Smart Intrusion Detection

Shubham Chopade[1], Atharva Kulkarni[2], Yash Chavan[3]
[1,2,3]*Student, Department of Electronics and Telecommunication, PCCOE, Pune, India*

***Abstract*: With the exponential increase in trespassing and thefts, home security has become a need of the hour. This being said, there are hundreds of different products in the market which claim to provide home security. Typical systems include alarms, cameras or motion trackers. But there is an inherent problem associated with each of these systems. Camera based systems generally record the footage of the crime and store it in a database which could only be accessed physically; alarm-based systems trigger an alarm which may or may not be heard; and lastly motion trackers detect motion and triggers an alarm or a light bulb. These systems could be categorized as open loop systems which do not provide any type of feedback to the user when he/she is not in vicinity. Although the most reliable system from the above is a camera-based system, people hesitate to install CCTV in their dwellings; the reason being high cost and violation of privacy. Thus, to get over the problems faced by using traditional security systems, we designed a low cost closed loop home security system. It does not consist of a camera, which helps in protecting one's privacy as well as reduce the cost.**

***Keywords*: Home security, intruders, low cost.**

1. Introduction

We plan to create a system which could eliminate the hurdles of cost, privacy, and feedback. This system would work using the IoT platform which is fit with a microwave sensor, Hall Effect sensor and accelerometer, microcontroller ESP8266, and rechargeable batteries. The system will detect the presence of an intruder in one's dwelling at any undesired time and notify the user by a high priority pop-up notification on an Android Smartphone. It also offers the functionality of connecting with multiple trusted users. The device also offers the facility of arming and disarming the alarm system according to the presence of device in the vicinity; using the location-based services. The primary aim of our project is to provide the people in India with a smart and reliable home security system. The system will not only detect the intruder's presence but also, notify the owner with a high priority notification on Android smartphone. There are other ways to make the owner aware about the trespassing in his/her dwelling like, sending an SMS or making a high priority call. These other modes are accessed only when the user is not connected to the internet. When an intrusion is detected by the device, the data is first collected by the device. It is checked whether the intrusion detected is of the family member itself using the location services of the user. If the condition is true, then no alarm will be generated. Otherwise, the data will be sent over the cloud and accordingly the user will be informed by the notification. The mandatory conditions for using our system are: at least one smartphone at the user's house, uninterrupted Wi-Fi connection with internet connected. The smartphone is a mandate because Android is the only way the device can be configured. We have developed an android app for the same. Also, internet will ensure that the notifications are being delivered to the owner.

