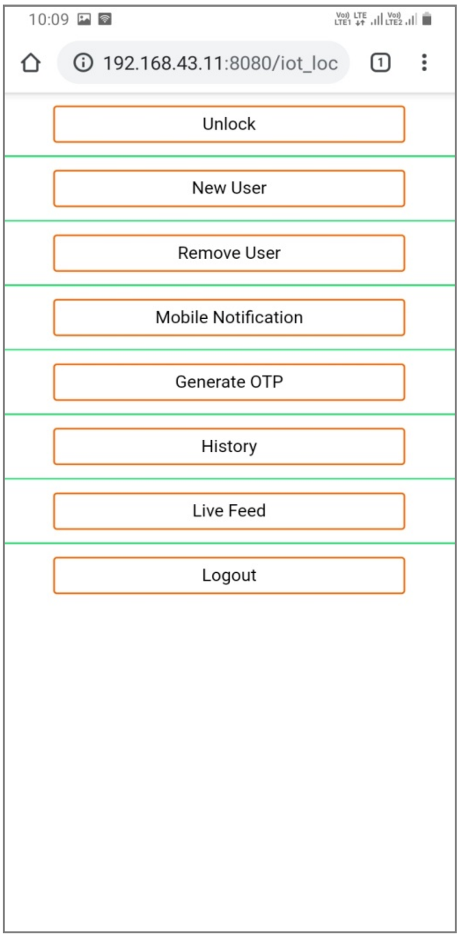


Figure 7. Main Menu

Main menu is shown in the adjacent figure. It has option to "Unlock" which opens the lock and welcome message is displayed in LCD. And if mobile notification is turned on it sends notification to registered mobile number as shown in figure 18 and logs the time and username in database in server.

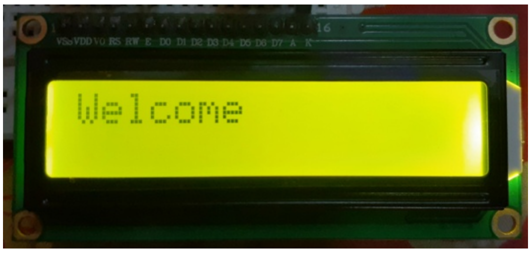
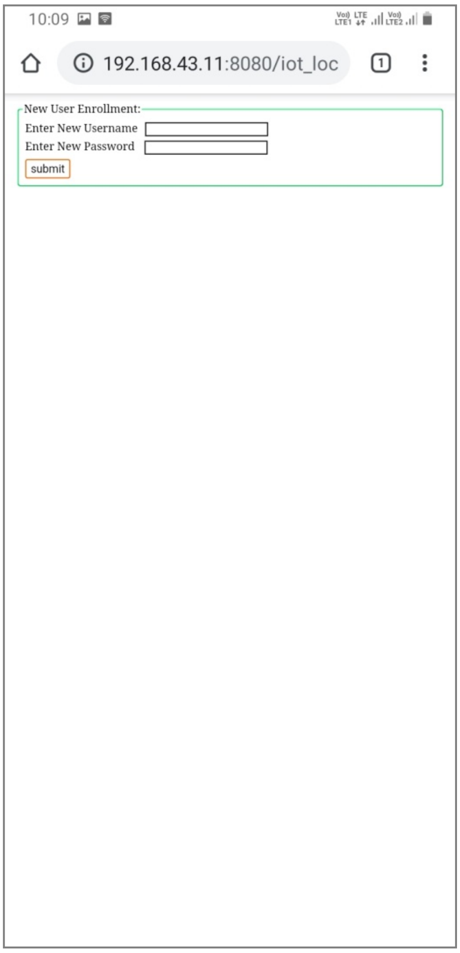


Figure 8. Welcome Message

3. New User Enrolment

By clicking "New User" in the Main Menu it opens the page to new user enrolment, where a new user has to create his username and password. After clicking "submit" LCD screen shows message to place finger as shown in the figure below. The new user then has to place his finger on finger print sensor to register his finger print. Appropriate message is display on the LCD whether Fingerprint is registered or some error occurred. After an user is added a notification is sent for the same to registered mobile no. if notifications are enabled as shown in figure 19.