2. Methodology

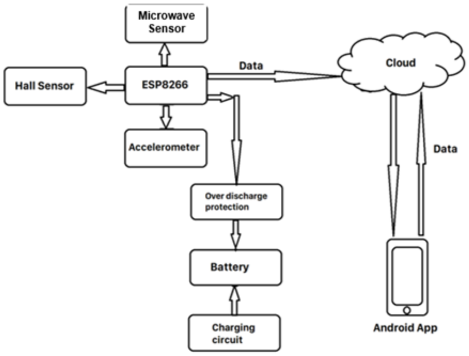


Fig. 1. Block diagram of system

The flow of data is explained in the below Fig. 1. Initially the data is collected by the micro-controller using the sensors. Then the processed data is checked with the cloud and if the conditions match, then the user is notified on the android app. The whole system is battery backed therefore, contains circuits like charging circuit and over discharge protection. Fig. 1. Shows the basic interfacing of three sensors with the microcontroller ESP8266. The microcontroller has 16 GPIO pins which can be used to connect different input and output transducers. It is a low power 32-bit RISC processor with high durability and compactness. The most important aspect of this processor is it has inbuilt Wi-Fi module. Therefore, it can be used for internet of things (IoT) applications. At the input side of the block diagram, there are three sensors connected namely; Hall Magnetic Sensor 3144 Module, MPU-6050 Six-Axis accelerometer and Microwave Sensor. Out of the three sensors, accelerometer and hall sensor must be mounted on the door or window. The main operation is identifying the changes in the position of the door or window. The accelerometer basically measures acceleration forces. This electromagnetic device is mounted on a module MPU-6050 six-axis. The module consists of 3-axis accelerometer and 3-axis gyroscope which processes complex 6-axis motion fusion algorithms; which in-turn can be used to detect both the acceleration forces as well as tilt of the device. There are 8 pins provided to access this module. It offers a range of functionalities like serial clock (SCL), serial data (SDA), Auxiliary Serial data (XDA), Auxiliary serial clock (XCL), I2C address select (AD0), interrupt (INT), the other two pins for the supply voltage (VCC) and ground (GND). The use of gyroscope can be used in further development of our system. Hall effect magnetic sensor works on the principle of hall effect. Basically, the output voltage of the device varies with the changes in magnetic field. It is a three-terminal sensor; input voltage (1) with range 4.5V-6V, ground (2), output voltage (3). Since, the input voltage requirement is more than all of the other devices, there needs to be a separate supply for this sensor. Radar microwave sensor uses "microwave doppler radar" technique to detect a moving object. This sensor has been developed as an alternative to PIR motion sensor. Unlike PIR sensor it only detects the objects reflecting back specific frequencies. Hence, it can be calibrated to detect only humans. The additional feature that it adds to our system is pet friendliness. This feature is important because, the device must not generate any false alarms. It would hamper reliability to a great extent if any unwanted motion is detected and notified to the user. This was about the input side of our system. The microcontroller is connected to the internet all the time, ideally. Hence, the data is being continuously uploaded to the cloud using the internet. The cloud acts as a mediator between the device and user. When any information is transmitted about the device, it can be accessed by the user using a smartphone which is configured with the device. The system is designed to be portable. Hence, the microcontroller is powered by an 18650 2500 mAh Rechargeable Li-ion battery. The battery supplies a voltage of 4.2 ± 0.5V. The capacity of the battery is 2500 mAh. As per our testing results, the battery can provide a backup up to 60 days. The Lithium-Ion battery is mainly for robotic applications. It is very light weight and small size compared to Ni-Cd, Ni-MH and lead acid batteries. It has a very long life without losing charging capacity and weighs just 41 gm. Moreover, the main advantage is low self-discharge rate. The battery self-discharges by 20% in the first week but, only 4-6% in latter months. For the charging purpose, it requires a charging circuitry. Also, an over discharge protection, in case the microcontroller is drawing a heavy current.

3. Flow chart and working

Initially, when the device is in the armed state the sensors are in active state. The theft can be detected when an intruder enters the dwelling through the door or window. The placement mode of the device can be set using the android app. When the mode selected for the device is wall placement, then the radar microwave sensor is activated. This sensor detects any human motion in the room hence, generates and sends the data over the cloud. When the door or window placement mode is activated, then the user has a choice between hall sensor and accelerometer depending on the position of the device; if it is to be placed on the door then accelerometer sensor will be activated, else Hall Effect sensor will be responsible for the intrusion detection.

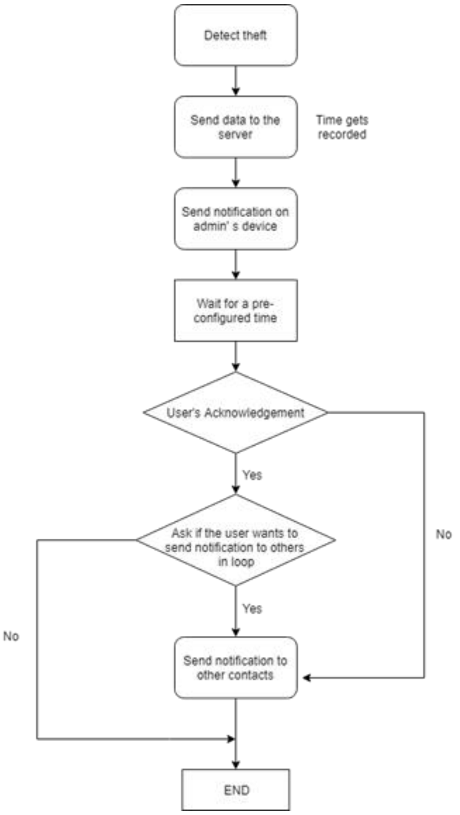
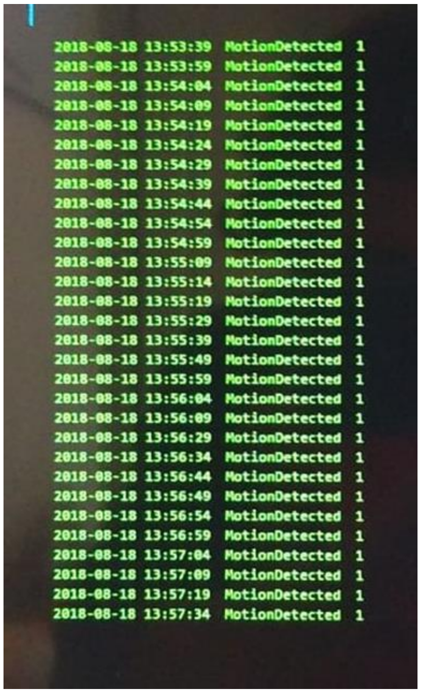

Detect theft
Send data to the server
Time gets recorded
Send notification on admin' s device
Wait for a pre-configured time
User's Acknowledgement
Yes
Ask if the user wants to send notification to others in loop
Yes
No
No
Send notification to other contacts
END

Fig. 2. Flow chart

The device goes into sleep mode when there is no activity. This act helps in power saving hence, a longer battery life. The interrupt to the microcontroller wakes it up from the sleep mode. Data is generated when an intruder enters one's dwelling. The generated data is first compared with all the default conditions. If it does not match, then it is sent over the cloud. The time when the data was generated gets recorded. If the admin's android mobile is connected to the internet, then a high priority notification will be generated else, the user will receive an automated text message, informing the user about the intrusion at his/her dwelling. It is displayed on the owner's android phone. After receiving the notification, if the user does not respond to the notification within a pre-configured time, then the same notification is forwarded to the other five immediate contacts associated with the device. If the user responds to the notification within the specified time, then user has the options of either disarming the system or sending the message to the immediate contacts. The user is also offered the choice of informing the police using the notification itself. If the user chooses to disarm the system, then the system goes into sleep mode. All the sensors are inactive when the device is disarmed. The device can again be armed using the android app installed in the user's mobile phone. The same process continues again, the device waits for an intrusion to be detected. The total time of execution from detecting the theft to notifying the user takes around 10 seconds. There is a delay introduced in the process to avoid fake alarms. There would be cases when the owner itself will enter the house while it is armed and forgot to disarm it. So, those extra 8 seconds will allow the user to disarm the alarm using his/her android phone.