New User Enrollment:

Enter New Username

Enter New Password

Figure 9. New User Enrolment page

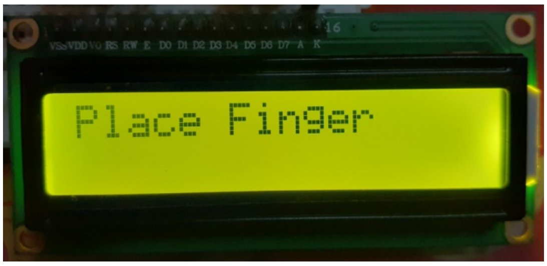
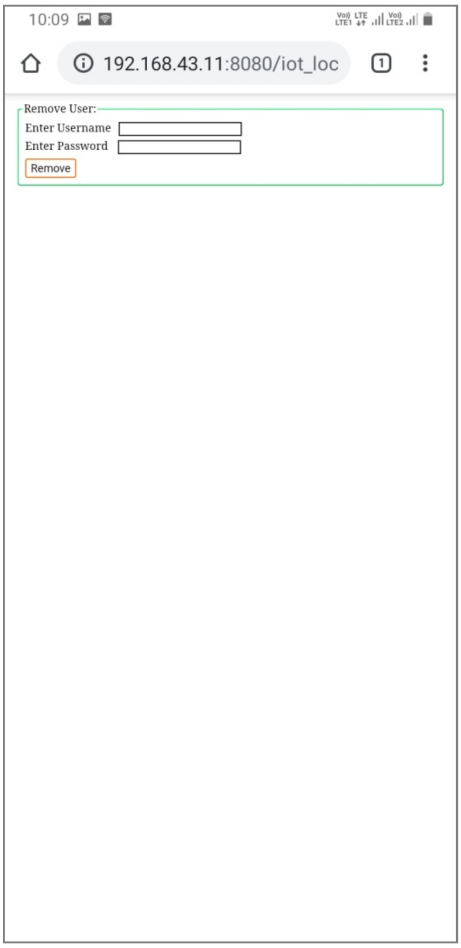


Figure 10. Place Finger Message

4. Remove User



Remove User:

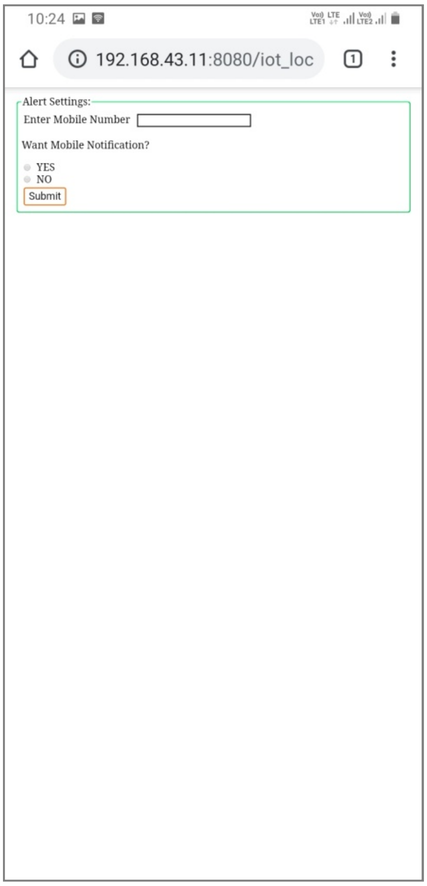
Enter Username

Enter Password

Figure 11. Remove User page

By clicking "Remove User" in the Main Menu it opens the page to remove user, where we have to enter username and password of the user we want to remove. After clicking "Remove" if the entered information is correct. All the information about the user is removed from the database and if notifications are enabled then notification about the same is sent to the registered mobile number.