4. Testing

We took the readings of motion detected using radar microwave sensor. The data was uploaded on cloud using an API "io.adfruit.com". The API is available free for the first 30 days with limited access. Fig. 3. Shows the log of motion detected by the sensor and displayed on the application developed for android. The sensor is configured to respond every 5 seconds after the motion has been detected in the trial as shown the above picture. But, it can also be configured to the minimum of 2 seconds delay.



```
2018-08-18 13:53:39  MotionDetected  1
2018-08-18 13:53:59  MotionDetected  1
2018-08-18 13:54:04  MotionDetected  1
2018-08-18 13:54:09  MotionDetected  1
2018-08-18 13:54:19  MotionDetected  1
2018-08-18 13:54:24  MotionDetected  1
2018-08-18 13:54:29  MotionDetected  1
2018-08-18 13:54:39  MotionDetected  1
2018-08-18 13:54:44  MotionDetected  1
2018-08-18 13:54:54  MotionDetected  1
2018-08-18 13:54:59  MotionDetected  1
2018-08-18 13:55:09  MotionDetected  1
2018-08-18 13:55:14  MotionDetected  1
2018-08-18 13:55:19  MotionDetected  1
2018-08-18 13:55:29  MotionDetected  1
2018-08-18 13:55:39  MotionDetected  1
2018-08-18 13:55:49  MotionDetected  1
2018-08-18 13:55:59  MotionDetected  1
2018-08-18 13:56:04  MotionDetected  1
2018-08-18 13:56:09  MotionDetected  1
2018-08-18 13:56:29  MotionDetected  1
2018-08-18 13:56:34  MotionDetected  1
2018-08-18 13:56:44  MotionDetected  1
2018-08-18 13:56:49  MotionDetected  1
2018-08-18 13:56:54  MotionDetected  1
2018-08-18 13:56:59  MotionDetected  1
2018-08-18 13:57:04  MotionDetected  1
2018-08-18 13:57:09  MotionDetected  1
2018-08-18 13:57:19  MotionDetected  1
2018-08-18 13:57:34  MotionDetected  1
```

Fig. 3. Motion detected log displayed on android application

5. Wireframes

The module provides with all the screens for setting up the device. Device setup module is basically used when the user wants to configure the device with his/her android smartphone. The first step is to scan the QR code provided on the backside of the device. Then the device detected screen pops up if the device is verified successfully. Then the user will be asked to enter the Wi-Fi SSID and password in the blanks appearing on the next screen. This will configure the device with Wi-Fi settings and ESP8266 will be connected to home Wi-Fi network. The user will be redirected to the next screen which will offer five choices for the placement of the device. Finally, the test screen will ensure the correct functionality of the device.