5. Mobile Notification Setting


10:24

192.168.43.11:8080/iot_loc

Alert Settings:

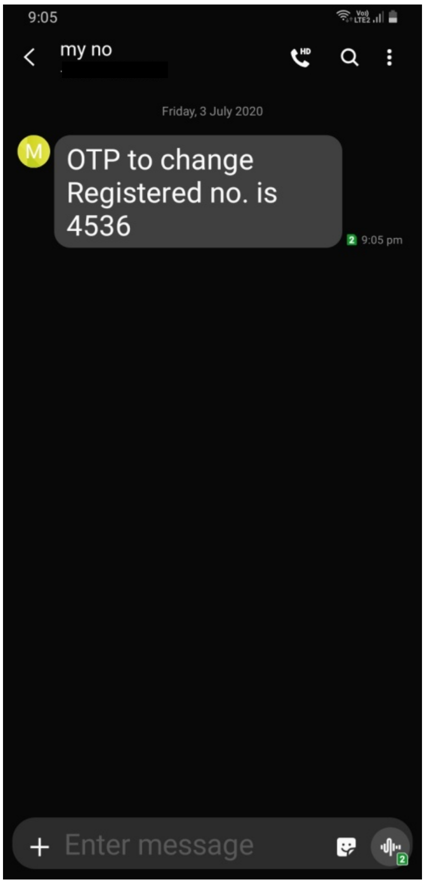
Enter Mobile Number ▭

Want Mobile Notification?

○ YES
○ NO

Submit

Figure 12. Alert Settings page


9:05

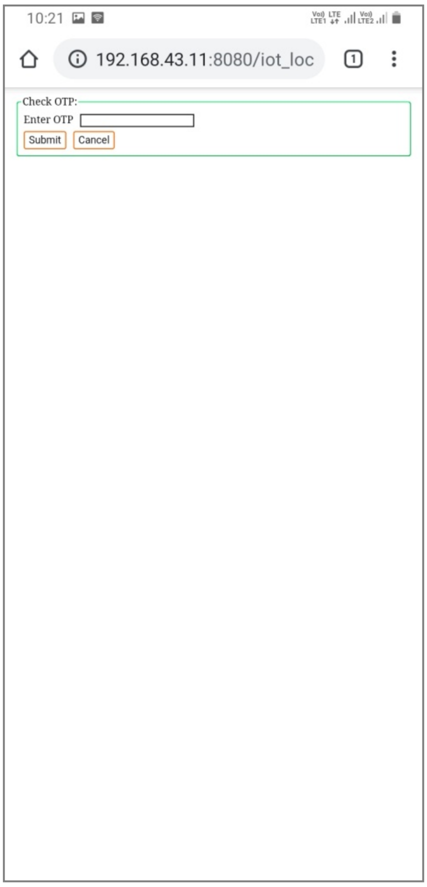
my no
[redacted]

Friday, 3 July 2020

M OTP to change Registered no. is 4536

9:05 pm

Figure 13. OTP to change no.


10:21

192.168.43.11:8080/iot_loc

Check OTP:

Enter OTP ▭

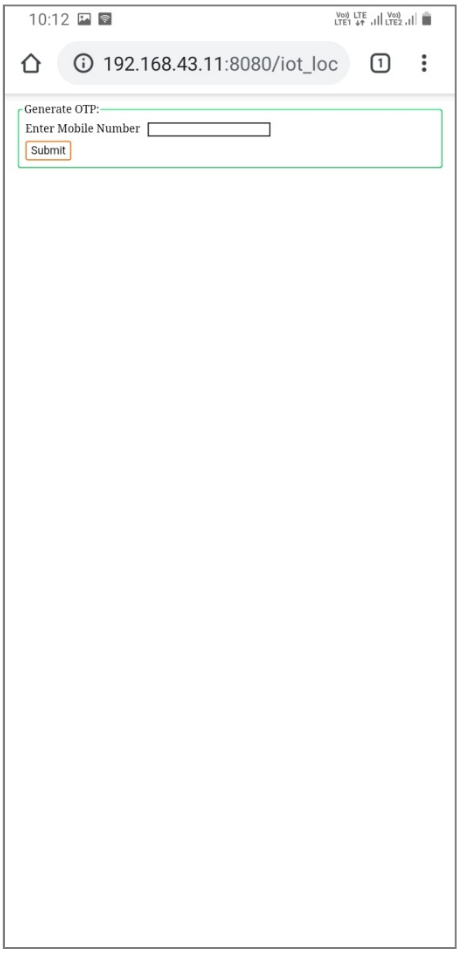
Submit Cancel

Figure 14. Form to enter OTP

By clicking on “Mobile Notification” in the Main Menu we can change the settings for SMS alert which the system sends whenever anyone tries to access the lock, when a user is added or when a user is removed. We need to enter mobile number then we have to select weather we want mobile notification or not after that we need to click on “Submit”. After that an OTP is sent to the entered mobile number as shown in figure 13, we need to enter the OTP in check OTP page and click on “Submit” to change the settings or we can click on “Cancel” to cancel the request.

6. Generate OTP

A registered user can generate OTP for someone else who wants to access the lock. In order to do so we need to click on “Generate OTP” option in the Main Menu. After that in the page to generate OTP we need to enter the mobile number of the person who wants to access the lock and click “Submit”. By doing so an OTP is sent to entered mobile number as shown in Figure 16. In order to access the lock the person needs to enter the OTP in Login Page.

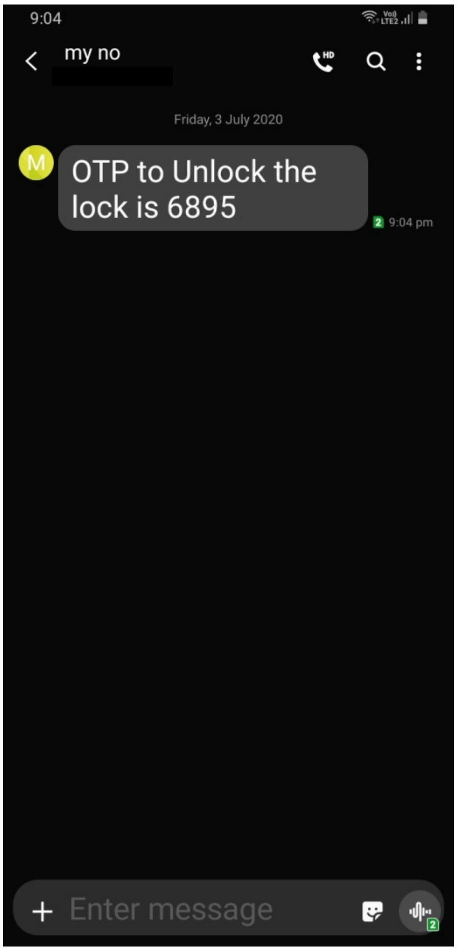


Generate OTP:

Enter Mobile Number

Submit

Figure 15. Generate OTP page



OTP to Unlock the lock is 6895

Figure 16. OTP message

7. History

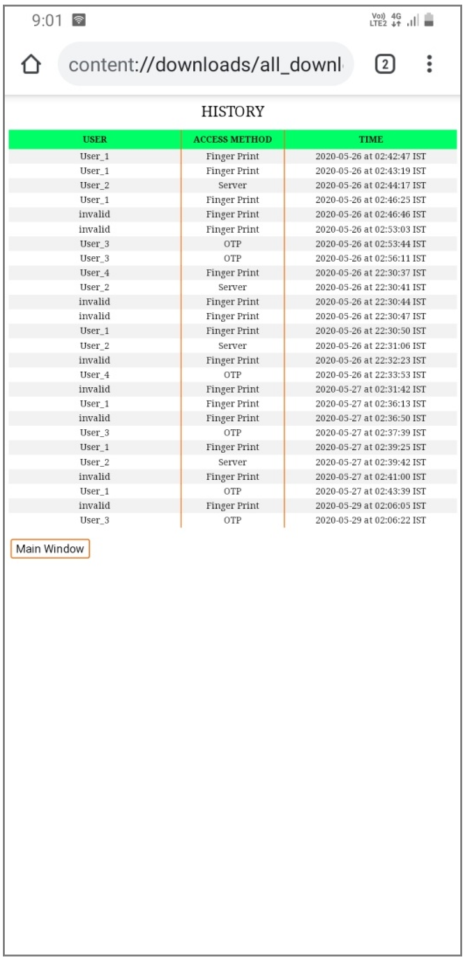
In order to watch who has accessed the lock and when the user need to click on “History” option in the Main Menu. By clicking it, it shows the complete log of who, how and when accessed the lock as shown in figure 17. First column shows the username of the user who has accessed the lock. The second column shows how the user has accessed the lock, if the user has accessed the lock physically then it shows “Finger Print” as the access method or if the user has accessed the lock from the web application then it shows “Server” in the access method or if the user has generated an OTP to access the lock which is used to access the lock then it shows “OTP” as the access method. Lastly, the third column shows date and time of when the lock has been accessed.

8. Live Feed

By clicking on “Live Feed” option in the Main Menu the user can access the camera and can watch its feed in real time.

9. Logout

User can logout from the web application by clicking on “Logout” option in the Main Menu.



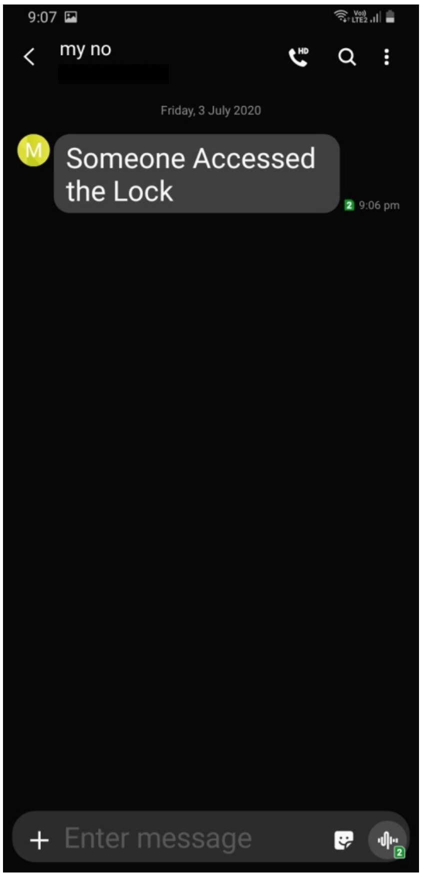
HISTORY

USER	ACCESS METHOD	TIME
User_1	Finger Print	2020-05-26 at 02:42:47 IST
User_1	Finger Print	2020-05-26 at 02:43:19 IST
User_2	Server	2020-05-26 at 02:44:17 IST
User_1	Finger Print	2020-05-26 at 02:46:25 IST
invalid	Finger Print	2020-05-26 at 02:46:46 IST
invalid	Finger Print	2020-05-26 at 02:53:03 IST
User_3	OTP	2020-05-26 at 02:53:44 IST
User_3	OTP	2020-05-26 at 02:56:11 IST
User_4	Finger Print	2020-05-26 at 22:30:37 IST
User_2	Server	2020-05-26 at 22:30:41 IST
invalid	Finger Print	2020-05-26 at 22:30:44 IST
invalid	Finger Print	2020-05-26 at 22:30:47 IST
User_1	Finger Print	2020-05-26 at 22:30:50 IST
User_2	Server	2020-05-26 at 22:31:06 IST
invalid	Finger Print	2020-05-26 at 22:32:23 IST
User_4	OTP	2020-05-26 at 22:33:53 IST
invalid	Finger Print	2020-05-27 at 02:31:42 IST
User_1	Finger Print	2020-05-27 at 02:36:13 IST
invalid	Finger Print	2020-05-27 at 02:36:50 IST
User_3	OTP	2020-05-27 at 02:37:39 IST
User_1	Finger Print	2020-05-27 at 02:39:25 IST
User_2	Server	2020-05-27 at 02:39:42 IST
invalid	Finger Print	2020-05-27 at 02:41:00 IST
User_1	OTP	2020-05-27 at 02:43:39 IST
invalid	Finger Print	2020-05-29 at 02:06:05 IST
User_3	OTP	2020-05-29 at 02:06:22 IST

Figure 17. History page

10. Physically accessing the Lock

In order to physically access the lock the user has to press the push button. By doing so, “Place Finger” message will be shown in the LCD after that the user has to place his finger on Fingerprint Sensor to access the lock if the fingerprint matches any other fingerprint in the database the lock is opened and “Welcome” message is displayed in the LCD. Information about every access is logged in the database in the server and if notifications are enabled then a SMS about the same is send to the registered mobile number.



[redacted]

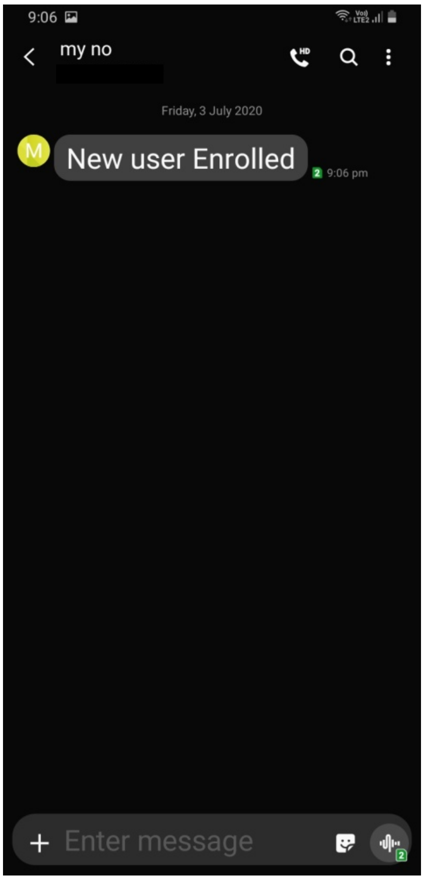
Friday, 3 July 2020

M

Someone Accessed the Lock

9:06 pm

Figure 18. Access Notification



[redacted]

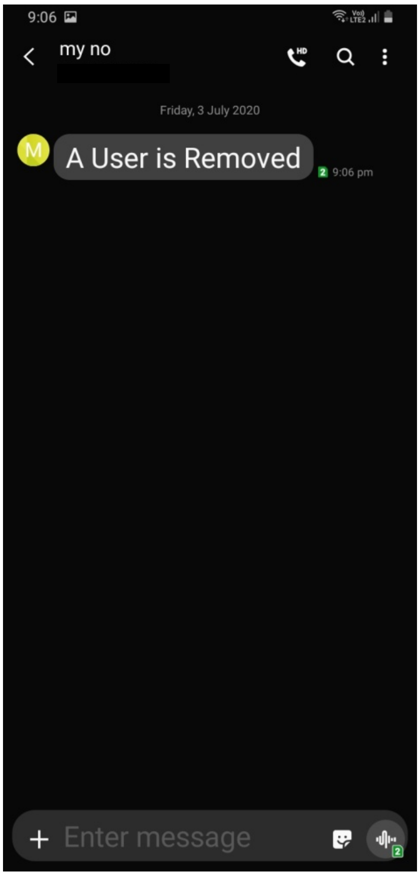
Friday, 3 July 2020

M

New user Enrolled

9:06 pm

Figure 19. User Added Notification



[redacted]

Friday, 3 July 2020

M

A User is Removed

9:06 pm

Figure 20. User Removed Notification