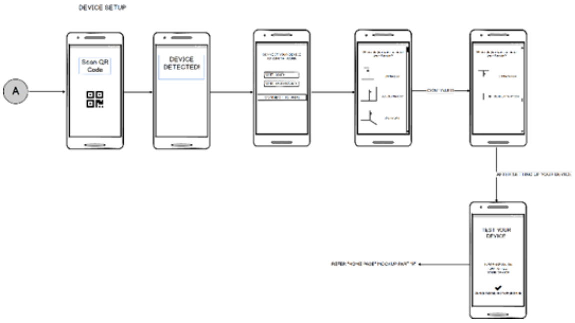


Fig. 4. Device setup module using Balsamiq studios

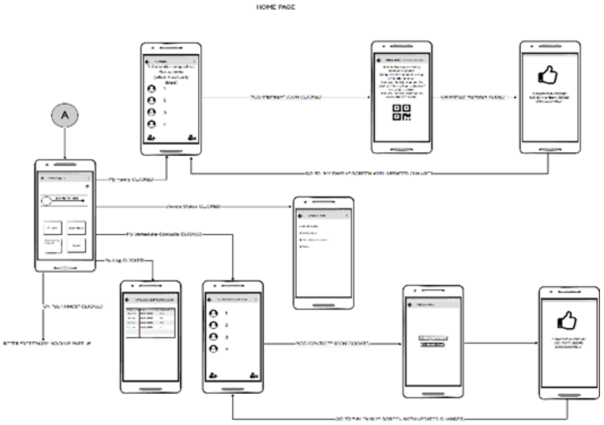


Fig. 5. Home page module using Balsamiq studios

The home page will consist of a slider bar, which will arm and disarm the system. Once the device is disarmed, the device will go into power saving mode and will not detect any intrusion. Basically, this is the main screen and will offer control to every other screen offered by the app. The screen will have four cards. Each card will redirect to a new activity. But, the card will also provide the live screen for the user which will allow to see the family members in the house and away from the house; device status parameters like battery status, device temperature, and individual sensor status. My log card will provide the user with the information of previous intrusions detected by the device in the past. The parameters will include, time of intrusion, date and detection status. My family card will display the users associated with a system. Every device can have a maximum of 5 family members and minimum of 1 member. The notification of intrusion will be received by the users added to My Family. My Immediate contacts are the second priority users after My Family users. The message received by the family members on intrusion can be forwarded to immediate contact users. Else, it will be automatically forwarded after the threshold time is reached. Join a family module is shown in Fig. 6. There are total three functionalities offered by this module. First is, the user can add multiple family members up to total of five users. The user to be added needs to scan the QR code generated on the existing user's android app. The new user needs to scan the code. The user will be redirected to the successfully added screen. Then further, the new user will be redirected to the home page. Second, if the user has an existing account, he/she must put the correct login credentials. The user will be redirected to the home screen. Third, if user selects forgot password option, a new screen will be opened and ask for the phone number. After clicking on VERIFY button, an OTP will be sent to the registered mobile number. The OTP will be auto detected by the application. The next activity will be changing the password.

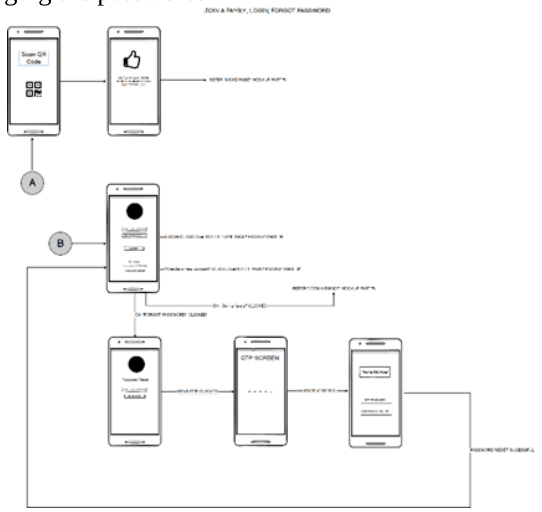


Fig. 6. Join a family module using Balsamiq studios

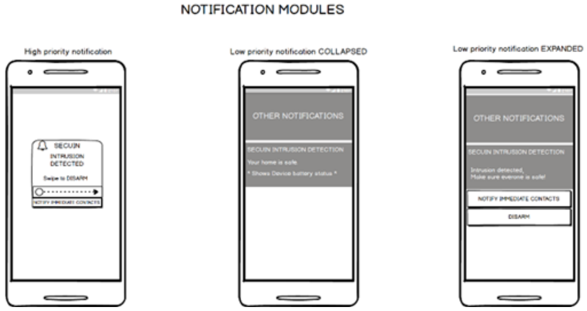

NOTIFICATION MODULES
High priority notification
SECUIN
INTRUSION DETECTED
Swipe to DISARM
NOTIFY IMMEDIATE CONTACTS
Low priority notification COLLAPSED
OTHER NOTIFICATIONS
SECUIN INTRUSION DETECTION
Your home is safe
* Shows Device battery status *
Low priority notification EXPANDED
OTHER NOTIFICATIONS
SECUIN INTRUSION DETECTION
Intrusion detected,
Make sure everone is safe!
NOTIFY IMMEDIATE CONTACTS
DISARM

Fig. 7. Notification module using Balsamiq studios

The user will be availed with two types of notification interfaces on Android as shown in Fig. 6.

A. *High priority notifications*

These notifications are ringed in the form of alarm. The most significant attribute of alarm notification is, it cannot be silenced. Hence, it is called as high priority notification.

B. *Low priority notifications*

These notifications are heads up and pops up on the status bar. Notifications can be also forced in the notification bar. So, it will notify the user about the status of device. The parameters displayed are, connectivity to the internet, battery status, temperature of device. These notifications can be collapsed and expanded as well. It provides with extra functionalities such as disarming the alarm. Following shown is the settings module in Fig. 8.

The settings module is responsible for altering four aspects. First are notifications; this function offers the user to set the notification tone. It also provides a choice for using the priority notifications. Second, alarm function allows the user to change the alarm volume and to set the vibrations for the same. Third, device button offers three functionalities. Change device will allow user to change the existing device. It can be done by removing the current device and scanning the QR code on the new device that is to be added. Sensitivity will allow the user to calibrate the device’s sensitivity. Ultimately, the last button logout will remove the account of the existing user. Then, the app will be redirected to the login page again. The settings module will function when the user opens the app for the first time. Initially a splash screen will appear, which displays our brand logo. If the user is opening the app for the first time, then on board screens will guide the user to brief about the product. Also, help the user in setting up the device. After the on boarding screens, the user will be redirected to the login module.

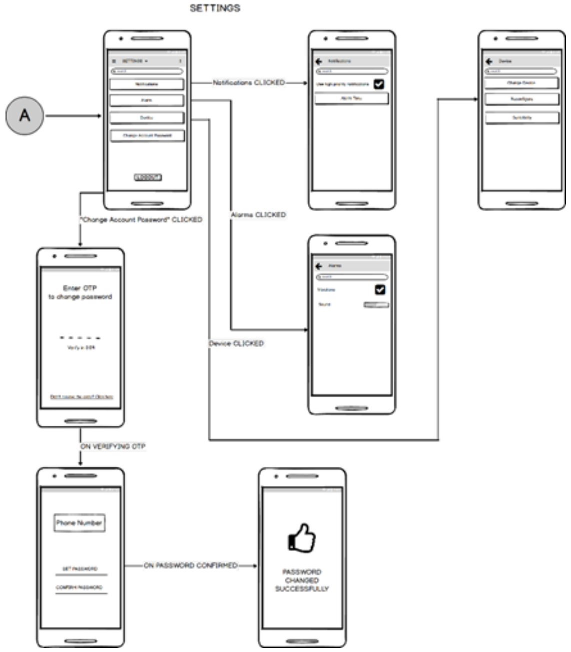


Fig. 8. Settings module using Balsamiq studios

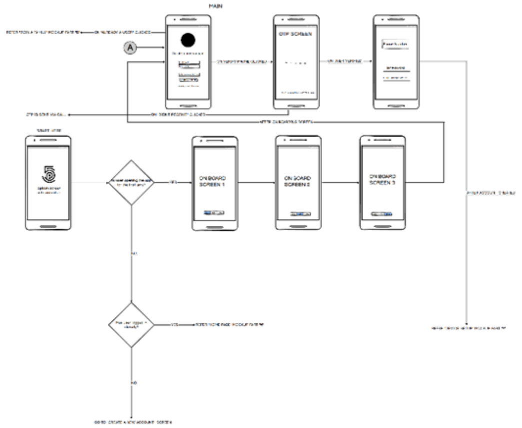


Fig. 9. Main module using Balsamiq studios

The mockups were designed using Balsamiq studios. The wireframes guide the programmer while designing and developing the app.

6. Conclusion

This paper presents the review of home security system. The system can be accessed and controlled using an android application. The development in security field is necessary, especially in India where the existing home security systems are costly and not closed loop.

References

[1] E. S. Kim, M. S. Kim, "Design and fabrication of security and home automation system", *Proceedings of International Conference on Computational Science and Its Applications Part III*, pp. 31-37, 2006.

[2] B. F. Wu, H. - Y. Peng, C. -J. Chen, "A practical home security system via mobile phones", *WSEAS Transactions on Communications*, vol. 5, pp. 1061-1066, 2006.

[3] L. Yang, S. -H. Yang, F. Yao, "Safety and security of remote monitoring and control of intelligent home environments", *Proceedings of IEEE International Conference on Systems Man and Cybernetics*, pp. 1149-1153, 2007.

[4] A. Alheraish, "Design and implementation of home automation system", *IEEE Transactions on Consumer Electronics*, vol. 50, pp. 1087-1092, 2004.

[5] S. M. Tsai, P.-C. Yang, S.-So Wu, S.-So Sun, "A service of home security system on intelligent network", *IEEE Transactions on Consumer Electronics*, vol. 44, pp. 1360-1366, 1998.